

# Resource Center

## Documentation





1. Blockbit GSM - Administrator's Guide	8
1.1 GSM - CHANGELOGS	9
1.1.1 Blockbit GSM version 2.4.2	11
1.1.2 Blockbit GSM version 2.4.1	12
1.1.3 Blockbit GSM version 2.4.0	14
1.1.4 Blockbit GSM version 2.3.0	15
1.1.5 Blockbit GSM version 2.2.2	18
1.1.6 Blockbit GSM version 2.2.1	19
1.1.7 Blockbit GSM version 2.2.0	20
1.1.8 Blockbit GSM version 2.1.1	21
1.1.9 Blockbit GSM version 2.1.0	23
1.1.10 Blockbit GSM version 2.0.13	24
1.1.11 Blockbit GSM version 2.0.12	25
1.1.12 Blockbit GSM version 2.0.11	26
1.1.13 Blockbit GSM version 2.0.10	27
1.1.14 Blockbit GSM version 2.0.9	28
1.1.15 Blockbit GSM version 2.0.8	29
1.1.16 Blockbit GSM version 2.0.7	31
1.1.17 Blockbit GSM version 2.0.6	32
1.1.18 Blockbit GSM version 2.0.5	33
1.1.19 Blockbit GSM version 2.0.4	34
1.1.20 Blockbit GSM version 2.0.2	35
1.1.21 Blockbit GSM version 2.0	36
1.1.22 Blockbit GSM version 1.2.3	37
1.1.23 Blockbit GSM version 1.2.1	38
1.1.24 Blockbit GSM version 1.2.0	39
1.1.25 Blockbit GSM version 1.1.3	40
1.1.26 Blockbit GSM version 1.1.0	41
1.2 GSM - VIRTUAL APPLIANCE	42
1.3 GSM - INSTALLATION FILES	44
1.4 GSM - How to Upgrade Kernel	45
1.4.1 GSM - How to Upgrade Kernel - How to generate a Backup	46
1.4.2 GSM - How to Upgrade Kernel - Console Access	49
1.4.3 GSM - How to Upgrade Kernel - System Update	51
1.4.4 GSM - How to Upgrade Kernel - Performing the Kernel Upgrade	56
1.4.5 GSM - How to Upgrade Kernel - Resetting the GSM	58
1.5 GSM - REVISIONS' HISTORY	59
1.6 GSM - INTRODUCTION	60
1.6.1 Resources – Blockbit GSM	61
1.6.2 Features – Blockbit GSM	62
1.6.3 Environment check for Blockbit GSM Installation	63
1.6.3.1 Installation requirements	64
1.6.4 About this Administrator Guide	65
1.7 ARCHITECTURE – BLOCKBIT GSM	66
1.8 INSTALLATION – BLOCKBIT GSM	68
1.8.1 GSM - Importing Virtual Machine	69
1.8.2 Start the Virtual Machine – First Access	74
1.9 CONFIGURING THE EXCEPTION	76
1.10 GSM - INSTALLATION WIZARD	80
1.11 GSM - NETWORK ENVIRONMENTS	84
1.12 GSM - NOTIFICATIONS VIA SNMP	86
1.12.1 GSM - Zabbix	87
1.13 GSM - WEB INTERFACE	94
1.14 GSM - BASIC OPERATION	96
1.15 GSM - USER PROFILE MENU	98
1.15.1 User Profile Menu - Profile	99
1.15.2 User Profile Menu – Logout	101
1.16 GSM - DEPLOYS PANEL	102
1.16.1 Deploys Panel - Search and Filters	104
1.16.2 Deploys Panel – Deploys List	105
1.16.2.1 Deploys Panel – Package column	107
1.16.2.2 Deploys Panel – Auditor column	108
1.16.2.3 Deploys Panel – Scheduled column	109
1.16.2.4 Deploys Panel – Progress column	110
1.16.2.5 Deploys Panel – Status column	111
1.16.2.6 Deploys Panel - Actions column	112
1.16.2.6.1 Deploys Panel – "Accept" button	113
1.16.2.6.2 Deploys Panel - "Reinstall" Button	114
1.16.2.6.3 Deploys Panel – "Cancel" button	115
1.16.2.6.4 Deploys Panel - "Activity" button	116
1.16.2.6.5 Deploys Panel – "Remove" button	117
1.17 GSM - INSTALL PACKAGE	118
1.17.1 What	119
1.17.2 Where	120
1.17.3 When	121
1.17.4 Who	122
1.18 GSM - MANAGEMENT	123
1.18.1 Devices	124
1.18.1.1 Inventory Tab	125

1.18.1.1.1 Inventory - Actions menu	126
1.18.1.1.2 Inventory - "Name" column	152
1.18.1.1.3 Inventory - Action buttons	153
1.18.1.1.4 Inventory - "Group" column	157
1.18.1.1.5 Inventory - "Model" column	159
1.18.1.1.6 Inventory - "License Status" column	161
1.18.1.1.7 Inventory - "Version" column	162
1.18.1.1.8 Inventory - "Template" column	163
1.18.1.1.9 Inventory - "Policy IPv4" column	164
1.18.1.1.10 Inventory - "Policy IPv6" column	165
1.18.1.1.11 Inventory - "Actions" column	166
1.18.1.2 Communities Tab	169
1.18.1.2.1 Communities - Actions menu	171
1.18.1.2.2 Communities - Columns	183
1.18.1.2.3 Communities - Communities Examples	184
1.18.1.3 Templates tab	197
1.18.1.3.1 Templates - Actions menu	198
1.18.1.3.2 Templates - Columns	205
1.18.1.4 Provisioning tab	213
1.18.1.4.1 Provisioning - Actions menu	215
1.18.1.4.2 Provisioning - Columns	243
1.18.1.5 Backups Tab	244
1.18.1.5.1 Backups - Actions Menu	246
1.18.1.5.2 Backups - Columns	252
1.18.1.5.3 Example - Device Backup	255
1.18.2 Profiles	280
1.18.2.1 Web Filter tab	282
1.18.2.1.1 Web Filter - Actions Menu	283
1.18.2.1.2 Web Filter - Columns	290
1.18.2.2 Application Control tab	298
1.18.2.2.1 Application Control - Actions menu	299
1.18.2.2.2 Application Control - Columns	306
1.18.2.3 Threat Protection Tab	311
1.18.2.3.1 Threat Protection - Actions menu	312
1.18.2.3.2 Threat Protection - Columns	319
1.18.2.4 Intrusion Prevention tab	327
1.18.2.4.1 Intrusion Prevention - Actions Menu	328
1.18.2.4.2 Intrusion Prevention - Columns	335
1.18.2.5 SSL Inspection tab	342
1.18.2.5.1 SSL Inspection - Actions menu	343
1.18.2.5.2 SSL Inspection - Columns	350
1.18.2.6 SD-WAN tab	354
1.18.2.6.1 SD-WAN - Actions menu	355
1.18.2.6.2 SD-WAN - Columns	362
1.18.3 Objects	368
1.18.3.1 Objects - Addresses	369
1.18.3.1.1 Objects - Addresses - Actions Menu	370
1.18.3.1.2 Objects - Addresses - Columns	388
1.18.3.2 Objects - Services	390
1.18.3.2.1 Objects - Services - Actions Menu	392
1.18.3.2.2 Objects - Services - Columns	405
1.18.3.3 Objects - Times	407
1.18.3.3.1 Objects - Times - Actions Menu	408
1.18.3.3.2 Objects - Times - Columns	415
1.18.3.4 Objects - Schedules	417
1.18.3.4.1 Objects - Schedules - Actions Menu	418
1.18.3.4.2 Objects - Schedules - Columns	425
1.18.3.5 Objects - Dictionaries	427
1.18.3.5.1 Objects - Dictionaries - Actions Menu	428
1.18.3.5.2 Objects - Dictionaries - Columns	436
1.18.3.6 Objects - Contents	438
1.18.3.6.1 Objects - Contents - Actions Menu	439
1.18.3.6.2 Objects - Contents - Columns	446
1.18.4 Users	448
1.18.4.1 Users tab	449
1.18.4.1.1 Users - Actions Menu	450
1.18.4.1.2 Users - Columns	454
1.18.4.2 Groups Tab	455
1.18.4.2.1 Groups - Actions Menu	456
1.18.4.2.2 Groups - Columns	463
1.18.5 Policies	467
1.18.5.1 Policy Packages Tab	468
1.18.5.1.1 Policy Packages - Actions menu	469
1.18.5.1.2 Policy Packages - Columns	477
1.18.5.2 Policy Templates tab	500
1.18.5.2.1 Policy Templates - Actions Menu	501
1.18.5.2.2 Policy Templates - Columns	509
1.19 GSM - ANALYTICS	515
1.19.1 Analyzer	516



1.19.1.1 Firewall	517
1.19.1.1.1 Firewall – Geolocation	521
1.19.1.1.2 Firewall – Zone Traffic	522
1.19.1.1.3 Firewall – Top User	524
1.19.1.1.4 Firewall – Top Service	525
1.19.1.1.5 Firewall – Top Source	526
1.19.1.1.6 Firewall – Top Policy	527
1.19.1.2 Web Filter	529
1.19.1.2.1 Web Filter - Allowed Sites and History	533
1.19.1.2.2 Web Filter - Denied Sites and History	534
1.19.1.2.3 Web Filter - History Categories - Total Traffic and Total Hits	535
1.19.1.2.4 Web Filter - History Content Types - Total Traffic and Total Hits	537
1.19.1.2.5 Web Filter - History Domains - Total Traffic and Total Hits	539
1.19.1.2.6 Web Filter - History Profiles - Total Traffic and Total Hits	541
1.19.1.2.7 Web Filter - Top Categories	543
1.19.1.2.8 Web Filter - Top Content Type	544
1.19.1.2.9 Web Filter - Top Domains	545
1.19.1.2.10 Web Filter - Top Domains by Time	546
1.19.1.2.11 Web Filter - Top Profiles	548
1.19.1.2.12 Web Filter - Top Users	549
1.19.1.2.13 Web Filter - Total Traffic and History	550
1.19.1.2.14 Web Filter - Users - Total Traffic and Total Hits	551
1.19.1.3 Application Control	553
1.19.1.3.1 Application Control - Allowed Application	556
1.19.1.3.2 Application Control - Denied Application	557
1.19.1.3.3 Application Control - History	558
1.19.1.3.4 Application Control - Top Allowed Categories	560
1.19.1.3.5 Application Control - Top Denied Categories	561
1.19.1.3.6 Application Control - Top Allowed Applications	562
1.19.1.3.7 Application Control - Top Denied Applications	564
1.19.1.4 Intrusion Prevention	568
1.19.1.4.1 Intrusion Prevention - Alerted, Blocked and History	572
1.19.1.4.2 Intrusion Prevention - Alerts by Geolocation	574
1.19.1.4.3 Intrusion Prevention - Impact - High	575
1.19.1.4.4 Intrusion Prevention - Impact - Medium	579
1.19.1.4.5 Intrusion Prevention - Impact - Low	583
1.19.1.4.6 Intrusion Prevention - Layer 3 Intrusion Protection	587
1.19.1.4.7 Intrusion Prevention - Intrusion Classification	590
1.19.1.4.8 Intrusion Prevention - Top Source	592
1.19.1.4.9 Intrusion Prevention - Top Destination	594
1.19.1.5 Threat Protection	596
1.19.1.5.1 Threat Protection - Threats and History	601
1.19.1.5.2 Threat Protection - Malwares and History	602
1.19.1.5.3 Threat Protection - Geolocation	603
1.19.1.5.4 Threat Protection - Impact - High	604
1.19.1.5.5 Threat Protection – Impact - Medium	606
1.19.1.5.6 Threat Protection – Impact - Low	608
1.19.1.5.7 Threat Protection – Malicious IP Classification	610
1.19.1.5.8 Threat Protection – Top Threat Types	613
1.19.1.5.9 Threat Protection – Top Users by Threats	615
1.19.1.5.10 Threat Protection – Top Users by Malware	617
1.19.1.5.11 Threat Protection – Top Malware	618
1.19.1.5.12 Threat Protection – Top Infected Domains	619
1.19.1.5.13 Threat Protection – Top Source	620
1.19.1.5.14 Threat Protection – Top Destination	622
1.19.1.6 User Behavior	624
1.19.1.6.1 User Behavior - History	627
1.19.1.6.2 User Behavior - Analysis Panel	628
1.19.1.6.3 User Behavior - Geolocation Information	650
1.19.1.7 Dashboard	652
1.19.2 Loggers	665
1.19.2.1 Logger installation	666
1.19.2.2 Loggers - Loggers	686
1.19.2.2.1 Loggers - Menu de ações	687
1.19.2.2.2 Loggers - Columns	695
1.19.2.3 Loggers - Clusters	698
1.19.2.3.1 Clusters - Actions Menu	700
1.19.2.3.2 Clusters - Columns	705
1.19.2.3.3 Clusters - Example	709
1.19.3 Reports	724
1.19.3.1 Reports - Actions Menu	725
1.19.3.1.1 Reports - Actions Menu - Create	726
1.19.3.1.2 Reports - Actions Menu - Delete	730
1.19.3.2 Reports - Columns	732
1.19.4 Events	733
1.19.4.1 Events - Query Editor	735
1.19.4.2 Events - Top Hits	738
1.19.4.3 Events - History	740
1.19.4.4 Events - Log Events	742

1.19.4.4.1 Events - Log Events - Event View	743
1.20 GSM - SETTINGS	744
1.20.1 System	745
1.20.1.1 System - "General" tab	746
1.20.1.2 System - "License" tab	753
1.20.1.3 System - "Updates" tab	756
1.20.1.4 System - "Backups" tab	757
1.20.1.4.1 System - Backups - Settings	758
1.20.1.4.2 System - Backups - Backups History	761
1.20.1.4.3 Example - Backup Manager	763
1.20.1.5 System - "Storages" tab	774
1.20.1.5.1 Storages - Actions Menu	775
1.20.1.5.2 Storages - Delete Storages	789
1.20.1.5.3 Storages - Columns	791
1.20.1.6 System - "High Availability" tab	792
1.20.1.6.1 High Availability - Cluster Settings	794
1.20.1.6.2 High Availability - Cluster Interfaces	796
1.20.1.6.3 High Availability - Cluster Status	797
1.20.1.6.4 High Availability - Example	799
1.20.1.7 System - "Certificates" tab	825
1.20.1.8 System - "Custom Branding" tab	827
1.20.1.9 System - Certificates tab	830
1.20.2 Network	834
1.20.2.1 Network - "General" tab	835
1.20.2.2 Network - "Interfaces" tab	836
1.20.2.3 Network - "E-mail" tab	838
1.20.3 Administration	840
1.20.3.1 Administration - "Administrators" tab	841
1.20.3.1.1 Administration - Administrators - Actions Menu	842
1.20.3.1.2 Administration - Administrators - Columns	846
1.20.3.2 Administration - "Users Profiles" tab	848
1.20.3.2.1 Administration - Users Profiles - Actions Menu	849
1.20.3.2.2 Administration - Users Profiles - Columns	857
1.20.3.3 Administration - "MFA" tab 2.5.0	858
1.20.3.4 Administration - "Auth Servers" tab	862
1.20.3.4.1 Administration - Auth Servers - Actions Menu	863
1.20.3.4.2 Administration - Auth Server - Columns	870
1.20.3.5 Administration - "Identity Provider" tab	872
1.20.3.5.1 Identity Provider - Service Provider	874
1.20.3.5.2 Identity Provider - Identity Provider	879
1.20.3.6 Administration - "Audit Log" tab	881
1.20.3.6.1 Audit View	883
1.20.3.7 Administration - "Access Control" tab	884
1.21 GSM - CLI - COMMAND LINE INTERFACE	885
1.21.1 GSM - [arp]	888
1.21.2 GSM - [arping]	889
1.21.3 GSM - [date]	890
1.21.4 GSM - [debug-backup]	892
1.21.5 GSM - [debug-deployer]	894
1.21.6 GSM - [debug-rotation]	895
1.21.7 GSM - [debug-sync]	896
1.21.8 GSM - [disable-snmp]	897
1.21.9 GSM - [enable-root]	898
1.21.10 GSM - [enable-snmp]	899
1.21.11 GSM - [ethtool]	901
1.21.12 GSM - [exit]	902
1.21.13 GSM - [fdisk]	903
1.21.14 GSM - [free]	905
1.21.15 GSM - [fsck]	906
1.21.16 GSM - [grep]	907
1.21.17 GSM - [help]	908
1.21.18 GSM - [history]	909
1.21.19 GSM - [hostname]	910
1.21.20 GSM - [ifconfig]	911
1.21.21 GSM - [ifstat]	913
1.21.22 GSM - [iotest]	914
1.21.23 GSM - [ip]	915
1.21.24 GSM - [ipcalc]	916
1.21.25 GSM - [less]	917
1.21.26 GSM - [logger-config]	918
1.21.27 GSM - [logger-devices-add]	921
1.21.28 GSM - [logger-devices-list]	922
1.21.29 GSM - [logger-disable]	923
1.21.30 GSM - [logger-enable]	924
1.21.31 GSM - [logger-key]	925
1.21.32 GSM - [lscpu]	926
1.21.33 GSM - [mkfs]	927
1.21.34 GSM - [more]	928
1.21.35 GSM - [netstat]	929

1.21.36 GSM - [ntpdate]	930
1.21.37 GSM - [passwd]	931
1.21.38 GSM - [ping]	932
1.21.39 GSM - [reboot]	933
1.21.40 GSM - [reset]	934
1.21.41 GSM - [reset-admin-blocks]	935
1.21.42 GSM - [reset-admin-password]	936
1.21.43 GSM - [reset-admin-sessions]	937
1.21.44 GSM - [reset-logs]	938
1.21.45 GSM - [rewizard]	939
1.21.46 GSM - [route]	940
1.21.47 GSM - [sar]	942
1.21.48 GSM - [set-network-dns]	943
1.21.49 GSM - [set-network-gateway]	944
1.21.50 GSM - [set-network-hostname]	945
1.21.51 GSM - [set-network-interface]	947
1.21.52 GSM - [set-network-timezone]	948
1.21.53 GSM - [show-devices]	949
1.21.54 GSM - [show-license]	950
1.21.55 GSM - [show-uuid]	951
1.21.56 GSM - [show-version]	952
1.21.57 GSM - [shutdown]	953
1.21.58 GSM - [tcpdump]	954
1.21.59 GSM - [tcpdump]	955
1.21.60 GSM - [telnet]	956
1.21.61 GSM - [tracpath]	958
1.21.62 GSM - [traceroute]	959
1.21.63 GSM - [update-gsm]	962
1.21.64 GSM - [update-license]	964
1.21.65 GSM - [upgrade-blockbit]	965
1.21.66 GSM - [uptime]	966
1.21.67 GSM - [vmstat]	967
1.21.68 GSM - [whois]	968
1.22 GSM - Manuals and How tos	971

# Blockbit GSM - Administrator's Guide

## Index

[Expandir todos](#) [Recolher todos](#)

# GSM - CHANGELOGS

To see the list containing the Changelogs from all previous versions, [click here](#).

## Release Notes 2.4.1.

Some features have been implemented in the release of Blockbit GSM 2.4.1:

- The [GSM API](#) has been implemented for remote queries.

The following table lists the improvements present in the Blockbit GSM 2.4.1:

Code	Description
15875	Correction done in the update of objects of the IP type included in groups of objects after the deploy.
25981	Correction done in the packages listing when adding a new ones on the Package templates.
31842	Improvement done in the device templates' deploy settings.
33991	Optimization done in the server's resources consumption.
34815	Correction done in the reports' .csv timestamp of the log sessions type.
34816	Correction done in the generation of reports.
35070	
34853	Correction done in the sending of unchecked e-mails.
35327	Improvement done in the Analyzer's logs presentation IPS.
35978	Improvement done in the access to the Application Control Profile's database.
36126	Correction done in the display of periods on the Analyzer's PDF reports.
36409	Improvement done in the display of <i>timestamps</i> on single cloned reports.
36960	Improvement done on the deploy of Policies.
39495	
39804	Correction done in the device search filter.
40191	Correction done in the Web Filter profile editing.
40192	Correction done in the IPS Profile search filter.
40940	Correction done in the Identity Provider certificate creation.
40942	Correction done to certificate import in Identity Provider.
41320	Correction done in the global action button for IPS signatures.
41411	Correction done in the validation of duplicate and obscure rules in Policy Package.
41951	Correction done in the deployment of Content type Objects.
42016	Optimization and security improvement done in the centralized backup service.
42157	Correction done in license application when device provisioning via ZTP.
43432	Correction done in the Firewall, Web Cache and DNS service on device template deployment.
43435	Correction done in the Web Filter service block message in Device Template.

<b>43439</b>	Correction done in the Device Template deployment of Threat Protection, IPS and SD-WAN service settings.
<b>43441</b>	
<b>43442</b>	
<b>43443</b>	
<b>43444</b>	
<b>47633</b>	Improvement done in the error message for Device Template configuration review.
<b>48485</b>	Optimization and security improvement done in the centralized backup service.

Previous Versions:

[Blockbit GSM version 2.4.0](#)

[Blockbit GSM version 2.3.0](#)

[Blockbit GSM version 2.2.2](#)

[Blockbit GSM version 2.2.1](#)

[Blockbit GSM version 2.2.0](#)

[Blockbit GSM version 2.1.1](#)

[Blockbit GSM version 2.1.0](#)

[Blockbit GSM version 2.0.13](#)

[Blockbit GSM version 2.0.12](#)

[Blockbit GSM version 2.0.11](#)

[Blockbit GSM version 2.0.10](#)

[Blockbit GSM version 2.0.9](#)

[Blockbit GSM version 2.0.8](#)

[Blockbit GSM version 2.0.7](#)

[Blockbit GSM version 2.0.6](#)

[Blockbit GSM version 2.0.5](#)

[Blockbit GSM version 2.0.4](#)

[Blockbit GSM version 2.0.2](#)

[Blockbit GSM version 2.0](#)

[Blockbit GSM version 1.2.3](#)

[Blockbit GSM version 1.2.1](#)

[Blockbit GSM version 1.2.0](#)

[Blockbit GSM version 1.1.3](#)

[Blockbit GSM version 1.1.0](#)

[Return](#)

# Blockbit GSM version 2.4.2

## Release Notes

14/10/2024

**Some features have been implemented in the release of Blockbit GSM 2.4.2:**

Improvement done in the deployment of policy packages and profiles related to dynamic and static application groups.

**The following table lists the improvements present in the Blockbit GSM 2.4.2:**

Code	Description
15875	Improvement done in the update of the GSM's deploy over IP objects that are within object groups in the NGFW.
25891	Correction done in the listing of GSM's Policy Packages when adding new Policy Packages.
33991	The GSM's CPU consumption through processes has been optimized.
34815	The timestamps, displayed on .CSV reports of the log session type, have been corrected.
34816	Improvement done in the generation of the "all types" reports, recurring daily, weekly and monthly and on their respective timestamps.
34853	The functioning of the button that activates the sending of reports via e-mail (in Analytics Reports) has been fixed.
35070	The GSM reports generation process has been optimized.
36126	Correction done in the display of periods of time on the Analyzer's PDF reports.
36960	Correction done on the deploy of Policy Packages.
39495	

# Blockbit GSM version 2.4.1

## Release Notes

21/11/2023

Some features have been implemented in the release of Blockbit GSM 2.4.1:

- The **GSM API** has been implemented for remote queries.

The following table lists the improvements present in the Blockbit GSM 2.4.1:

Code	Description
15875	Correction done in the update of objects of the IP type included in groups of objects after the deploy.
25981	Correction done in the packages listing when adding a new ones on the Package templates.
31842	Improvement done in the device templates' deploy settings.
33991	Optimization done in the server's resources consumption.
34815	Correction done in the reports' .csv timestamp of the log sessions type.
34816	Correction done in the generation of reports.
35070	
34853	Correction done in the sending of unchecked e-mails.
35327	Improvement done in the Analyzer's logs presentation IPS.
35978	Improvement done in the access to the Application Control Profile's database.
36126	Correction done in the display of periods on the Analyzer's PDF reports.
36409	Improvement done in the display of <i>timestamps</i> on single cloned reports.
36960	Improvement done on the deploy of Policies.
39495	
39804	Correction done in the device search filter.
40191	Correction done in the Web Filter profile editing.
40192	Correction done in the IPS Profile search filter.
40940	Correction done in the Identity Provider certificate creation.
40942	Correction done to certificate import in Identity Provider.
41320	Correction done in the global action button for IPS signatures.
41411	Correction done in the validation of duplicate and obscure rules in Policy Package.
41951	Correction done in the deployment of Content type Objects.
42016	Optimization and security improvement done in the centralized backup service.
42157	Correction done in license application when device provisioning via ZTP.
43432	Correction done in the Firewall, Web Cache and DNS service on device template deployment.
43435	Correction done in the Web Filter service block message in Device Template.



<b>43439</b>	Correction done in the Device Template deployment of Threat Protection, IPS and SD-WAN service settings.
<b>43441</b>	
<b>43442</b>	
<b>43443</b>	
<b>43444</b>	
<b>47633</b>	Improvement done in the error message for Device Template configuration review.
<b>48485</b>	Optimization and security improvement done in the centralized backup service.

# Blockbit GSM version 2.4.0

## Release Notes

27/02/2023

Some features have been implemented in the release of Blockbit GSM 2.4.0:

- The option to send [reports](#) generated by the analyzer via e-mail has been implemented.
- Support to [CGNAT](#) (Carrier Grade Network Address Translator) has been implemented.
- The [Anti-Spam Filter](#) functionality has been implemented.
- The display of the top 10 users per application in the form of a [Dashboard](#) has been implemented, in Monitor > Dashboard.

The following table lists the improvements present in the Blockbit GSM 2.4.0:

Code	Description
20509	
20730	Correction done in the search of Top categories in the Web Filter (Analyzer and Dashboard).
20732	
18153	Correction done in the Firewall when saving a Template.
18223	Correction done in the Firewall when editing a Template.
18224	Correction done in the settings screen of Templates.
18225	Correction done in the cloning process of Templates.
18286	Correction done in the "monitor" icon, which access the NGFW.
18287	Correction done in the NGFW remote accessing process.
18449	Improvement done in the display of the clone and delete options, which used to be available even without a selected item, in Device Templates.
20732	Correction done in Web Filter Top Categories' search box.
20734	Improvement done in the generation of reports on preset schedules.
24125	Correction done in the ACL permissions.
24270	Improvement done in the Log's display, in groups containing a Device, in Devices > Inventory.
24955	Improvement done in the apply of new Policies to a NGFW.
25841	Correction done when accessing the "Dashboard" screen.
26863	Improvement done when saving settings in Device Templates.
29325	Correction done when validating policies in "Policy Manager"
29584	Correction done when creating SD-WAN profiles in Device Template.
29587	Correction done when creating Intrusion Prevention (IPS) profiles in Device Template.
29675	Correction done when creating Query in Events.
29852	Correction done when performing deploy in cloned Device Template.
33769	Correction done in the CSV reports.
34815	Correction done in the timestamp reports (.csv) of <i>log sessions</i> type.
34853	Correction done when sending e-mails without selecting the checkbox.

# Blockbit GSM version 2.3.0

## Release Notes

31/10/2022

New features have been implemented in the release of Blockbit GSM 2.3.0:

- An [option to insert root certificates](#) for the Proxy's SSL Inspection has been implemented.
- A new function has been implemented to [check and validate Firewall Policies](#).
- A third peer has been implemented in [H.A.](#)
- The Sync Interval's minute insertion field in H.A has been standardized.
- The [PCAP option](#) has been implemented in Intrusion Prevention > Profile Creation.
- The timeout field has been reallocated in the [Firewall's Settings](#).

The following table lists the improvements present in the Blockbit GSM 2.3.0:

Code	Description
T1-1252	Correction done in the language selection box in the Wizard.
T1-1403	Improvement done in the time display in Events and in the Analyzer.
T1-1478	Correction done in the message displayed when confirming the password, in Settings > System > Backup.
T1-1541	Correction done in the default values displayed in TCP Max Orphans, in Settings > Authentication > Synchrony.
T2-2193	Improvement done in the naming of the "max" field to max connections. Max from "Timeout" has been transferred to timeout in Security Settings.
T3-198	Improvement done in the compatibility of deploys among the GSM's versions.
T3-340	Improvement done in the message displayed in the provisioning setup.
T3-354	Correction done in the navigation between tabs, in Administration > Devices.
T3-444	Improvement done in the creation of IPS profile with the PCAP option, in Profiles > Intrusion Prevention > 2.3.0 Profile.
T3-446	Improvement done in the creation of IPS Profiles of the Packet Logger type.
T3-450	Correction done in the PCAP options disable in the creation of IPS Profiles of the Packet Logger type.
T3-454	Improvement done in the signatures filtering when creating IPS Profiles of the Packet Logger type.
T3-583	
T3-459	Improvements done in the Policy package creation, in Policies > Policy Package > Create Package.
T3-463	Improvement done in the Deploys' screen.
T3-568	Improvement done in the signatures search in Intrusion Prevention – PCAP.
T3-595	Correction done in the Policy Packages' deploy authorization process.
T3-652	Improvement done in the creation of Loggers' clusters.
T3-653	Improvement done in the licensing keeping after setting up the environment in cluster.
SUS-1	Improvement done in the functioning of the management interface's assignments.
SUS-7	Improvement done in the SSL Inspection Profiles deletion process, after the deploy of Policy Packages.
SUS-42	Correction done in the message displayed when restoring snapshots from different versions of the GSM.
SUS-51	Improvements done in the system's field namings in Spanish.
SUS-52	Improvement done in access control's permissions.
SUS-53	Improvement done in the display of mandatory fields in Devices Communities.
SUS-67	Improvement done in the deploy of Policies.
SUS-72	Correction done in the information displayed in the backup process via SMB.
SUS-81	Improvement done in the display of App routings selected in IPv4 profiles that have been imported via deploy.

<b>SUS-89</b>	Correction done in the IPs obtention process in the DDNS configuration.
<b>SUS-100</b>	Correction done in the display of network interfaces after provisioning.
<b>SUS-127</b>	Improvement done in the synchronization of the NGFW base registered in the GSM.
<b>SUS-130</b>	Correction done in the password recovery process.
<b>SUS-132</b>	Correction done in the password field, in the e-mail settings.
<b>SUS-302</b>	Improvement done in the creation of rules for Policy Templates.
<b>SUS-309</b>	Improvement done in the Access to NGFWs via command interface via GSM.
<b>SUS-321</b>	Improvement done in the information saving process in the database.
<b>5219</b>	Improvement done in the deploy of Policies using App Control, IPS, ATP, Web Filter and SSL Inspection profiles.
<b>8415</b>	Correction done in the text of the language selection button.
<b>8440</b>	Improvement done in the assigned values in the TCP Max Orphans field.
<b>8505</b>	Improvement done in the time schedule display in the analyzer's graphics.
<b>8526</b>	Improvement done in the deploy of provisioning settings.
<b>8547</b>	Improvement done in the password verification when generating backup, in Settings > System > Backup.
<b>8549</b>	Correction done in the language used in the message that appears when asking for the user's password during the creation of a backup.
<b>9777</b>	Improvement done in the display of IPS Profiles in Zone Protection.
<b>9883</b>	Improvement done in the signs that show a mandatory field in Device Template and Policy Packages.
<b>9900</b>	Improvement done in the tab signaling during browsing.
<b>9929</b>	Improvement done in the (Web Filter, SD-WAN, App Control, Threat Protection, IPS and SSL Inspection) Templates and Profiles settings.
<b>9993</b>	Improvement done in the PCAP options display in the IPS settings with Packet Logger.
<b>9996</b>	Melhorias feitas no funcionamento de PCAP nas configurações de IPS.
<b>10000</b>	
<b>10004</b>	
<b>10010</b>	Improvement done in the deploy panel display.
<b>10130</b>	Correction done in the information previously inserted in the PCAP signatures field.
<b>10137</b>	Improvement done in the functioning of the IPS filter.
<b>10219</b>	Improvement done in the Loggers' clusters.
<b>10220</b>	Improvement done in the creation of backup profiles in Devices.
<b>10223</b>	Improvements done in the information previously inserted in the App Control "workers" field.
<b>10275</b>	Correction done in the Policies Packages' deploy script.
<b>12830</b>	Improvement done in the functioning of the main screen's expand button, used to show more options on the main menu.
<b>13677</b>	Improvement done in the display of standard values in the NGFW's modules settings.
<b>13698</b>	Correction done in the naming of the GSM's backup storage, from SFTP to SSH.
<b>13722</b>	Correction done in the message displayed in the subtitles when deleting Device Templates.
<b>13728</b>	Improvement done in the NGFWs accessibility through the GSM.
<b>13958</b>	Correction done in the display of configuration fields in Device Templates.

<b>13963</b>	Improvement done in the editing of the NGFW's Device Templates.
<b>14144</b>	Improvement done in the Policy Packages deploy.
<b>14208</b>	Improvement done in the deploy of Device Templates to NGFWs.
<b>14663</b>	Improvement done in the saving of information on the Device Templates fields when creation a new profile.
<b>15237</b> <b>15240</b> <b>15248</b>	Improvement done in the compatibility and functioning of NGFWs' Policies from previous versions with the GSM 2.3.0.
<b>18153</b> <b>18223</b> <b>18224</b>	Improvement done in the functioning of Device Templates with the Firewall's settings activated.
<b>20509</b> <b>20730</b> <b>20732</b>	Correction done in the search of Top cathegories in the Web Filter (Analyzer and Dashboard).

# Blockbit GSM version 2.2.2

## Release Notes

02/08/2022

The following table lists the improvements done in the release of the Blockbit GSM 2.2.2:

Code	Description
<b>T1-287</b>	Correction done in the license key reapplication.
<b>T1-1080</b>	Improvement done in the creation of snapshots with password.
<b>T1-1403</b>	Improvement done in the time display in Events and in the Analyzer.
<b>T1-1431</b>	Improvement done in the ETH settings when creating a Device, in the Provisioning tab.
<b>T1-1478</b>	Correction done in the message displayed when requesting the password in the creation of a Backup, in Settings > System > Backups.
<b>T1-1541</b>	Correction done in the default values displayed in TCP Max Orphans, in Settings > Authentication > Synchrony.
<b>T2-964</b>	Improvement done in the loading of files required for the REDIS to work in full capacity.
<b>T2-1086</b>	Correction done in the language used in some parts of the Wizard.
<b>SUS-100</b>	Improvement done in the network interfaces display after provisioning.
<b>5307</b>	

# Blockbit GSM version 2.2.1

## Release Notes

30/05/2022

Some features have been implemented in the release of Blockbit GSM 2.2.1:

- Support to *Whitelist* has been implemented, so that set IP addresses can access the management interface.

The following table lists the improvements done in the release of the Blockbit GSM 2.2.1:

Code	Description
T1-637	Improvement done in the creation of policies' deploys.
T1-842	Correction done in the version number display in IPv4 and IPv6 Policies.
T1-871	Improvement done in the memory value displayed in the Logger.
T1-976	Improvement done in the VPN IPSEC Site to Site general settings.
T1-1041	A command for updating the Logger has been implemented.
T2-6	Improvement done in the security of the updates redirecting.
T2-1054	Correction done in the Device Templates' saving.

# Blockbit GSM version 2.2.0

## Release Notes

23/08/2021

Several features have been implemented in the release of Blockbit UTM 2.2.0:

- An option to clone Profiles ([Web Filter](#), [App Control](#), [Threat Protection](#), [Intrusion Prevention](#), [SSL Inspection](#), [SD-WAN](#)) between GSM versions has been implemented.
- An option to clone Policy [Packages](#) and [Templates](#) between GSM versions has been implemented.

The following table lists the improvements done in the release of the Blockbit GSM 2.2.0:

Code	Description
T1-201	Correction done in the audit Logs settings editing.
T1-230	Improvement done in the Policy Packages with objects deploy.
T1-419	Correction done in the Traffic Monitor option in IPv4 and IPv6 Policies setup.
T1-586	Improvement done in the SAML access restrictions validation.
T1-773	Correction done in the version display in the terminal.
T1-937	Improvement done in the cloning and editing of Device Templates.
T1-942	Improvement done in the update validation.
T1-977	Improvement done in the update Logs display.
T1-981	Improvement done in the Policy Templates' group creation.
T1-987	Improvement done in the GSM's Backup restoration through Snapshot.
T1-999	Improvement done in the policy rules export from the GSM to the UTM.
T1-1012	Improvement done in the Device Template setup with SDWAN export.
T2-7	Improvement done in the data search of the Logger.
T2-129	Correction done in the Logs generation in Analyzer and Events.
T2-145	Improvement done in the version selection for Backup restoration.
T2-199	Improvement done in the Security Events and Analyzer's Logs display.
T2-207	Improvement done in the display of the Web filter's reports.
T2-238	Improvement done in the time display in the Security Events' Logs.
T2-282	Update done in Rpc.statd, Open SSH, Nginx; DH Key Exchange (PCI DSS). The Cryptography module has also been improved.
T2-391	Improvement done in the Policy Templates setup and IPv4 and IPv6 Policies.
T2-395	Improvement done in the Application Control profile cloning.
T2-528	Improvement done in the Wizard's redirecting.
T2-756	Improvement done in the e-mail settings.
T2-757	Improvement done in the pages display in Policy Templates.
T2-758	Improvement done in the import of Policy Templates with NAT from other GSM versions.
GSM-1844	Improvement done in the messages displayed in the cloning of Device Templates.
GSM-1954	Improvement done in the manual process of system update.
GSM-1955	Improvement done in the information saving in e-mail Settings.
GSM-1961	Improvement done in the items display in Policy Templates.



# Blockbit GSM version 2.1.1

## Release Notes

23/08/2021

Several features have been implemented in the release of the Blockbit GSM 2.1.1:

- Implemented object search bar in [Zone Protection](#).
- Implemented message referring to the storage's status in *Backups* history.
- Added tool to clone profiles in [Web filter](#), [Application Control](#), [Threat Protection](#), [Intrusion Prevention](#), [SSL Inspection](#) and [SD-WAN](#).
- Added tool to clone [Policy Templates](#), [Policy Packages](#) and [Device Templates](#).
- Implemented [auto sync option](#) in the GSM's first synchronization.
- Implemented multiple categories selection option in [Web filter Profile](#).
- Implemented function to clone Header and Footer Policies in [Policy Packages](#).

The following table lists the improvements done in the release of the Blockbit GSM 2.1.1:

Code	Description
<b>GSM-2</b>	Implemented function to clone Policy Templates.
<b>GSM-3</b>	
<b>GSM-5</b>	Improvement done in the Logger services execution.
<b>GSM-147</b>	Improvement done in the status monitoring.
<b>GSM-148</b>	Improvement done in the process validation in Deploy.
<b>GSM-166</b>	Improvement done in the standard Proxy ports setup.
<b>GSM-248</b>	Modification done in the message displayed when editing SD-WAN profiles.
<b>GSM-269</b>	Improvement done in the editing of Web filter profiles.
<b>GSM-387</b>	Improvement done in the characters insertion in System > General > Network > Interfaces.
<b>GSM-482</b>	Improvement done in the creation and configuration of profiles.
<b>GSM-517</b>	Improvement done in the display of information when synchronizing bound Devices for the first time.
<b>GSM-894</b>	Correction done in the saving of interfaces in provisioning.
<b>GSM-970</b>	Improvement done in the Logger's settings when desynchronizing a UTM device.
<b>GSM-1093</b>	Improvement done in the synchrony with UTM devices.
<b>GSM-1291</b>	Correction done in the export of SSL Profiles from a UTM device.
<b>GSM-1349</b>	Improvement done in the creation of objects in IPV6 Policies.
<b>GSM-1722</b>	Improvement done in the results display in Analytics > Events.
<b>GSM-1768</b>	Improvement done in the deploy of Device Templates.
<b>GSM-1769</b>	Improvement done in the Policy Templates importing.
<b>GSM-1771</b>	Improvement done in the deploy of IPV6 Policy Packages.
<b>GSM-1773</b>	Improvement done in the IPV6 Policy Packages application.
<b>GSM-1813</b>	Improvement done in the SAML authentication.
<b>GSM-1834</b>	Correction done in the XML import from the IDP SAML.
<b>GSM-1837</b>	Improvement done in the cloning of Policy Templates.

<b>GSM-1842</b>	Improvements done in the Device Template cloning process.
<b>GSM-1841</b>	
<b>GSM-1815</b>	
<b>GSM-1812</b>	
<b>GSM-1811</b>	
<b>GSM-1810</b>	
<b>GSM-1845</b>	Improvement done in the creation of Policy Packages, IPV4/IPV6 rules.
<b>GSM-1846</b>	Correction done in the process of Policy Packages cloning.
<b>GSM-1847</b>	Improvement done in the creation of Policy templates, IPV4/IPV6 rules.
<b>GSM-1857</b>	Improvement done in the TLS security protocols.
<b>GSM-1874</b>	Improvement done in the Zone Protection profiles creation.
<b>GSM-1888</b>	Improvement done in the Web filter creation.
<b>GSM-1890</b>	Correction done in the data replication in the Loggers' Clusters.
<b>GSM-1897</b>	Correction done in the Backup display in the Logger.
<b>GSM-1898</b>	Correction done in the Log Backup restoration of the Logger.

# Blockbit GSM version 2.1.0

## Release Notes

16/04/2021

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit GSM 2.1.0:

- Implementation of the [centralized backup](#) management service for Firewalls;
- Implementation of the centralized management service for [loggers backup](#);
- Implementation of the [automatic backup service of Manager configurations](#);
- Implementation of the [Manager's high availability](#) service;
- Implementation of the [high availability service for Loggers](#);
- Addition of [Login Disclaimer](#) for GSM administrative users;
- System integration with [SAML](#) identity providers;
- Implementation of the Analyzer log maintenance and [retention](#) policy;
- Addition of the command [\[set-network-hostname\]](#), allowing to define the hostname of the system through the CLI.

The following table lists the improvements made in the release of Blockbit GSM:

Code	Description
<b>GSM-740</b>	Correction in the creation of policies with DPI profile
<b>GSM-754</b>	Correction in UTM remote authentication by GSM
<b>GSM-1091</b>	Correction applied to cloning of Policy Templates policies
<b>GSM-1140</b>	Correction in the device communities deploy window
<b>GSM-1189</b>	Correction in the progress bar in the deployment of device communities
<b>GSM-1266</b>	Correction in the password field in the form for creating and editing Devices
<b>GSM-1269</b>	Fix device deployment scheduling
<b>GSM-1293</b>	Correction applied to custom branding deploy
<b>GSM-1378</b>	Improved manager performance
<b>GSM-1380</b>	Correction in the display of the label device in the backup registration form
<b>GSM-1474</b>	Correction in the display of the items listed in the Analyzer reports
<b>GSM-1480</b>	Correction in the SMB storage creation window
<b>GSM-1486</b>	Fixes in the Device Logger creation window
<b>GSM-1487</b>	
<b>GSM-1489</b>	Implementation of the new disable-snmp CLI command
<b>GSM-1502</b>	Application control button fixes
<b>GSM-1515</b>	Various improvements and adjustments to the layout and custom branding features, enabling use as Whitelabel
<b>GSM-1524</b>	
<b>GSM-1525</b>	
<b>GSM-1547</b>	Correction in the display of custom branding after restoration by snapshot
<b>GSM-1550</b>	Correction in the synchronization of the rules of the Policy Package version 2.0.7 to 1.5.15

# Blockbit GSM version 2.0.13

## *Release Notes*

02/08/2022

### Updates and improvements presented in the BLOCKBIT GSM Version 2.0.13:

Code	Description
<b>GSM-2013</b>	Correction done in the message displayed when inputting special characters in the password field, in Settings > Network > E-mail.
<b>T1-1080</b> <b>T1-1478</b> <b>8549</b>	Improvement done in the creation of snapshots protected by password.
<b>T1-1403</b>	Improvement done in the time display in Events and in the Analyzer.
<b>T1-1431</b>	Improvement done in the ETH settings when creating a Device, in the Provisioning tab.
<b>T2-1086</b>	Correction done in the language used in some parts of the Wizard.
<b>8526</b>	Improvement done in the deploy of provisioning settings.

# Blockbit GSM version 2.0.12

## *Release Notes*

30/05/2022

### Updates and improvements presented in the BLOCKBIT GSM Version 2.0.12:

Code	Description
<b>T1-871</b>	Correction done in the information displayed in the Logger's settings.
<b>T1-1041</b>	Improvement done in the GSM's update command.
<b>T1-1057</b>	Improvement done in the deploy of Device Templates between a UTM and a GSM.
<b>T2-6</b>	Improvement done in the GSM's update patch.
<b>T2-825</b>	Improvement done in the Policy packages' cloning process.
<b>T2-1054</b>	Correction done in the saving process of Device Templates.
<b>T2-1100</b>	Correction done in the saving of forms when creating a community, in Devices.
<b>T2-1119</b>	Improvement done in the deploy of Application control with Policies.

# Blockbit GSM version 2.0.11

## *Release Notes*

24/08/2021

Updates and improvements presented in the BLOCKBIT GSM Version 2.0.11.

Code	Description
T1-87	Improvement done in the creation of Zone Protection rules through the Device Template.
T1-201	Correction done in the e-mail settings display in the Audit Logs.
T1-230	Improvement done in the Policy Packages deploy.
T2-129	Improvement done in the Logs display by date.
T2-145	Correction done in the Backup restoration.
T2-282	Update done in Rpc.statd, Open SSH, Nginx; DH Key Exchange (PCI DSS) cryptography module has been improved.
T2-391	Improvement done in the Policy Templates setup and IPV4 and IPV6 Policies.

# Blockbit GSM version 2.0.10

## Release Notes

23/08/2021

### Updates and improvements presented in the BLOCKBIT GSM Version 2.0.10.

Code	Description
<b>GSM-5</b>	Improvement done in the execution of Logger services.
<b>GSM-166</b>	Improvement done in the Proxy settings, in Device Templates.
<b>GSM-387</b>	Improvement done in the editing of the GSM's fields.
<b>GSM-482</b>	Improvement done in the creation and configuration of profiles.
<b>GSM-543</b>	Improvement done in the information displayed in the UTM's analyser in comparison to the GSM's.
<b>GSM-747</b>	Improvements and optimizations in the number of registers of the UTM and GSM's Analyser.
<b>GSM-894</b>	Correction done in the validation of doubled network interfaces in provisioning.
<b>GSM-1105</b>	Improvement done in the license validation process.
<b>GSM-1349</b>	Improvement done in the creation of service objects, in Ipv6 Policies.
<b>GSM-1639</b>	Correction done in the block information displayed in the Analyzer.
<b>GSM-1708</b>	Correction in the user validation in the deploy of Policy Packages.
<b>GSM-1728</b>	Improvements and optimizations in the Query Editor of Security Events.
<b>GSM-1743</b>	Improvement in the number of registers of "Top Allowed Applications", in Analyser > App Control.
<b>GSM-1857</b>	Security update in the TLS protocol.
<b>GSM-1874</b>	Improvement done in the field validation in the Device Template creation, in Zone Protection.
<b>GSM-1875</b>	Correction done in the display of doubled items, in Devices > Inventory.
<b>GSM-1886</b>	Correction done in the editing of Scheduling Groups.
<b>GSM-1888</b>	Improvement done in the field validation in the profile creation, in Web filter.
<b>GSM-1893</b>	Improvements in the layout of the Reports page, in User Behavior.
<b>GSM-1924</b>	Security update in the interface provisioning service of system administration.
<b>GSM-1927</b>	Correction done in the deletion of Device Templates.

# Blockbit GSM version 2.0.9

## Release Notes

17/05/2021

The following table lists the improvements made in the release of Blockbit GSM 2.0.9.

Code	Description
<b>GSM-147</b>	Improvements in the remote device monitoring service.
<b>GSM-148</b>	Correction done in the validation of processes in the Deploy of Device Templates.
<b>GSM-248</b>	Modification done on the message displayed when filling up SD-WAN Profiles without a valid address.
<b>GSM-269</b>	Implementation of multiple options selection in the web filter profile.
<b>GSM-970</b>	Improvement done in the exclusion of UTM/devices bound in the Logger chart.
<b>GSM-1093</b>	Improved the synchrony time of a UTM to the GSM.
<b>GSM-1291</b>	Correction done in the validation of the amount of CPUs when creating multiple SSL profiles.
<b>GSM-1722</b>	Change of the nomenclature "History" in "Analytics".
<b>GSM-1729</b>	Improvements done in the Logger chart update system.
<b>GSM-1768</b>	Improvement done in the application of Device Templates in the UTM's setup.
<b>GSM-1769</b>	Adjustments done in the import of Policy Templates in groups of Policy Packages.
<b>GSM-1771</b>	Correction done in the Deploy of IPv6 Policies, including origin address setup.
<b>GSM-1773</b>	Update done in the import of IPv6 Policy Packages with inspection and IPS Profile.
<b>GSM-1809</b>	Correction done in the specification of the Service field: Proxy.
<b>GSM-1810</b>	Correction done in Device Template naming in SD-WAN Profiles.
<b>GSM-1811</b>	Improvements done in the creation of Device Templates, Policy Packages and Policy Templates.
<b>GSM-1812</b>	Improvements done in the rule and Device Templates, SD-WAN and DPI profiles, and Policy Groups ID cloning process.
<b>GSM-1815</b>	
<b>GSM-1837</b>	
<b>GSM-1846</b>	
<b>GSM-1845</b>	Correction done in the change of Policy Package IPv4 to IPv6.
<b>GSM-1847</b>	Correction done in the change of Policy Templates IPv4 to IPv6.



# Blockbit GSM version 2.0.8

## Release Notes

25/03/2021

Several features and fixes have been implemented, the list below shows the improvements made in the launch of Blockbit GSM 2.0.8:

- Creation of the command "[disable-snmp](#)" allowing the service to be disabled.

The following table lists the improvements made in the release of Blockbit GSM

Code	Description
<b>GSM-747</b>	Correction of the information displayed in the GSM and UTM Analyzer
<b>GSM-1107</b>	Correction in the interfaces after snapshot restoration
<b>GSM-1239</b>	Correction in the display of package names in the deploy panel
<b>GSM-1256</b>	Correction applied to the list of tasks in the deploy panel
<b>GSM-1346</b>	Improvement in the performance of the device creation process in GSM
<b>GSM-1378</b>	Improvement in the performance of the GSM Manager
<b>GSM-1379</b>	Correction applied to the reinsertion of SSH keys when changing or adding Devices
<b>GSM-1401</b>	Improvements applied to synchronization with UTMs
<b>GSM-1474</b>	Corrections applied to reports displayed by the Analyzer
<b>GSM-1486</b>	Improvements in the fields of Loggers configuration forms
<b>GSM-1488</b>	Correction applied in the language displayed in the interface
<b>GSM-1498</b>	Correction in the validation of the fields in the form of general system settings
<b>GSM-1502</b>	Correction applied in the language of the system buttons
<b>GSM-1504</b>	Correction applied to the fields of the System settings form
<b>GSM-1505</b>	Correction applied in the field of service doors
<b>GSM-1515</b>	Layout improvements enabling use as Whitelabel
<b>GSM-1634</b>	
<b>GSM-1624</b>	
<b>GSM-1634</b>	
<b>GSM-1548</b>	Fixes in the deployment of Policy packages
<b>GSM-1550</b>	Corrections applied to synchronization with UTMs 1.5
<b>GSM-1560</b>	Correction in the export of csv reports from the Log session
<b>GSM-1573</b>	Correction applied to CLI command "help"
<b>GSM-1609</b>	Correction applied in the synchronization of IPv4 rules
<b>GSM-1616</b>	Correction in the direction of the links in the Analyzer filters
<b>GSM-1622</b>	Correction in the display of system version in the CLI
<b>GSM-1627</b>	Correction applied to the Setup Wizard settings
<b>GSM-1632</b>	Correction of IPS links in Analyzer

<b>GSM-1640</b>	Correction applied to user exclusion messages from the Administration panel
<b>GSM-1650</b>	Correction in the display of the Web filter reports
<b>GSM-1675</b>	Correction in the display of Security Events reports
<b>GSM-1695</b>	Correction of accepted names when configuring IPS profiles
<b>GSM-1696</b>	Fixes applied when deploying policy templates
<b>GSM-1712</b>	Correction in the log counter of the histories in Security Events
<b>GSM-1713</b>	Correction in disk partitioning of Loggers
<b>GSM-1738</b>	Correction applied to the display of top hits in Events in Analytics
<b>GSM-1746</b>	Correction in the display of the user selection menu in User Behavior in Analyzer
<b>GSM-1749</b>	Correction in the display of the history in Security Events

# Blockbit GSM version 2.0.7

## *Release Notes*

14/12/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit GSM 2.0.7:

Code	Description
<b>GSM-1266</b>	Improvement applied to the characters accepted in the password field in the Devices register
<b>GSM-1269</b>	Correction in scheduling deploys
<b>GSM-1293</b>	Improvements to the Custom branding deployment

# Blockbit GSM version 2.0.6

## *Release Notes*

04/11/2020

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit GSM 2.0.6:

Code	Description
<b>GSM-740</b>	Correction in the creation of policies with a profile of DPI in UTM
<b>GSM-754</b>	Correction in the login of UTMs through the GSM device inventory
<b>GSM-1091</b>	Correction in cloning of Policy Templates and Packages
<b>GSM-1140</b>	Correction applied to the display of devices in the Communities Deploy window
<b>GSM-1189</b>	Correction to the progress bar in Communities Deploy

# Blockbit GSM version 2.0.5

## Release Notes

04/09/2020

- [Brand customization](#) of UTMs linked to GSM, through the deployment of templates;
- [Brand customization](#) also in GSM, applied directly to the product, such as:
  - Product's name;
  - Product icon;
  - Logo (in SVG extension);
  - Background image;
  - Menu colors.
- The Zero Touch Provisioning system has been improved, making it possible to [provision a large number of devices](#) (batch), by importing a CSV file;
- Implementation of the integration of authentication of administrator users with the [LDAP server](#);
- Implementation of the [SNMP service](#) for system monitoring.

Several features and fixes have been implemented, the list below shows the improvements made in the launch of Blockbit GSM 2.0.5:

Code	Description
<b>GSM-751</b>	Correction applied to the ordering of rules in the Zone Protection templates
<b>GSM-753</b>	Correction in the display of the version of the templates in the deploy panel
<b>GSM-868</b>	Correction in the display of the graphical interface when using empty certificate
<b>GSM-872</b>	Correction applied when updating policy packages deploy
<b>GSM-880</b>	Fixed application control application in service templates
<b>GSM-895</b>	Correction in the logger timezone configuration
<b>GSM-925</b>	Correction in ordering the application of policy groups
<b>GSM-926</b>	Correction applied to the display of tags in policies
<b>GSM-932</b>	Correction in the creation of new Zone Protection for UTMs version 2.0.4

# Blockbit GSM version 2.0.4

## Release Notes

22/06/2020

- GSM 2.0.4 allows you to integrate the system with the RADIUS authentication server.

Several features and fixes have been implemented, the list below shows the improvements made in the release of Blockbit GSM 2.0.4:

Code	Description
<b>GSM-61</b>	Correction in the UTM user synchronization with GSM.
<b>GSM-708</b>	Corrections applied in the configurations deploy.
<b>GSM-729</b>	
<b>GSM-743</b>	
<b>GSM-748</b>	
<b>GSM-749</b>	
<b>GSM-752</b>	
<b>GSM-756</b>	
<b>GSM-755</b>	
<b>GSM-730</b>	Correction applied in the "Network" field in Device Community.
<b>GSM-741</b>	Corrections applied to the Zero Touch Provisioning.
<b>GSM-746</b>	
<b>GSM-756</b>	
<b>GSM-742</b>	Correction to the zone protection rules.
<b>GSM-745</b>	Correction in the removal of devices in the inventory panel.
<b>GSM-747</b>	Correction in the integration between UTM and Analyzer.
<b>GSM-759</b>	System integration with RADIUS authentication server.
<b>GSM-783</b>	Correction applied to the CSV file of the log sessions.

# Blockbit GSM version 2.0.2

## New Features

Several features and corrections have been implemented, next, is a summary of the improvements made in the release of Blockbit GSM 2.0.2:

- Improvements and inclusion of services in Device Templates;
- Global Search functionality included on the Application Control profiles;
- Improvements in the policy packages deploy process;
- Improvements in Zero Touch Provisioning functionalities;
- Improvement on the Analyzer reports;
- Corrections applied to Logger-config in standalone mode;
- Backup restore size optimization;
- And more...

# Blockbit GSM version 2.0

## Release Notes

### Features – BLOCKBIT GSM

- New Zero Touch Provisioning service for automatic application of settings;
- Device Manager improvements: Organize your devices by version of "Firmware", geographic region, administrative users, customers or organizational units, providing easier management of the network;
- Role Based Administration: New centralized panel for policy management based on inspection profiles;
- New centralized panel for viewing session logs;
- New centralized panel for exporting and scheduling reports in multiple formats: HTML, PDF, CSV;
- New log summarization and processing service;
- Workflow for Audit and Deployment Control (workflow auditing and deployment control);
- Deploys Panel improvements: Track and manage the installation of the BLOCKBIT GSM configuration packages on managed devices;
- Usability improvements: Compatibility of visual identity and usability between the centralized management application and the local management application;
- Option for administrator to reset password via email.



# Blockbit GSM version 1.2.3

The following table exhibits the improvements made in the release of BLOCKBIT GSM version 1.2.3

Code	Description
<b>GSM-7</b>	Correction in the option to delete selected items.
<b>GSM-10</b>	Correction in the report display on Analyzer.
<b>GSM-12</b>	Correction in the description field in device template.
<b>GSM-14</b>	Correction in the network settings in the general and e-mail tabs.
<b>GSM-18</b>	Improvements in the Analyzer search limit.
<b>GSM-121</b>	Correction in the SD-WAN profile listing.
<b>GSM-125</b>	Correction in Action View on the reports window.
<b>GSM-126</b>	Correction in the migration from GSM 1.1 to 1.2.1.
<b>GSM-127</b>	Improvements to the line limit of Analyzer reports.
<b>GSM-128</b>	Correction in GSM versioning.
<b>GSM-129</b>	Correction applied to device template deploy.
<b>GSM-130</b>	Correction applied on the enable of services when deploying a device template.
<b>GSM-146</b>	Correction applied on the enable of default policy when deploying device template.

# Blockbit GSM version 1.2.1

The following table exhibits the improvements made in the release of BLOCKBIT GSM version 1.2.1

Code	Description
<b>GSM-15</b>	Correction in band control limitation by GSM.
<b>GSM-66</b>	Correction applied in displaying the synchronized UTMs information.
<b>GSM-68</b>	Correction applied to traffic logs in GSM deploy.
<b>GSM-120</b>	Correction applied to the logs creation in CSV format.

# Blockbit GSM version 1.2.0

The following table exhibits the improvements made in the release of BLOCKBIT GSM version 1.2.0

Code	Description
<b>GSM-3109</b>	New feature: Audit and change control tool.
<b>GSM-3127</b>	Task workflow notifications.
<b>GSM-3443</b>	Improvements in the management of Device Communities.
<b>GSM-3468</b>	Improvements in the management of Device Templates.
<b>GSM-3479</b>	Improvements in the management of sevicees.
<b>GSM-3831</b>	Improvements in the upgrade system.
<b>GSM-12064</b>	Improvements in the event navigation with DrillDown.
<b>GSM-12382</b>	Improvements in the management of policies.
<b>GSM-12447</b>	Improvements in the usability of the configuration interfaces.
<b>GSM-12448</b>	Improvements in the usability of the task panel.
	BLOCKBIT GSM supports BLOCKBIT UTM versions 1.4.7 and 1.5.3.

# Blockbit GSM version 1.1.3

The following table exhibits the improvements made in the release of BLOCKBIT GSM version 1.1.3

Code	Description
BB-12233 BB-12244 BB-12245	Improvements made to the API that integrates with BLOCKBIT UTM with support for "Group" synchronisms.
BB-12325	Correction applied to the group registration screen that had errors to display groups.
BB-12360	Correction applied to search in the group screen.
BB-12369	Correction applied to displaying the groups during the filter.
BB-12371	Correction applied to the removal of BLOCKBIT UTM users, automatically updating on BLOCKBIT GSM.
BB-12386	Correction applied to the identification of groups with the same nomenclature coming from different UTMs.

# Blockbit GSM version 1.1.0

The following table exhibits the improvements made in the release of BLOCKBIT GSM version 1.1.0

<b>Security report with statistics in Network Traffic</b> A new security reports view feature with Network Traffic statistics has been implemented.
<b>Security report with statistics in Policy Usage</b> A new security reports view feature with Policy Usage statistics has been implemented.
<b>Analysis report with statistics in Application Usage</b> A new security reports view feature with Application Usage statistics has been implemented.
<b>Security report with statistics in Web Traffic</b> A new security reports view feature with Web Traffic statistics has been implemented.
<b>Security report with Threat Protection statistics</b> A new security reports view feature with statistics in Threat Protection has been implemented.
<b>Security report with statistics in Intrusion Prevention</b> A new security reports view feature with statistics in Intrusion Prevention has been implemented.
<b>Security report with statistics in User Timeline</b> A new security reports view feature with statistics in User Timeline has been implemented.
<b>Log Search</b> A log search tool with advanced search capability has been implemented, enabling the administrator to add filters with any type of field detected automatically in the stored log.
<b>Logger Manager</b> A new tool has been implemented to manage multiple logging devices, enabling the administrator to register, manage and have a global view of all Loggers.
<b>Report Manager</b> A tool has been implemented to generate, manage and export reports. It also allows the administrator to customize the results by adding filters to correlate data.
<b>Commands for Logger management</b> New commands were deployed on the CLI console to manage the Logger storage device.
<b>Service for Loggers Monitor</b> A tool was deployed to monitor the status of the connection of all registered Loggers devices.
<b>Manager Integration with BLOCKBIT UTM 1.4</b> Allows to manage the new BLOCKBIT UTM 1.4 settings.
<b>Validation of conflicting and equivalent rules</b> A new feature to validate conflicting and equivalent rules in the policy package has been implemented.
<b>Centralized distribution of update packages</b> A new feature to coordinate updates for multiple devices managed by GSM BLOCKBIT has been implemented.
<b>Event filter by time</b> Allows to filter by time to search on Events.
<b>Command to reset logs and reports</b> A new command has been implemented on the CLI interface to remove all logs and reports of the system.

# GSM - VIRTUAL APPLIANCE

## Versions

### VMware

### KVM/Proxmox

### Citrix/XenServer

VMware	
Version	CHECKSUM
GSM 2.4.2	87a6cf323ede17940566313f4ed3654a
GSM 2.4.1	00ccff0d29d59af7a15f366775e1a4c9
GSM 2.4.0	d60b3eaa3d4603beaa21de454e4da87c
GSM 2.3.0	bd7dc89f171372cb4b4a4bb5c5d898d2
GSM 2.2.2	cd616e8620131071de87004abe07abc6
GSM 2.2.1	d20d0138dfa4eb6002ac809e4ab72d9b
GSM 2.2.0	3701777a9e73abe90962e94fbacecaa0
GSM 2.1.1	d2f71ea790f34c3258739aaafaf6dd1a
GSM 2.1.0	a48f11fafbb06a48bc00d5ffde0abf59
GSM 2.0.13	b468b8977d4e90be6ac3b8c5756a46c9
GSM 2.0.12	dfaf25858d7115849732ab72348a83f1
GSM 2.0.11	27845ee784019ef7d8c7ae03e582229f
GSM 2.0.10	ed5f013e959a2e0900da62c02763a937
GSM 2.0.9	e09c470f15627a074a496ecf6e36e908
GSM 2.0.8	a96322139a658247b708380157a4443f
GSM 2.0.7	4e1fbcea70bce5aeb7dd9836bbaea729
GSM 2.0.6	592493910248e27ad5edd8b7ab73bdc9
GSM 2.0.5	7e943d35fd995872ebc57a3dc3f78b84
GSM 2.0.4	b6f8a3a75142b11e1c569d3332949770
GSM 2.0.3	bc80248799f9ea2bcc83c8771267852f
GSM 2.0	b867a0e707a71fcc28e9a74cfe350886
GSM 1.2.3	df014b2ef1573af90bdd171c9357ea7f
GSM 1.2.1	fa3577b472359acb8c97c91321ef1f97
GSM 1.1	88280df14573af6ce20537b109114dbe

KVM/Proxmox	
Version	CHECKSUM
GSM 2.4.2	809281f93a2a60378905ba4f7cb240b2
GSM 2.4.1	629a23d052b01a9ed0f8a0e12085fd64
GSM 2.4.0	28aa09d0f83ae539b8cc16c3171402d1
GSM 2.2.2	995809e0a409310195b8061aa6ebcbf0
GSM 2.2.1	db0f28b101487179ee9d3f6e4cab7863
GSM 2.2.0	d090dfc1137b635afca2714ef577cd6e

<a href="#">GSM 2.1.1</a>	7da37bb54ec1d46cd0baad3e60c1bc4f
<a href="#">GSM 2.0.12</a>	97c2b846305862bb5626e9a828307158
<a href="#">GSM 2.0.11</a>	124f88954a830bb16c270f2d05388149
<a href="#">GSM 2.0.10</a>	89bf6e8873418605b732ee5190bec90b

Citrix/XenServer	
Version	CHECKSUM
<a href="#">GSM 2.4.2</a>	87a6cf323ede17940566313f4ed3654a
<a href="#">GSM 2.4.1</a>	00ccff0d29d59af7a15f366775e1a4c9
<a href="#">GSM 2.4.0</a>	d60b3eaa3d4603beaa21de454e4da87c
<a href="#">GSM 2.3.0</a>	bd7dc89f171372cb4b4a4bb5c5d898d2
<a href="#">GSM 2.2.2</a>	cd616e8620131071de87004abe07abc6
<a href="#">GSM 2.2.1</a>	d20d0138dfa4eb6002ac809e4ab72d9b
<a href="#">GSM 2.2.0</a>	3701777a9e73abe90962e94fbacecaa0
<a href="#">GSM 2.1.1</a>	d2f71ea790f34c3258739aaafaf6dd1a

[Back to top](#)

# GSM - INSTALLATION FILES

In this page are available the firmware files for the installation of the Blockbit GSM in physical appliances.

Version	CHECKSUM
<a href="#">GSM 2.4.2</a>	92b29901e008fe3da74d4c2f50fe8502
<a href="#">GSM 2.4.1</a>	e2b3db0fb149bef7d938e2a887e2d6c3
<a href="#">GSM 2.4.0</a>	8315ec2fb46c236138a7d46f2b03104f
<a href="#">GSM 2.3.0</a>	e68afbfc938e938d9907cf71c3ac6a2
<a href="#">GSM 2.2.2</a>	31242c80c68f9bc8157c067b54d984e5
<a href="#">GSM 2.2.1</a>	7adefee66c97b8e56f2efe207d87a4b0
<a href="#">GSM 2.2.0</a>	0a36e4b2c72e1b6e225cb2ffa98bbb82
<a href="#">GSM 2.1.1</a>	e9ff46963393222e435dcc9844e766fd
<a href="#">GSM 2.1.0</a>	dd02a87dca8bb536f6a0dd0ec74bad02
<a href="#">GSM 2.0.13</a>	81e97bf11484f8d190a75d05a106b8a0
<a href="#">GSM 2.0.12</a>	cfb06dd8351c3a0f0939609a275e6b0f
<a href="#">GSM 2.0.11</a>	e3cdfbebb7587c7172e2054f0c68960f
<a href="#">GSM 2.0.10</a>	cddc1af89bacc2daf685d535d291a762
<a href="#">GSM 2.0.9</a>	5d3c773b65b7f0330978e76c7d2d00f7
<a href="#">GSM 2.0.8</a>	fda15dac67d97c849af97df55dc75f4a
<a href="#">GSM 2.0.7</a>	62399bc08034a76838ce54a819847991
<a href="#">GSM 2.0.6</a>	a417a052cfa60e0148aa2162c00278e9
<a href="#">GSM 2.0.5</a>	6e8addcbcdf5e4bca112d6b404a0fd5
<a href="#">GSM 2.0.4</a>	29ea5353fc3fb0a3b0ccb15659be64f6
<a href="#">GSM 2.0</a>	f517753f9603d5bef0a0e3c63b0ed4f2
<a href="#">GSM 1.2.3</a>	b232130d5b0cb1408bfba8b5bb0b681c
<a href="#">GSM 1.2</a>	e4e1a8f87d5dbe1a7b2b4bc5336c38a7
<a href="#">GSM 1.1</a>	fa4da0323641522e250dfe750c83111e



# GSM - How to Upgrade Kernel

In this document we will cover the download and execution process of the kernel update installer on Blockbit GSM.

After reading and applying the steps in this tutorial you will be able to update your Blockbit GSM kernel easily and safely.

## Requirements

It is important to perform the step-by-step mentioned in this guide, since the kernel update will not be performed automatically by GSM.



In addition, we ALWAYS recommend that a system BACKUP of the latest version be performed before any update or upgrade procedure is performed and that the generated file be saved in a safe place. For more information on how to generate a snapshot, see this [page](#).

In this guide, it will be necessary to execute a command to update the kernel manually through the CLI, for that, it will be necessary to have [access to the console](#).



For more information on how to [access via the console](#) or how to [update your product](#), refer to the Blockbit GSM manual.

## Contents

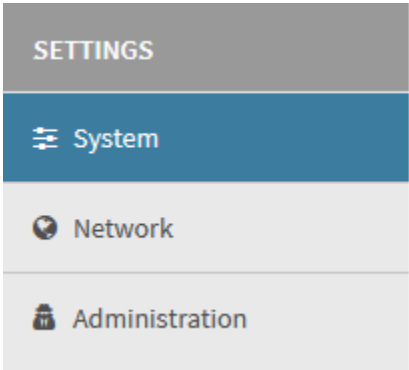
In this how to the following topics will be covered:

- [How to generate a Backup](#);
- [Console Access](#);
- [System Update](#);
- [Performing the kernel update](#);
- [System Reboot](#).

Initially we will analyze how to [generate a Snapshot](#).

# GSM - How to Upgrade Kernel - How to generate a Backup

Initially, log in to the interface, locate the Settings menu in the side menu on the left of the screen and click on the System option.



System option

The following window will be displayed:

System

General

License

Update

Sessions

Services

Download

Upload

Save

Hostname

gsm

Domain

blockbit.com

Timezone

America/Sao\_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)

\* Language

English

System - General



Click on the [Download] option located at the top right of the screen, the following window will be displayed:

System Backup
X

\* Key

\* Confirm Key

Cancel Save

System - General - System Backup

System Backup
X

\* Key

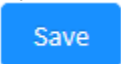
\* Confirm Key

Cancel Save

System Settings – System Backup



To perform the backup, it is necessary to create a secure key. *It must contain at least eight characters with uppercase and lowercase letters, numbers and special characters. Without this key, it is not possible to restore the backup.*

- This screen displays two options: “Key” and “Confirm Key”;
  - Key:** Insert the encryption key that protects the backup;
  - Confirm Key:** Confirm the encryption key;
- Clicking the **Save**  button will display the screen for selecting the location and name of the backup file of Blockbit GSM. Choose your preferred location and folder to save it.

Backup was successful.



**ATTENTION:** Performing this backup is essential to ensure the integrity of your data. After taking the snapshot, store it in a safe place.

After performing the steps previously mentioned, the backup will have been successfully generated.

Next, we'll look at [how to access the console](#).

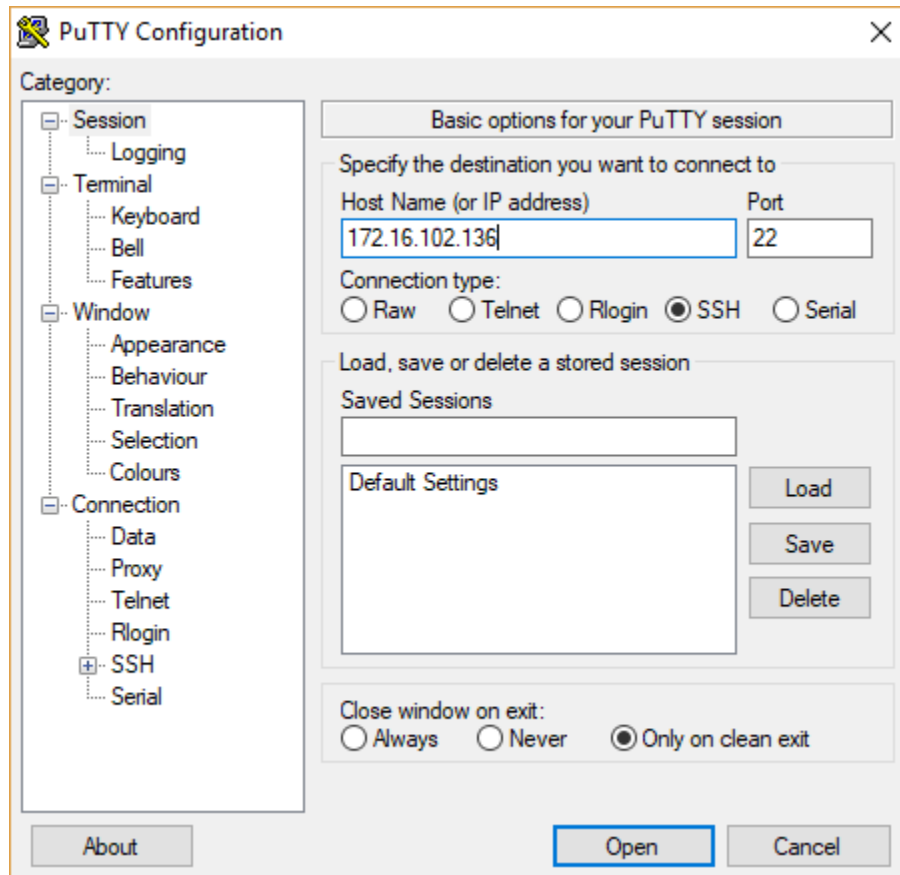
# GSM - How to Upgrade Kernel - Console Access

Blockbit GSM provides a Command Line Interface (CLI) console feature, which allows the administrator to execute administrative and troubleshooting commands for the main system services. To perform the configuration, you need an SSH client and Console. The minimum recommended applications are:

- *PUTTY*;
- *CygWin*;
- *Mobaxterm*.

Below we will present step by step how to access the Blockbit UTM CLI console:

1. Check that the access device has a recommended SSH client already installed. In this case, we will exemplify the process using the "PUTTY" application;
2. Access the SSH console and fill in the fields:
  - **Host Name (or IP Address):** Enter the IP address of the Blockbit UTM. Ex.: 172.16.102.136;



*PuTTY Configuration*

- Click on the "Open" button.

3. The console will be displayed, prompting for a username and password;

In "login as:" type the user "admin" and press "Enter".

The image below shows the commands of the main system services.

```

admin >help
arp                ip                reset-admin-sessions  uptime
arping            ipcalc           reset-logs           vmstat
date              less            restore-logger-backup whois
debug-backup      logger-backup    rewizard
debug-deployer    logger-certificate-sync route
debug-ha          logger-config    sar
debug-rotation    logger-config-sync set-network-dns
debug-sync        logger-connect   set-network-gateway
delete-logger-backup logger-devices-add set-network-hostname
disable-snmp       logger-devices-list set-network-interface
enable-root        logger-disable    set-network-timezone
enable-snmp        logger-enable     show-devices
ethtool           logger-key        show-license
exit              logger-storage    show-logger-backups
fdisk             logger-update-schedule show-uuid
free             lscpu            show-version
fsck             mkfs             shutdown
grep            more            snapshot
ha-failover      netstat         tcpdump
ha-up            ntpdate         tcptop
help            passwd          telnet
history         ping           tracepath
hostname        reboot         traceroute
ifconfig        reset          update-gsm
ifstat          reset-admin-block update-license
iotest          reset-admin-password upgrade-kernel
admin >

```

Blockbit UTM – Command Line Interface



For more information on how to access via the console, refer to this [page](#) of the Blockbit GSM manual.

As a backup of the system settings has already been made (if you have not already done this, see this [page](#)) the next step will be to turn off the [secondary interface](#) and [update the system](#).

# GSM - How to Upgrade Kernel - System Update

Before updating the kernel, it will be necessary to purchase the packages related to UTM 2.0.8, to do so, access the Primary Cluster console and enter the command **[*update-gsm*]**:



**ATTENTION:** We ALWAYS recommend that a FULL BACKUP of the latest system version and reports be made before any update or upgrade procedure is performed and that the files are saved in a safe place.

```

admin >update-gsm
Loaded plugins: fastestmirror
Determining fastest mirrors
gsm-apply-update: running
gsm-apply-update: >/etc/yum.repos.d/BlockBit-centos.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-epel.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-gsm.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-bases.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-elastic.repo
gsm-apply-update: update system packages
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
bases-local | 2.9 kB 00:00:00
centos-local | 2.9 kB 00:00:00
elastic-local | 2.9 kB 00:00:00
epel-local | 2.9 kB 00:00:00
gsm-local | 2.9 kB 00:00:00
(1/15): bases-local/2.0/x86_64/filelists_db | 24 kB 00:00:01
(2/15): bases-local/2.0/x86_64/primary_db | 43 kB 00:00:01
(3/15): bases-local/2.0/x86_64/other_db | 19 kB 00:00:00
(4/15): centos-local/2.0/x86_64/filelists_db | 370 kB 00:00:04
(5/15): elastic-local/2.0/x86_64/primary_db | 13 kB 00:00:01
(6/15): elastic-local/2.0/x86_64/other_db | 1.1 kB 00:00:00
(7/15): centos-local/2.0/x86_64/primary_db | 857 kB 00:00:06
(8/15): centos-local/2.0/x86_64/other_db | 211 kB 00:00:02
(9/15): elastic-local/2.0/x86_64/filelists_db | 202 kB 00:00:02
(10/15): epel-local/2.0/x86_64/primary_db | 6.9 kB 00:00:00
(11/15): epel-local/2.0/x86_64/filelists_db | 2.9 kB 00:00:01
(12/15): epel-local/2.0/x86_64/other_db | 5.1 kB 00:00:00
(13/15): gsm-local/2.0/x86_64/primary_db | 44 kB 00:00:01
(14/15): gsm-local/2.0/x86_64/other_db | 3.3 kB 00:00:00
(15/15): gsm-local/2.0/x86_64/filelists_db | 1.7 MB 00:00:07
Metadata Cache Created
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
--> Package atp-blacklist.x86_64 0:2021021020812-0.el7.centos will be updated
--> Package atp-blacklist.x86_64 0:202102150811-0.el7.centos will be an update
--> Package atp-geopip.x86_64 0:202102150901-0.el7.centos will be updated
--> Package atp-geopip.x86_64 0:202102150901-0.el7.centos will be an update
--> Package atp-threats.x86_64 0:2021021030809-0.el7.centos will be updated
--> Package atp-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package bbos-scripts.x86_64 0:2.0.6-80 will be updated
--> Package bbos-scripts.x86_64 0:2.0.7-69 will be an update
--> Package gsm-apply.x86_64 0:2.0.6-80 will be updated
--> Package gsm-apply.x86_64 0:2.0.7-69 will be an update
--> Package gsm-backend.x86_64 0:2.0.6-80 will be updated
--> Package gsm-backend.x86_64 0:2.0.7-69 will be an update
--> Package gsm-console.x86_64 0:2.0.6-80 will be updated
--> Package gsm-console.x86_64 0:2.0.7-69 will be an update
--> Package gsm-manager.x86_64 0:2.0.6-80 will be updated
--> Package gsm-manager.x86_64 0:2.0.7-69 will be an update
--> Package gsm-repos.x86_64 0:2.0.6-80 will be updated
--> Package gsm-repos.x86_64 0:2.0.7-69 will be an update
--> Package gsm-schema.x86_64 0:2.0.6-80 will be updated
--> Package gsm-schema.x86_64 0:2.0.7-69 will be an update
--> Package ips-threats.x86_64 0:2021021030809-0.el7.centos will be updated
--> Package ips-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package wgs-class.x86_64 0:2021021030809-0.el7.centos will be updated
--> Package wgs-class.x86_64 0:202102120800-0.el7.centos will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
atp-blacklist x86_64 202102150811-0.el7.centos bases-local 1.2 M
atp-geopip x86_64 202102150901-0.el7.centos bases-local 12 M
atp-threats x86_64 202102160809-0.el7.centos bases-local 2.7 M
bbos-scripts x86_64 2.0.7-69 gsm-local 14 k
gsm-apply x86_64 2.0.7-69 gsm-local 43 k
gsm-backend x86_64 2.0.7-69 gsm-local 65 k
gsm-console x86_64 2.0.7-69 gsm-local 29 k
gsm-manager x86_64 2.0.7-69 gsm-local 76 M
gsm-repos x86_64 2.0.7-69 gsm-local 11 k
gsm-schema x86_64 2.0.7-69 gsm-local 25 k
ips-threats x86_64 202102160809-0.el7.centos bases-local 1.4 M
wgs-class x86_64 202102120800-0.el7.centos bases-local 285 M
=====
Transaction Summary
Upgrade 12 Packages

Total download size: 378 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydelta not installed.
warning: /var/cache/yum/x86_64/2.0/bases-local/packages/atp-blacklist-202102150811-0.el7.centos.x86_64.rpm: Header V4 RSA/SHA1 Signature,
key ID b08c6759: NOKEY
Public key for atp-blacklist-202102150811-0.el7.centos.x86_64.rpm is not installed
(1/12): atp-blacklist-202102150811-0.el7.centos.x86_64.rpm | 1.2 MB 00:00:06
Public key for bbos-scripts-2.0.7-69.x86_64.rpm is not installed ] 647 kB/s | 4.0 MB 00:09:52 ETA
(2/12): bbos-scripts-2.0.7-69.x86_64.rpm | 14 kB 00:00:01
(3/12): gsm-apply-2.0.7-69.x86_64.rpm | 43 kB 00:00:01
(4/12): gsm-console-2.0.7-69.x86_64.rpm | 20 kB 00:00:00
(5/12): gsm-backend-2.0.7-69.x86_64.rpm | 65 kB 00:00:01
(6/12): gsm-repos-2.0.7-69.x86_64.rpm | 11 kB 00:00:00
(7/12): gsm-schema-2.0.7-69.x86_64.rpm | 25 kB 00:00:00
(8/12): atp-threats-202102160809-0.el7.centos.x86_64.rpm | 2.7 MB 00:00:05
(9/12): atp-geopip-202102150901-0.el7.centos.x86_64.rpm | 12 MB 00:00:12
(10/12): ips-threats-202102160809-0.el7.centos.x86_64.rpm | 1.4 MB 00:00:03
(11/12): gsm-manager-2.0.7-69.x86_64.rpm | 76 MB 00:00:25
(12/12): wgs-class-202102120800-0.el7.centos.x86_64.rpm | 285 MB 00:01:05
-----
Total 4.9 MB/s | 378 MB 00:01:17
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-BlockBit
Importing GPG key 0xb08c6759:

```

#### Command Line Interface – update-gsm

To confirm that the system has been updated, use the command **[show-version]**.

```

admin >show-version
BLOCKBIT GSM 2.0.8 build 21010423

```



After installing the update previously mentioned, [we will now update your UTM kernel](#).

Before updating the kernel, it will be necessary to purchase the packages related to UTM 2.0.8, to do so, access the Primary Cluster console and enter the command **[update-gsm]**:



**ATTENTION:** We ALWAYS recommend that a FULL BACKUP of the latest system version and reports be made before any update or upgrade procedure is performed and that the files are saved in a safe place.

```

admin >update-gsm
Loaded plugins: fastestmirror
Determining fastest mirrors
gsm-apply-update: running
gsm-apply-update: >/etc/yum.repos.d/BlockBit-centos.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-epel.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-gsm.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-bases.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-elastic.repo
gsm-apply-update: update system packages
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
bases-local | 2.9 kB 00:00:00
centos-local | 2.9 kB 00:00:00
elastic-local | 2.9 kB 00:00:00
epel-local | 2.9 kB 00:00:00
gsm-local | 2.9 kB 00:00:00
(1/15): bases-local/2.0/x86_64/filelists_db | 24 kB 00:00:01
(2/15): bases-local/2.0/x86_64/primary_db | 43 kB 00:00:01
(3/15): bases-local/2.0/x86_64/other_db | 19 kB 00:00:00
(4/15): centos-local/2.0/x86_64/filelists_db | 370 kB 00:00:04
(5/15): elastic-local/2.0/x86_64/primary_db | 13 kB 00:00:01
(6/15): elastic-local/2.0/x86_64/other_db | 1.1 kB 00:00:00
(7/15): centos-local/2.0/x86_64/primary_db | 857 kB 00:00:06
(8/15): centos-local/2.0/x86_64/other_db | 211 kB 00:00:02
(9/15): elastic-local/2.0/x86_64/filelists_db | 202 kB 00:00:02
(10/15): epel-local/2.0/x86_64/primary_db | 6.9 kB 00:00:00
(11/15): epel-local/2.0/x86_64/filelists_db | 2.9 kB 00:00:01
(12/15): epel-local/2.0/x86_64/other_db | 5.1 kB 00:00:00
(13/15): gsm-local/2.0/x86_64/primary_db | 44 kB 00:00:01
(14/15): gsm-local/2.0/x86_64/other_db | 3.3 kB 00:00:00
(15/15): gsm-local/2.0/x86_64/filelists_db | 1.7 MB 00:00:07
Metadata Cache Created
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
--> Package atp-blacklist.x86_64 0:2020110208012-0.el7.centos will be updated
--> Package atp-blacklist.x86_64 0:202102150811-0.el7.centos will be an update
--> Package atp-geopip.x86_64 0:202011020901-0.el7.centos will be updated
--> Package atp-geopip.x86_64 0:202102150901-0.el7.centos will be an update
--> Package atp-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package atp-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package bbos-scripts.x86_64 0:2.0.6-80 will be updated
--> Package bbos-scripts.x86_64 0:2.0.7-69 will be an update
--> Package gsm-apply.x86_64 0:2.0.6-80 will be updated
--> Package gsm-apply.x86_64 0:2.0.7-69 will be an update
--> Package gsm-backend.x86_64 0:2.0.6-80 will be updated
--> Package gsm-backend.x86_64 0:2.0.7-69 will be an update
--> Package gsm-console.x86_64 0:2.0.6-80 will be updated
--> Package gsm-console.x86_64 0:2.0.7-69 will be an update
--> Package gsm-manager.x86_64 0:2.0.6-80 will be updated
--> Package gsm-manager.x86_64 0:2.0.7-69 will be an update
--> Package gsm-repos.x86_64 0:2.0.6-80 will be updated
--> Package gsm-repos.x86_64 0:2.0.7-69 will be an update
--> Package gsm-schema.x86_64 0:2.0.6-80 will be updated
--> Package gsm-schema.x86_64 0:2.0.7-69 will be an update
--> Package ips-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package ips-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package wgs-class.x86_64 0:202010300800-0.el7.centos will be updated
--> Package wgs-class.x86_64 0:202102120800-0.el7.centos will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
atp-blacklist x86_64 202102150811-0.el7.centos bases-local 1.2 M
atp-geopip x86_64 202102150901-0.el7.centos bases-local 12 M
atp-threats x86_64 202102160809-0.el7.centos bases-local 2.7 M
bbos-scripts x86_64 2.0.7-69 gsm-local 14 k
gsm-apply x86_64 2.0.7-69 gsm-local 43 k
gsm-backend x86_64 2.0.7-69 gsm-local 65 k
gsm-console x86_64 2.0.7-69 gsm-local 29 k
gsm-manager x86_64 2.0.7-69 gsm-local 76 M
gsm-repos x86_64 2.0.7-69 gsm-local 11 k
gsm-schema x86_64 2.0.7-69 gsm-local 25 k
ips-threats x86_64 202102160809-0.el7.centos bases-local 1.4 M
wgs-class x86_64 202102120800-0.el7.centos bases-local 285 M
=====
Transaction Summary
Upgrade 12 Packages

Total download size: 378 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydelta not installed.
warning: /var/cache/yum/x86_64/2.0/bases-local/packages/atp-blacklist-202102150811-0.el7.centos.x86_64.rpm: Header V4 RSA/SHA1 Signature,
key ID b08c6759: NOKEY
Public key for atp-blacklist-202102150811-0.el7.centos.x86_64.rpm is not installed
(1/12): atp-blacklist-202102150811-0.el7.centos.x86_64.rpm | 1.2 MB 00:00:06
Public key for bbos-scripts-2.0.7-69.x86_64.rpm is not installed ] 647 kB/s | 4.0 MB 00:09:52 ETA
(2/12): bbos-scripts-2.0.7-69.x86_64.rpm | 14 kB 00:00:01
(3/12): gsm-apply-2.0.7-69.x86_64.rpm | 43 kB 00:00:01
(4/12): gsm-console-2.0.7-69.x86_64.rpm | 20 kB 00:00:00
(5/12): gsm-backend-2.0.7-69.x86_64.rpm | 65 kB 00:00:01
(6/12): gsm-repos-2.0.7-69.x86_64.rpm | 11 kB 00:00:00
(7/12): gsm-schema-2.0.7-69.x86_64.rpm | 25 kB 00:00:00
(8/12): atp-threats-202102160809-0.el7.centos.x86_64.rpm | 2.7 MB 00:00:05
(9/12): atp-geopip-202102150901-0.el7.centos.x86_64.rpm | 12 MB 00:00:12
(10/12): ips-threats-202102160809-0.el7.centos.x86_64.rpm | 1.4 MB 00:00:03
(11/12): gsm-manager-2.0.7-69.x86_64.rpm | 76 MB 00:00:25
(12/12): wgs-class-202102120800-0.el7.centos.x86_64.rpm | 285 MB 00:01:05
-----
Total 4.9 MB/s | 378 MB 00:01:17
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-BlockBit
Importing GPG key 0xb08c6759:

```

#### Command Line Interface – update-gsm

To confirm that the system has been updated, use the command **[show-version]**.

```

admin >show-version
BLOCKBIT GSM 2.0.8 build 21010423

```

After installing the update previously mentioned, we will now [update your UTM kernel](#).

# GSM - How to Upgrade Kernel - Performing the Kernel Upgrade

Access the GSM console to enter the system, in this step we will upgrade the system to the most current version, this step will also install the Kernel.



**ATTENTION:** It is worth emphasizing again that it is recommended to ALWAYS do a FULL BACKUP of the latest version of the system and the reports before executing any update or upgrade procedure and that the files are saved in a safe place..



Note that the upgrade process interferes with the interfaces configured in standalone loggers. For more information about the upgrade-blockbit command, see this [page](#).



**ATTENTION:** At the end of the execution of this command, it will be necessary to restart your UTM.



To avoid interruptions due to a network outage, it is suggested that the upgrade process be done directly through the appliance's console.

In the CLI of the Primary Cluster run the command **[upgrade-blockbit]** as shown below.

```
admin >upgrade-blockbit
NOTE:
Upgrade process must NOT be Interrupted!
After ending upgrade process, system will be restart automatically

Are you sure do you want upgrade version 2.0 to 2.1 (restart system is required)? [y/N]y
During the update process, logger service will be unavaible, are you sure about continuing? [y/N]y
Have you made a full system backup? [y/N]y

Testing connection to update server:
Connection succeeded

will restart when the upgrade is complete
Upgrading...

- No SSL mode enabled
- Downloading packages

- No SSL mode enabled
- Downloading packages
warning: /var/cache/yum/x86_64/2.1/bases-local/packages/atp-blacklist-202102150811-0.el7.centos.x86_64.rpm: Header V4 RSA/SHA1 Signature,
key ID b08c6759: NOKEY
Importing GPG key 0xb08c6759:
Userid   : "ONMEV3064BITS (Development and Support) <infosuporte@brc.com.br>"
Fingerprint: 1796 7f4b ed4a db4f f3a2 669f 49f9 044b b08c 6759
Package   : gsm-repos-2.0.8-114.x86_64 (@gsm/7)
From      : /etc/pki/rpm-gpg/RPM-GPG-KEY-BlockBit
NOTE:
Kernel Upgrade process must NOT be Interrupted!

Checking for license...
Checking for available upgrade...
Downloading kernel upgrade...
##### 100.0%
Kernel upgrade downloaded
Kernel upgrade downloaded. Installing...
Checking environment...
Preparing environment...
Environment ok.
Testing installer integrity...
Installer integrity ok.
Unpacking installer...
Installer unpacked.
Running installer...
Finding installation disk...
Mounting installation disk...
Installing new kernel files. It will take a while...
Installing new initramfs...
Setting new kernel as bootable...
Cleaning up old entries...
New kernel installed!
Kernel upgraded from 3.10.0-957.10.1 to 5.8.8-1
A reboot is required!
Rebooting in 60 seconds
Connection to 172.31.170.14 closed by remote host.
Connection to 172.31.170.14 closed.
```

Command Line Interface – upgrade-blockbit

When the installation is finished, the kernel update will have already been carried out successfully, however just as the command itself displays on the screen, it will be necessary to restart the system.

After the machine boots, check that the kernel has been updated to version 5.8 and the system has been updated to version 2.1;

To check the system version, run the command [**show-version**]:

```
admin >show-version
BLOCKBIT GSM 2.1.0 build 21021709
admin >|
```

*Command Line Interface – show-version*

When the installation is finished, the kernel update will have already been carried out successfully, however just as the command itself displays on the screen, it will be necessary to [restart the system](#).

# GSM - How to Upgrade Kernel - Resetting the GSM

Finally, to complete the upgrade, run the **[reboot]** command to reboot the system.

```
blockbit >reboot
PolicyKit daemon disconnected from the bus.
We are no longer a registered authentication agent.
Connection to 172.16.102.137 closed by remote host.
Connection to 172.16.102.137 closed.

[2017-09-12 12:08.23] ~
[maderno.SPLT7BMM2K2] > █
```

*Command Line Interface – reboot*

After the system reboots, the kernel update will have been successfully completed and the Blockbit GSM will be ready for normal use.



**ATTENTION:** If the device loses connection during the Kernel upgrade process or if there is another type of failure, run the **[upgrade-blockbit]** command again.

This concludes the installation of the Kernel, for more in-depth information about the system features, access the [Blockbit GSM administrator's guide](#).

# GSM - REVISIONS' HISTORY

## Document Version Control

DATE	DESCRIPTION OF THE CHANGES
01/06/2017	Initial Release.
17/10/2018	Addition of content and revision.
22/02/2019	Update to the GSM 1.2.1 version.
17/01/2020	Update to the GSM 2.0 version.
22/06/2020	Update to the GSM 2.0.4 version.
04/09/2020	Update to the GSM 2.0.5 version.
04/11/2020	Update to the GSM 2.0.6 version.
14/12/2020	Update to the GSM 2.0.7 version.
14/12/2020	Update to the GSM 2.0.8 version.
17/05/2021	Update to the GSM 2.0.9 version.
23/08/2021	Update to the GSM 2.0.10 version.
24/08/2021	Update to the GSM 2.0.11 version.
30/05/2022	Update to the GSM 2.0.12 version.
02/08/2022	Update to the GSM 2.0.13 version.
25/03/2021	Update to the GSM 2.1.0 version.
23/08/2021	Update to the GSM 2.1.1 version.
22/09/2021	Update to the GSM 2.2.0 version.
30/05/2022	Update to the GSM 2.2.1 version.
02/08/2022	Update to the GSM 2.2.2 version.
31/10/2022	Update to the GSM 2.3.0 version.
27/02/2023	Update to the GSM 2.4.0 version.

# GSM - INTRODUCTION

Thank you for choosing Blockbit GSM.

This Administrator's Guide provides instructions on how to install, configure, and use Blockbit GSM. Once you reach the end of this Guide, you will be able to use all the features and resources of Blockbit GSM.

Global Security Management has been developed to manage multiple solutions for Blockbit. Through it, you can manage Device Profiles, Inventory Management and Automation, Monitoring and many other solutions. This will be detailed further in this document.

The benefits your company will have by using Blockbit GSM are various: Time savings, reduction of costs, reduction of configuration errors, standardization of security policies and consequently a drastic reduction of threats and cyber-attacks, one of its biggest advantages: It's because it does not restrict the number of managed devices. For a better understanding, here's an example: Assuming you are a network administrator of 1,000 stores and you need to block access to a particular social network domain for each store, without Blockbit GSM it will be necessary to configure each store's Firewall to perform the lock. However, with Blockbit GSM it is possible to lock all stores at the same time, just make the proper configuration on Blockbit GSM and perform deploy to all stores, simple, fast and effective.

In addition, Blockbit GSM provides greater control to the administrator by allowing the installation of loggers, which enables a holistic view of the network and its users through widgets, graphs, events, and reporting.

Blockbit GSM delivers complete flexibility, standardization and protection for your business through a simplified, fast, easy-to-configure and uncomplicated platform, giving the network administrator a complete view of your business's security management. Blockbit GSM meet the needs of small, medium and large companies.



# Resources – Blockbit GSM

- **Device Grouping:** This feature provides the possibility to group devices according to your needs, which causes considerable ease in the process of installing the configurations;
- **Role Based Administration:** Its main idea is to enable the control of several users, monitor their permissions for devices and granularity;
- **Device Template-based Configuration:** Templates are a set of general Blockbit UTM device configurations, consisting of System, Authentication, Firewall, Web Cache, Web Filter, Antimalware, IPS, ATP, Traffic Shaping, SD-WAN, and DNS, so you can initialize the devices using the global settings quickly, practically and without errors, reducing TCO (total cost of ownership), maximizing IT staff performance and avoiding any possible configuration errors;
- **Centralized User Management:** This feature provides the administrator with the ability to design policies based on authenticated users and groups;
- **Policy Template-based Management:** Enables the creation of policies and policy groups to control device access protected networks, quickly, easily, and without error;
- **Workflow for Audit and Deployment Control:** Blockbit GSM was developed with change management in mind, and all configurations are forwarded for approval to a previously selected auditor, allowing: Receiving and registering installation requests for configuration packages, evaluating the implications, costs, benefits and risks of proposed changes, justify and approve changes and scheduling of facilities;
- **VPN Community Management:** Build VPN communities - Virtual Private Network on Blockbit GSM. These settings allow secure, fast and encrypted communication between devices.

Blockbit GSM was developed through an Architecture based on ease of use and understanding, to minimize errors and give a complete view of management to the system administrators.

## Features – Blockbit GSM

- **Policy Manager:** In just one configuration interface, easily group security policies by the device, organizational unit, threat types, or controls. It is possible to integrate several resources into a single policy, such as WEB Category, Application Control, Bandwidth Control, Multiple Services, QoS - Quality of Service, Time and Traffic Quota, Link Selection and Redundancy, and Virus and Malware Control;
- **Policy Template:** Enables the creation of groups of policies allowing the reuse of other groups already created on the Policy Manager screen, gaining agility and practicality;
- **Device Manager:** Organize your devices by "Firmware" version, geographic region, administrative users, clients or organizational units, facilitating network management;
- **Device Communities:** Set VPN scopes settings and security parameters and easily distribute between devices;
- **Device Templates:** Define global system settings in a global way among Device Templates;
- **Deploys Panel:** Track and manage the installations of the [Blockbit](#) GSM configuration packages on the managed devices.

# Environment check for Blockbit GSM Installation

To perform Blockbit GSM installation its necessary to familiarize with Blockbit solutions, this guide is primarily intended to provide you with information about setting up and managing Blockbit GSM.

Before proceeding with the installation, check the installation requirements.

Remember that we offer full support through our partners and service channels, who will be delighted to assist you.

# Installation requirements

Ensure that communication with the internet is active, as the licensing, system upgrade and database processes require an internet connection.

## Minimum requirements for installing Manager:

- **Processing:** Quad Core (BB 1000);
- **Memory:** 16 GB RAM;
- **Storage:** 128GB;
- **Virtualization platform:** VMware, XenServer or KVM.

## Minimum requirements for installing Remote Analyzer:

- **Processing:** Octa Core (BB 1000);
- **Memory:** 32GB RAM;
- **Storage 1:** 128 GB;
- **Storage 2:** 256 GB (desirable Raid w / SSD or SAS disks);
- **Virtualization platform:** VMware, XenServer or KVM.

## Minimum requirements for installing the GSM + Internal Analyzer:

- **Processing:** Octa Core (BB 2000);
- **Memory:** 32GB RAM (evaluate increase as per project);
- **Storage 1:** 128 GB;
- **Storage 2:** 256 GB (desirable Raid w / SSD or SAS disks);
- **Virtualization platform:** VMware, XenServer, KVM or *ProxMox*.
- **Public cloud platforms:** *AWS*, *Azure*, *Oracle*, *Google* and *IBM*.

To perform the installation and configuration you need an SSH client, serial console, and a web browser. Here are the recommended minimum applications:

## Web Browser:

- Mozilla Firefox version 45;
- Google Chrome version 51;
- Microsoft Internet Explorer 9.

## Remote Access (SSH and Console):

- PUTTY;
- CygWin;
- Mobaxterm.


# About this Administrator Guide

This Guide has been developed especially for your administrator. All sections have been structured to make the installation process easy and fast. The whole step by step is presented with examples, making it easier to understand and clarify doubts.

Throughout the guide, you can find some icons followed by text. They are intended to alert you to an important note or note about that section.

Let's learn more about these icons:

- **Alert:** Indicates notes or instructions that you should be followed with extra attention during the Blockbit GSM installation process:

Example of a alert message.

Alert


- **CLI - Command Line Interface:** Also known as Shell, refers to the commands that must be entered, next to this symbol will be the command to be entered:

**Command Line**

Example of a command line.


CLI – Command Line Interface

- **Tip:** Refers to suggestions that make the Blockbit GSM installation process easier.

Example of a hint message.

Tip

- **Note:** Refers to notes or notes that are intended to assist the Blockbit GSM installation process:

Example of a note message.

Note

- **Information:** Refers to additional information regarding Blockbit GSM:

Example of an information message.

Information

# ARCHITECTURE – BLOCKBIT GSM

This section will introduce the Blockbit GSM Architecture.

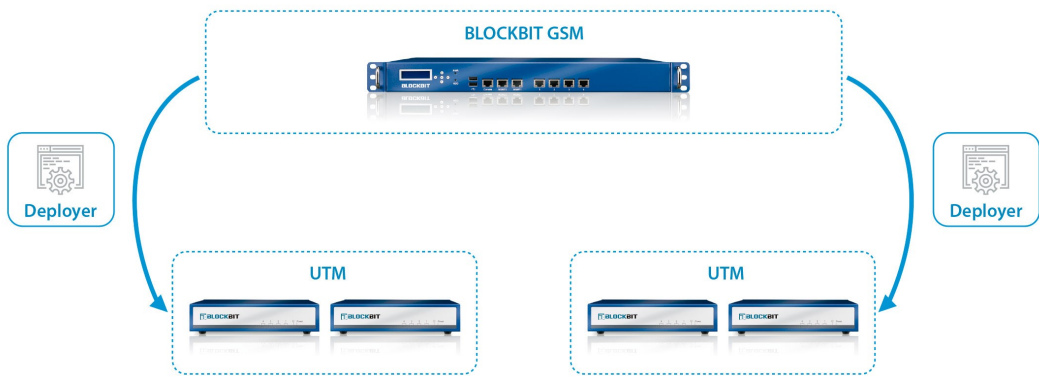
Architecture is presented by a set of layers of components that integrated, define the technical aspects of the services offered by the system.

## Platform

To understand Architecture, you need to understand the purpose of Blockbit GSM and how the devices communicate.

Blockbit GSM (Global Security Management) is designed to manage multiple Blockbit solutions. When connecting a Blockbit UTM device to the Blockbit GSM, creates a secure Tunnel is established using encrypted communication, allowing the application of the generated configurations.

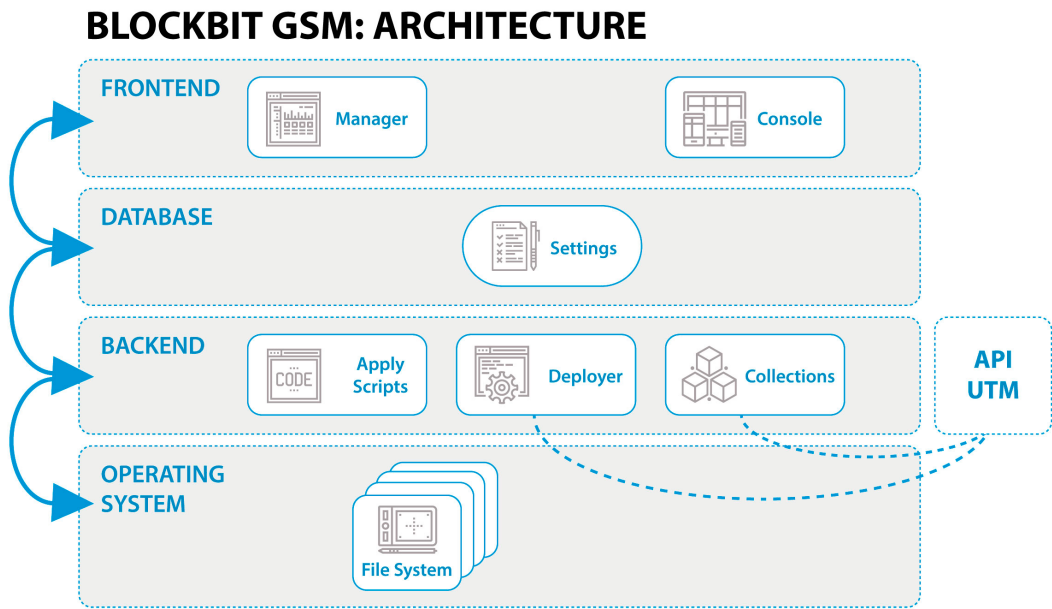
All settings applied through Blockbit GSM are generated in file packages and are exported and implemented in Blockbit UTM.



Architecture – Blockbit GSM platform

## Architecture

The architecture of Blockbit GSM has been developed so that the system simplifies the centralized management of devices.



Blockbit GSM – Architecture.

The architecture is divided into the following component:

- Frontend;
- Backend;
- Data storage;
- Operational system.

More details about these components will be shown below:

## Architecture – Frontend

The frontend is the development layer that provides the web interface and system controls. With Frontend capabilities, you can access any kind of information and execute configuration commands on the GSM Blockbit services.

Frontend layer interfaces ensure that the end user does not have direct access to the other components available in other layers of the System Architecture.

The system is designed to offer two types of interface in the Frontend: Manager and Console layer:

- **Manager:** This is a Web application for device administration. It is through it that the administrator defines all the system configuration parameters and manages the configuration packages that will be installed on the remote devices;
- **Console:** Console: Administrative command line interface used for troubleshooting on the Blockbit GSM device. This Frontend interface can be accessed through an SSH terminal connection.

## Architecture – Backend

The backend is the development layer that provides the commands and programs that apply the settings requested through the Frontend interfaces to centralized management services and the Operating System.

Due to the system's modular feature using services that are independent of each other, information between the Frontend and Backend features is carried through two encrypted and key-authenticated paths: Database or SSH Connection.

- **ApplyScripts:** The main function of AppleScript is to read the configuration parameters stored in the database and rewrite these settings in the services and operating system;
- **Deployer:** This is the service responsible for installing the configuration packages generated through the Manager on the remote devices. Deployer is a Backend application that uses the public API implemented in [Blockbit UTM](#);
- **Collectors:** These are Backend services that use the [Blockbit UTM API](#) to synchronize device information. Information such as License, Users, Network Cards, etc.

## Data Storage

The data warehouse layer is the middle tier that provides the capabilities for storing and transferring information between the Frontend and Backend components. It is through the database system that Frontend writes system settings and parameters to be applied to the Backend and Operating System components.

## Operating System

The [Blockbit GSM Operating System](#) is also maintained by the [Blockbit](#) research and development team, where the open source tools packages used to implement the services are available.

To simplify compatibility with the Appliances and ensure a good performance in the execution of the services, [Blockbit GSM](#) runs on a Linux Kernel Operating System based on Intel x86 Architecture.

# INSTALLATION – BLOCKBIT GSM

This section will introduce the step-by-step installation of the [Blockbit](#) GSM.

Blockbit GSM is only available in Virtual Machines compatible with the following solutions: VMware, XenServer and KVM.

To install Blockbit GSM follow the guidelines below.

- [Importing Virtual Machine](#);
- [Start the Virtual Machine – First Access](#).



# GSM - Importing Virtual Machine

Download the Open Virtual Appliance (OVA) from Blockbit UTM, which can be requested through the Trial registration at our website: <http://www.blockbit.com>.

We will demonstrate the installation using VMware ESXi 6.5.0 software as an example:

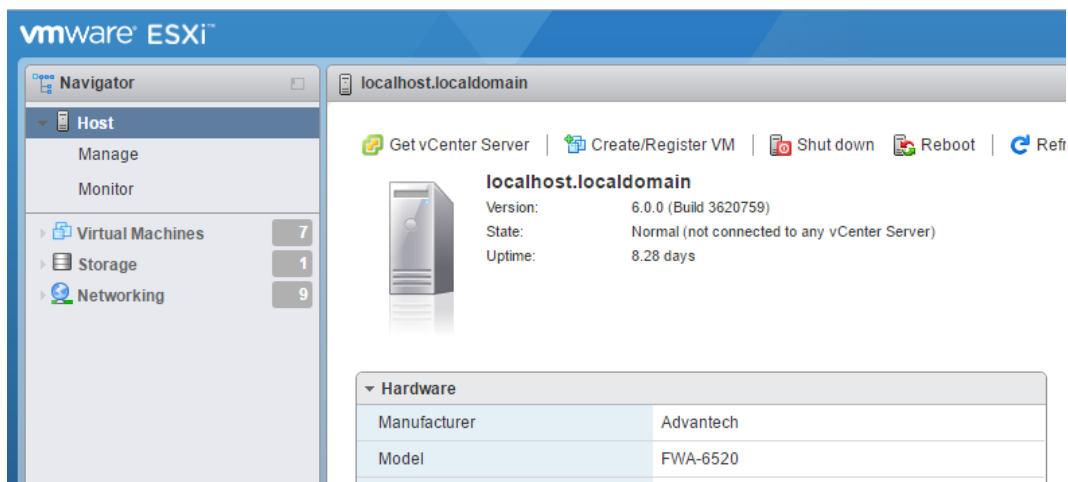
1. Connect to the Internet, using the browser of your choice, and access the VMware ESXi management console on the VMware Host Client;
2. Fill in the fields with the following information:
  - **User name:** User registered in VMware;
  - **Password:** User password;



*Login VMware.*

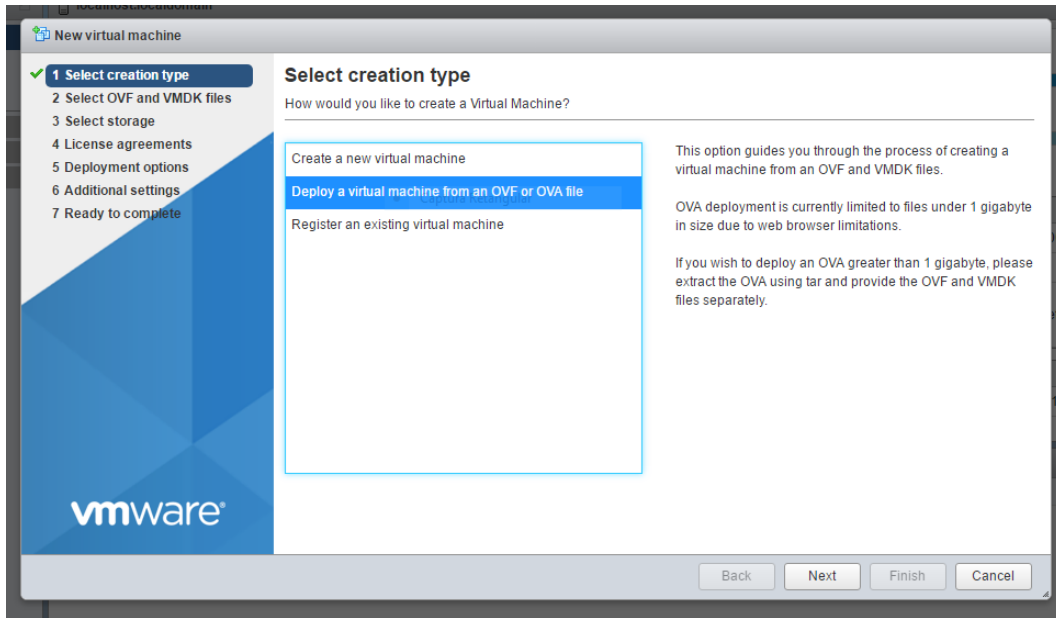
- Click on **“Log in”**.

3. Click on **“Create/Register VM”**;



*Console VMware.*

4. Select the option "Deploy a virtual machine from an OVF or OVA file";

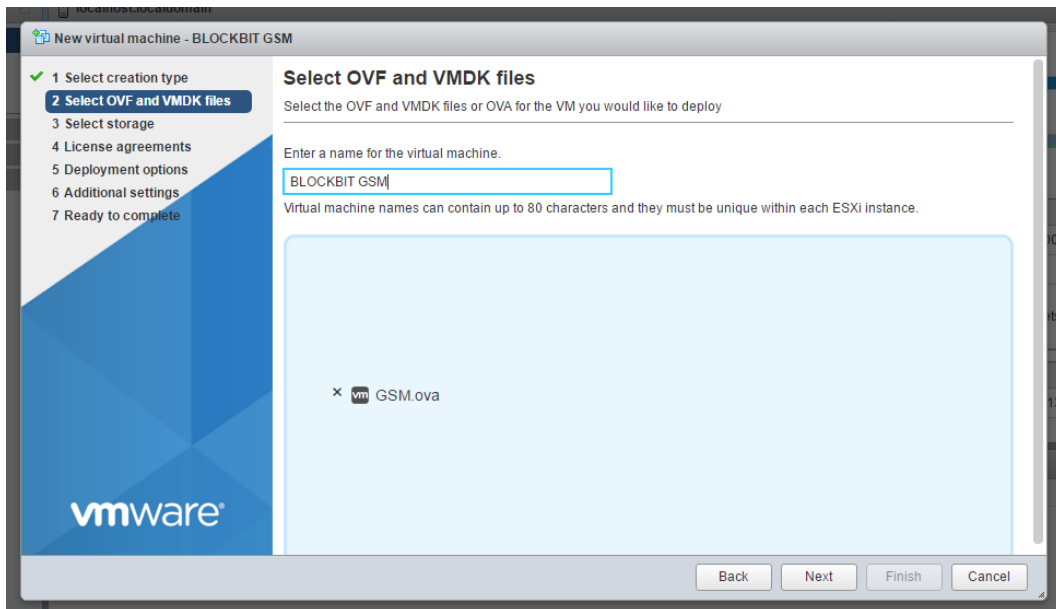


*Select creation type.*

Click on "Next".

5. Select the Blockbit UTM image you have download at our website. Fill in the following field:

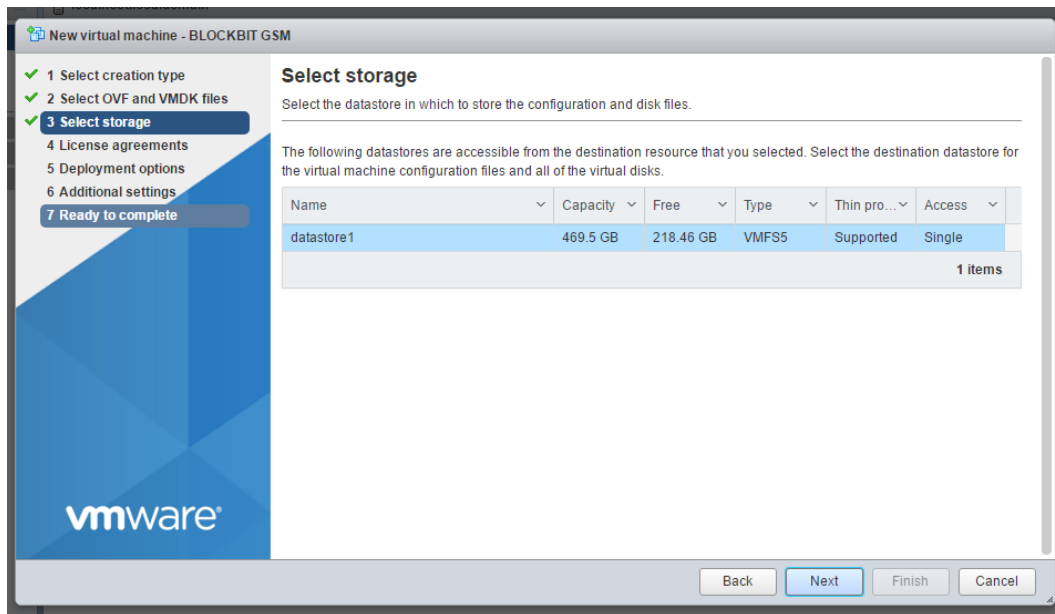
- **Enter a name for the virtual machine:** Enter the machine's name. E.g.: Blockbit GSM;



*Select OVF and VMDK files.*

- Click on "Next".

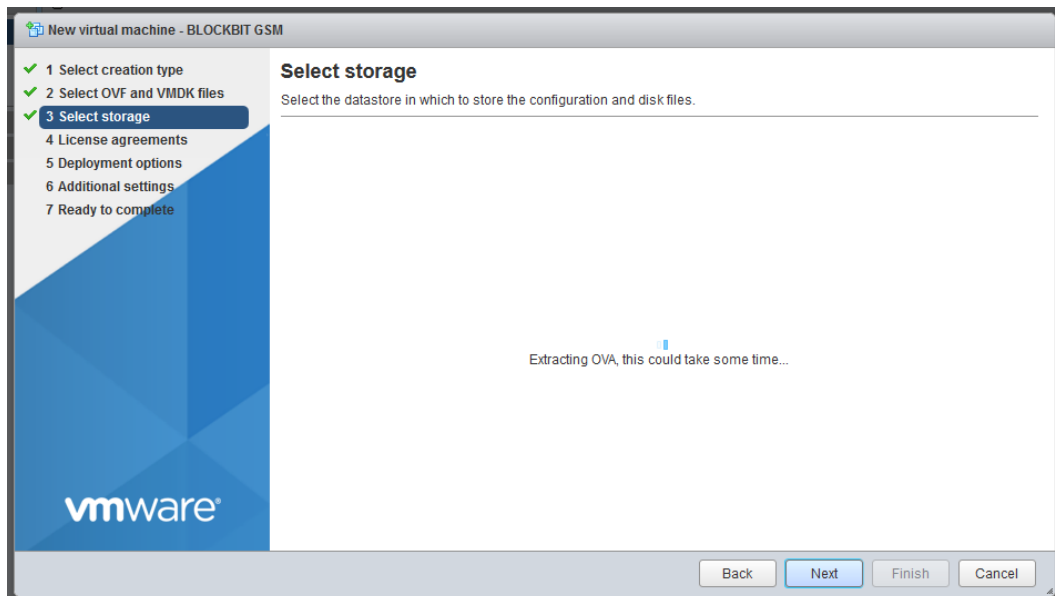
6. Select the datastore in which to store the configuration and disk files. E.g.: datastore1



Select Storage.

Click on "Next";

7. Wait until the OVA is completely uploaded. During this process, the following message will be displayed: "Extracting OVA, this could take some time...";



Select storage – "Extracting OVA, this could take some time..."

8. Set the virtual machine configuration:

- **Network mappings:** select a suitable network mode for your environment. : Bridged mode;
- **Disk provisioning:** select the option of your choice. Ex.: Thin;

- **Thick Disk:** a type of discs fully allocated in the data store, i.e., if you create a Thick disk with 20GB, it will occupy 20GB of your data store;
- **Thin Disk:** a type of disk that allocates only the space that is written by the operating system of the virtual machine. For instance, if you create a 20GB disk for a VM, it will initially occupy only a few KB / MB in the data store, however, by the time you start writing data to it through the operating system, its size can reach up to limit of 20GB.

For more information, see the VMware manual. In this example, we will use the disk provisioning type "Thin".

The screenshot shows the 'New virtual machine - BLOCKBIT GSM' wizard. On the left, a progress bar indicates five steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options (current step), and 5 Ready to complete. The main area is titled 'Deployment options' with the subtitle 'Select deployment options'. It contains two sections: 'Network mappings' with a dropdown menu set to 'bridged' and a sub-dropdown set to 'Filial'; and 'Disk provisioning' with two radio buttons, 'Thin' (selected) and 'Thick'. At the bottom right, there are four buttons: 'Back', 'Next' (highlighted in blue), 'Finish', and 'Cancel'.

*Deployment options*

Click on "Next".

9. Review these setting before finishing the upload wizard;

The screenshot shows the 'New virtual machine - BLOCKBIT GSM' wizard at the 'Ready to complete' step. The progress bar on the left now highlights step 5. The main area is titled 'Ready to complete' with the subtitle 'Review your settings selection before finishing the wizard'. It contains a table summarizing the settings:

Product	Unknown
VM Name	BLOCKBIT GSM
Disks	GSM.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	bridged: Filial
Guest OS Name	Unknown

Below the table, there is a yellow warning icon and the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right, there are four buttons: 'Back', 'Next', 'Finish' (highlighted in blue), and 'Cancel'.

*Ready to complete.*

Clique no botão "*Finish*".

The import has completed, just click on the "Power on" Button to start the virtual machine and proceed to install the Blockbit GSM.

# Start the Virtual Machine – First Access

When you start the virtual machine for the first time, the following screen will be displayed:

```
BLOCKBIT GSM 1.2
.
..
...
Setting up swapspace version 1, size = 1653756 KiB
LABEL=accessdenied, UUID=cb7ff9b7-aa40-4cf9-b643-5b4266a529e3
Command successful.
Command successful.
Command successful.

Install system. Wait!
_351MiB 0:00:46 [4.52MiB/s] [=====] 1 60% ETA 0:00:30
```

Starting Blockbit GSM for the first time

There is no need to perform any steps, just wait until the login screen is displayed.

```
BLOCKBIT GSM 1.2
564D1EAE-F92D-BCF0-22EE-4C6EBDCAC608

localhost login: _
```

Login screen - Blockbit GSM

You will now need to configure IP. To configure IP, perform the following steps:

1. **Localhost login:** Log in via the CLI console, using the default credentials, as follows: User "admin" and password "admin";
2. Change **Blockbit** GSM IP address.



*The default IP address of **Blockbit** GSM is 192.168.1.1. In this guide, we will use the IP address 172.16.102.235 as an example. If you want to change, follow the steps below:*

Configuration details:

**IP:** 172.16.102.235 **Mask:** 255.255.254.0

**Default route:** 172.16.102.1

Enter the following commands:

```
ifconfig eth0 172.16.102.235/23 up
route add default gw 172.16.102.1 dev eth0
```

After performing this procedure, the IP address has changed.

To ensure greater security to the environment we will carry out the change of the default password procedure.



*It is highly recommended to change the default password of the console "admin" user. To change the default password, you must create a strong password. This password must contain at least 8 characters with letters uppercase and lowercase letters, numbers, and special characters.*

To change the password, enter the following command:

```
Type in the command "passwd" and press "Enter".  
Type in the current password and press "Enter".  
Type in the new password twice.
```

By completing this process, the password will be updated.

# CONFIGURING THE EXCEPTION

This section will present how to perform the exception configuration in the web browsers: Google Chrome, Mozilla Firefox and Microsoft Internet Explorer.

When performing the first access to the Blockbit GSM Web Interface, it is normal for browsers to display a security alert stating a certificate error. This is because the browser does not recognize any certification authority that validates access to this page as trusted. Therefore, it is necessary to perform the exception configuration in the web browser. Follow the steps below:

1. To access the web interface, use a recommended browser;
2. Connect to the internet browser and access the address: <https://192.168.1.1>. If you have changed the IP address, use the changed IP.



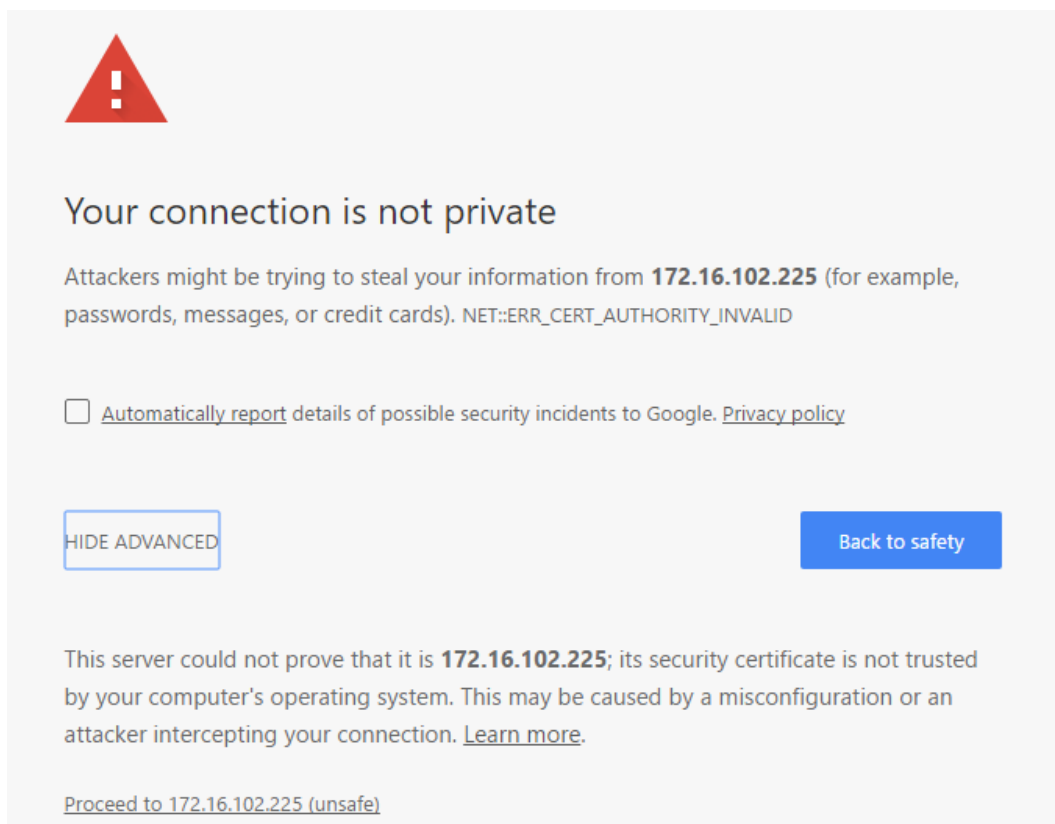
In case the Browser issues a **SECURITY ALERT**, follow the recommendations below.

Each Browser has its procedure to add a connection to the exception list to be recognized as trusted. The guidelines on how to perform this procedure are as follow.

## Google Chrome exception configuration

To configure Google Chrome exception follow the steps below:

1. Click on "Hide Advanced";
2. Click on the "Proceed to 172.16.13.202 (unsafe)" button to accept this page as trusted.



Chrome Exception – "Proceed to 172.16.32.212 (unsafe)"

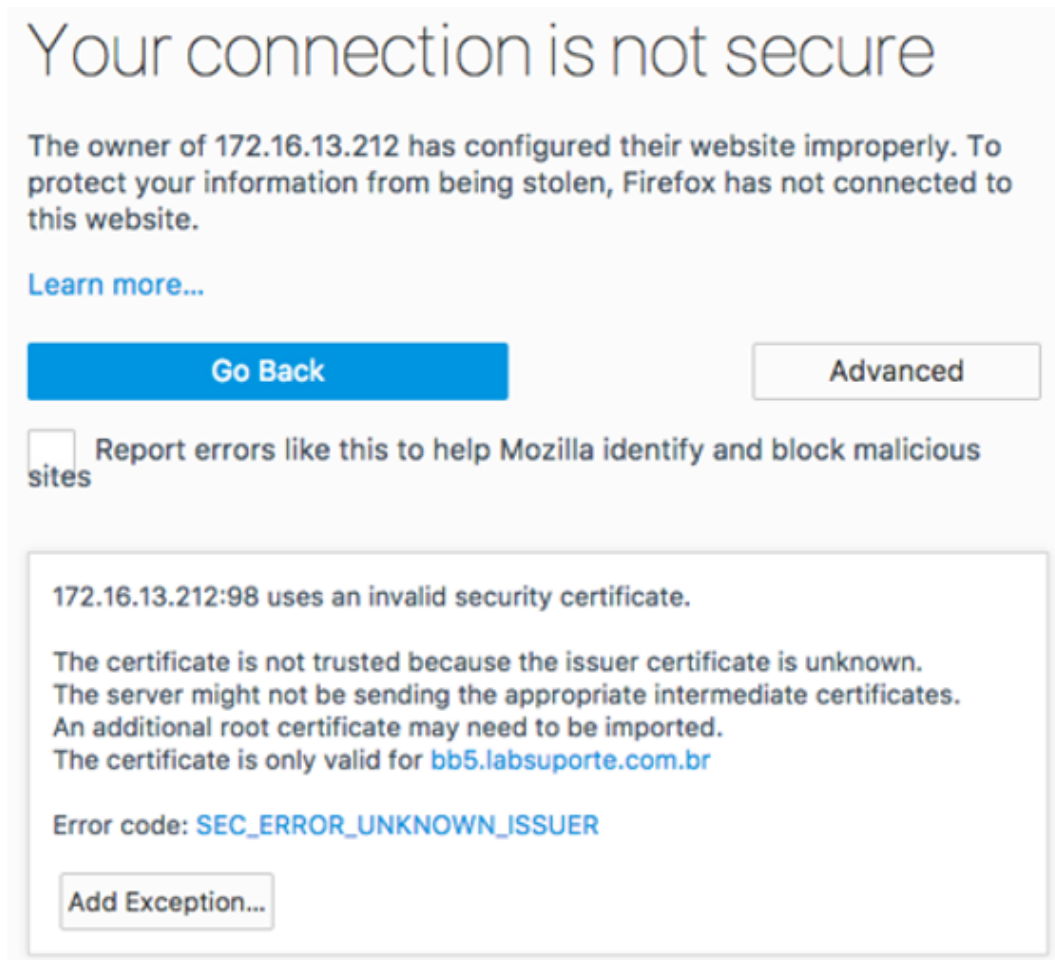
Google Chrome exception configuration has been performed successfully.

## Mozilla Firefox exception configuration

To configure the exception in Mozilla Firefox, follow these steps:

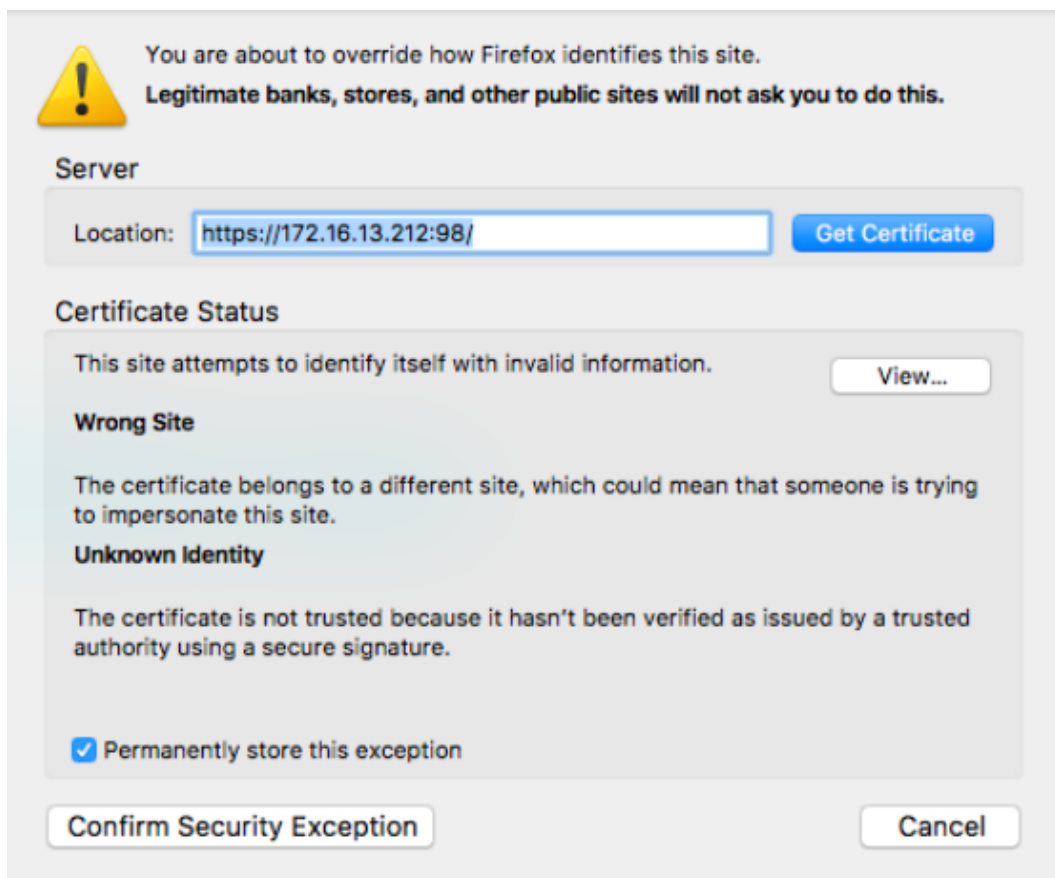


1. Click on "Advanced";
2. Click on "Add Exception...";



Mozilla Firefox Exception – Your connection is not secure

3. Click on "Confirm Security Exception".



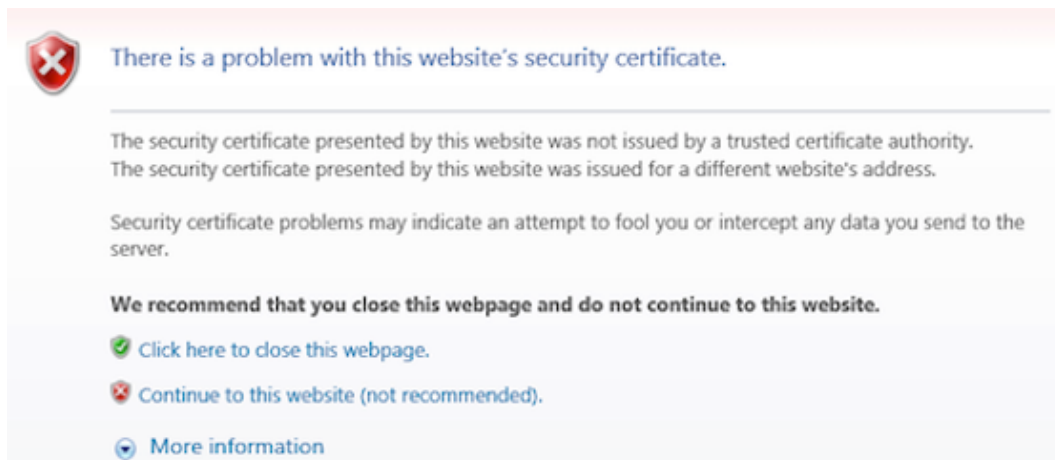
Mozilla Firefox Exception – Confirm Security Exception

Mozilla Firefox exception configuration has been performed successfully.

## Microsoft Internet Explorer exception configuration

To configure Microsoft Internet Explorer, follow the steps below:

1. Click on "Continue to this web site (not recommended)".



Microsoft Internet Explorer Exception – There is a problem with this website's security certificate.

Microsoft Internet Explorer exception configuration has been performed successfully.

# GSM - INSTALLATION WIZARD

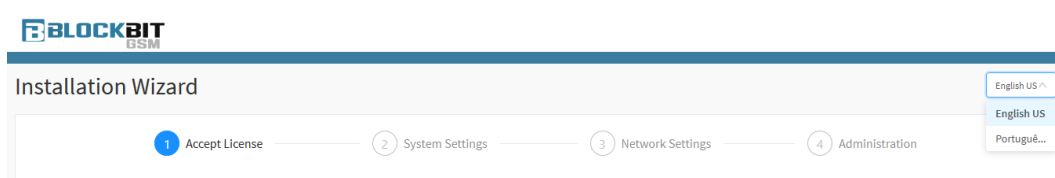
This section will guide you on how to configure the Blockbit GSM Installation Wizard.

To perform the installation of the Installation Wizard, four steps are required: Accept License, System Settings, Network Settings, and Administration. Follow the guidelines below.

## Language Selection

You can select the language of your choice (English US or Portuguese BR). The default language is "English US". To change the language, follow the steps below:

1. Click on the upper right corner "English US" and choose the desired language;



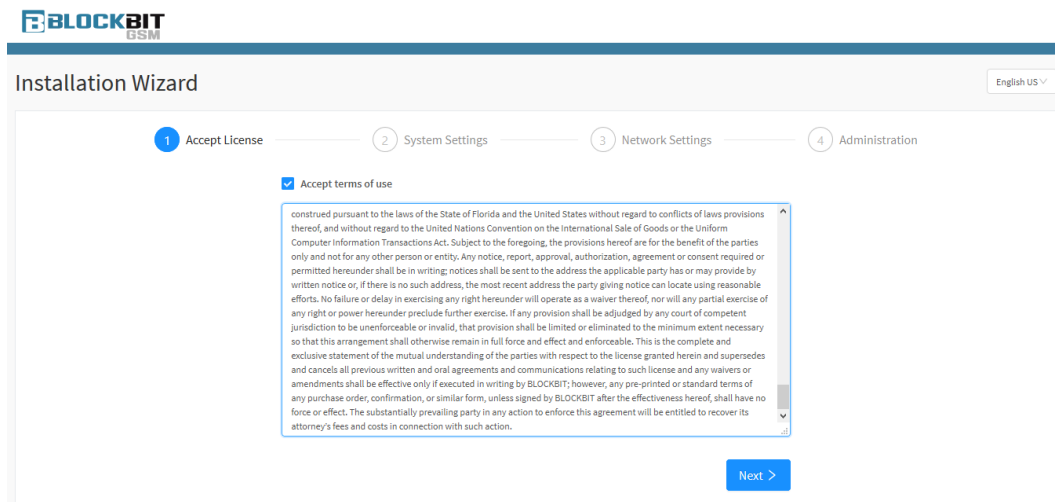
Installation Wizard – Language Selection

When you set the language, your interface will be updated with the chosen language.

## Installation process

The following is an step by step example of the wizard installation:

1. **Accept License:** Displays the terms of use of Blockbit GSM. Read the term and select the checkbox: "Accept terms of use";



Installation Wizard – Accept License.

Next >

Click the Next[ ] button.

2. **System Settings:** Fill in the fields with the following information:

- **Hostname:** Enter the hostname according to the FQDN - Fully Qualified Domain Name. E.g.: GSM;
- **Domain:** Network domain. E.g.: [blockbit.com](http://blockbit.com);
- **Timezone:** Select the timezone in which your company is located. E.g.: America/Sao\_Paulo;
- **Language:** Select the default language. E.g.: English.

The screenshot shows the 'Installation Wizard' interface for BlockBit GSM. The title bar includes the 'BLOCKBIT GSM' logo and a language dropdown set to 'English US'. The wizard has four steps: 1. Accept License, 2. System Settings (current), 3. Network Settings, and 4. Administration. The 'System Settings' section contains four fields: 'Hostname' (text input with 'GSM'), 'Domain' (text input with 'blockbit.com'), 'Timezone' (dropdown menu with 'America/Sao\_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)'), and 'Language' (dropdown menu with 'English US'). At the bottom right are '< Previous' and 'Next >' buttons.

*Installation Wizard – System Settings.*

- Click the **Next**  button to proceed or **Previous**  to return to the previous menu.

3. **Network Settings:** Fill in and set the following fields:

- **Interface:** Select the network interface you wish to configure. E.g.: eth0;
- **IP Address:** Set the appropriate IP address for your network. E.g.: 172.16.102.235;
- **Netmask:** Set the network mask. E.g.: 255.255.254.0;
- **Gateway:** Set default network route. E.g.: 176.16.102.1;
- **DNS Server 1:** Set the primary network or internet DNS server. E.g.: 176.16.102.161;
- **DNS Server 2:** Set the secondary network or internet DNS server. E.g.: Google Secondary DNS 8.8.4.4;
- **NTP Server 1:** Set the primary Network Time Protocol. E.g.: [a.ntp.br](http://a.ntp.br);
- **NTP Server 2:** Set the secondary Network Time Protocol. E.g.: [b.ntp.br](http://b.ntp.br).

**BLOCKBIT** GSM

## Installation Wizard

English US ▼

1 Accept License — 2 System Settings — **3 Network Settings** — 4 Administration

\* **Interface**  
eth0

\* **IP Address**  
172.16.102.235

\* **Netmask**  
255.255.0.0

\* **Gateway**  
176.16.102.1

\* **DNS Server**  
172.31.102.184

**DNS Server**  
8.8.4.4

\* **NTP Server**  
a.ntp.br

**NTP Server**  
b.ntp.br

< Previous   Next >

*Installation Wizard – Network Settings.*



It is imperative that Blockbit GSM and Blockbit UTM be synchronized by the same NTP server.


Next >

< Previous

- Click the **Next** button to proceed or **Previous** to return to the previous menu.

#### 4. Administration: Fill in the following field information:

- Name:** Enter the administrator's name. E.g.: admin;
- Email:** Enter the administrator's email. This email will be used as login on Blockbit GSM. E.g.: [admin@blockbit.com](mailto:admin@blockbit.com);
- Password:** Enter a password that is at least eight characters long. The password must contain uppercase, lowercase letters, and special characters;
- Confirm Password:** Confirm the password provided in the previous step.



## Installation Wizard

English US ▾

✓ Accept License — ✓ System Settings — ✓ Network Settings — 4 Administration

\* Name

\* E-mail

\* Password



\* Confirm Password

[< Previous](#) [Save](#)

Installation Wizard – Administration



The administrator's email will be used as the login for Blockbit GSM.

- Click the **Save**  button to finalize the procedure or in **Previous**  to return to the previous menu.

Once the steps above are finished the installation has been completed successfully.

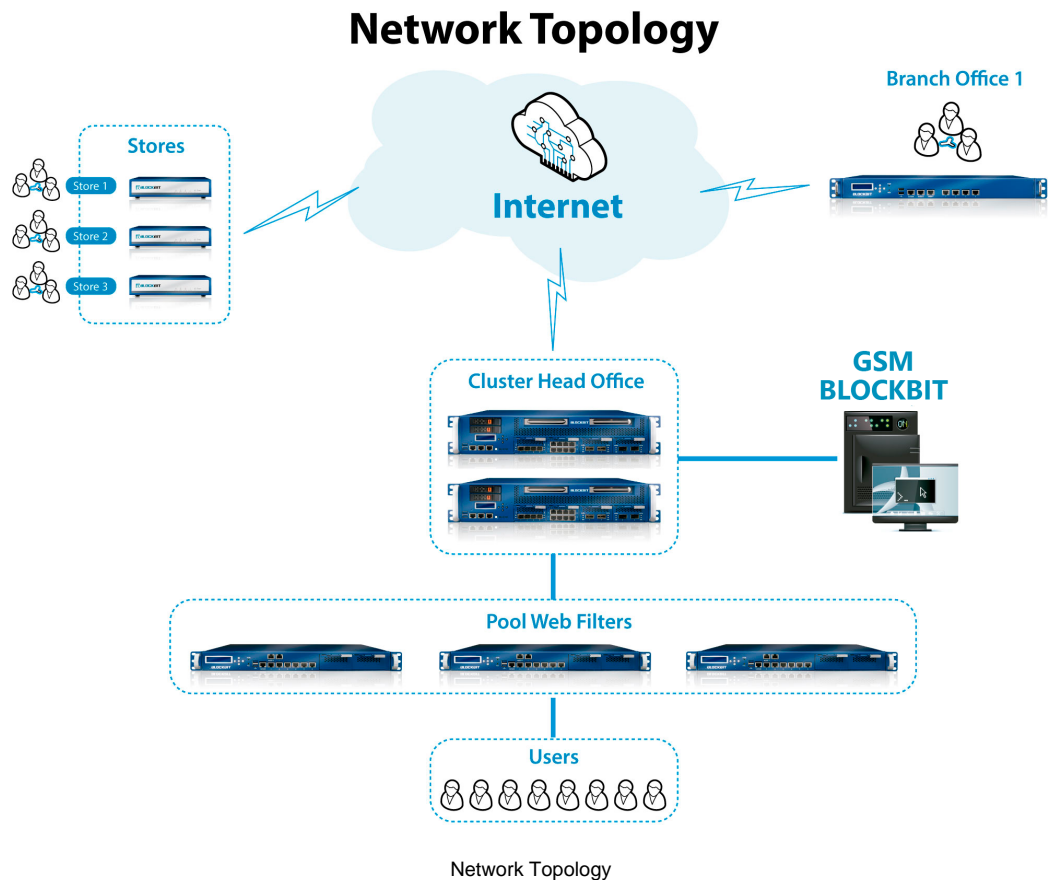
# GSM - NETWORK ENVIRONMENTS

This section will display an example network environment using GSM Blockbit.

To better contextualize this Administrator's Guide, we will use a fictitious topology, but very common among the likely environments that must implement the Blockbit GSM.

Blockbit GSM focuses on environments with many capillarities, that is, large environments remotely connected, but with similarities between remote points, thus reducing the Total Cost of Ownership (TCO) of managing the solution and maximizing ROI - Return on Investment from the company.

The network topology below is a suggested deployment of Blockbit solutions for the Blockbit UTM and Blockbit GSM products:



In this example we will be using the following IP address table:

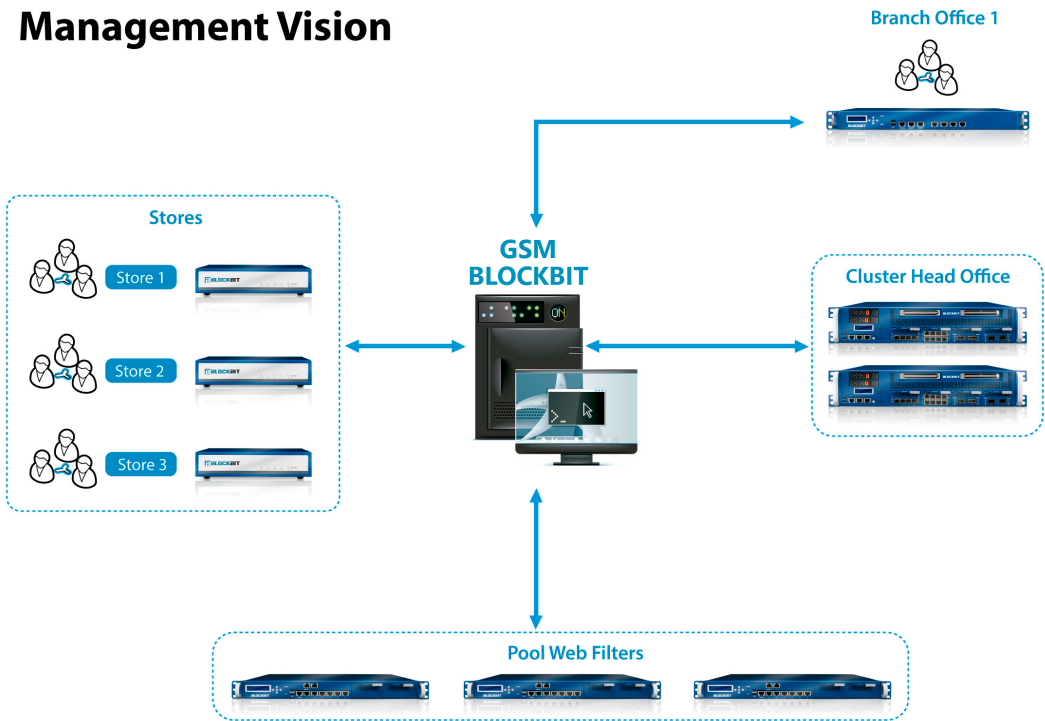
IP addressing

Name	External IP Address	Internal/protected network	Blockbit GSM group
Cluster Head Office	172.16.102.220	192.168.220.0/24	Head Office
Branch Office	172.16.102.221	192.168.221.0/24	Branch Office
Store 1	172.16.102.222	192.168.222.0/24	Stores
Store 2	172.16.102.223	192.168.223.0/24	Stores
Store 3	172.16.102.224	192.168.224.0/24	Stores
Webfilter 1	172.16.102.225	192.168.220.0/24	Pool Web Filters
Webfilter 2	172.16.102.226	192.168.220.0/24	Pool Web Filters
Webfilter 3	172.16.102.227	192.168.220.0/24	Pool Web Filters



In the following image we have the management view with focus on Blockbit GSM, in which it communicates with all Blockbit UTM devices, which are grouped in 4 groups: Head Office, Branch Office, Pool Web Filters and Stores.

## Management Vision



Management Vision

With this grouping, you can apply the customized settings and policies for each of the groups according to your needs.

# GSM - NOTIFICATIONS VIA SNMP

GSM has the ability to configure the system for sending notifications by SNMP trap. Unlike an SNMP data collection service, a "Trap" is a notification service initiated by the monitored server, this initiates the communication and delivery of alerts to the remote SNMP server. The service supports communication with the SNMP v1, SNMP v2 and SNMP v3 protocols.

In GSM, the SNMP configuration is all done through the console command [\[enable-snmp\]](#).

Below we will detail a little about the differences between the versions of the SNMP protocol.

- **SNMP v1**

The first version of SNMP has an extremely fragile authentication scheme, its only security mechanism being "community names". These represent a management group with specific permissions, that is, the assignment of the rights to use the SET and GET instructions on a given parameter to members of this community. The storage of these names is local, that is, each agent that implements SNMP must register the permissions given to each management community that can make use of its parameters.

It is important to note that permissions are given to a particular community, not specific management stations, in fact, there is no listing of members of a community.

The "authentication" of an NMS "Network Management Station" is done through the declaration, sent in text format, of the name of the community to which it belongs. The NMS, therefore, must maintain a list of the relevant community names for each agent in the network. To simplify the management task, there is a tendency to maintain a certain uniformity in the management groups registered in the various entities of the network, but this is not mandatory.

The main flaw of this security model lies in the fact that anyone who knows the community name with the appropriate privileges can send an SNMP command over the network. To make matters worse, as there is no privacy in SNMPv1, information about community names is sent in text form and without encryption in UDP messages that travel over the network, it is extremely simple for an attacker to intercept these names and relate them to stations which are destined.

Given this total insecurity generated by the combination of the lack of privacy with the simple and decentralized authentication model, almost all implementations of this version of SNMP in production systems disable the SET instruction, and restrict the parameters accessible by the GET instructions to non-confidential information. This attitude greatly limits the functionality of the protocol, but at the same time guarantees security in environments where it is essential.

- **SNMP v2**

Originally, a reform of the SNMP security model was part of the goals in creating the second version of the protocol. SNMPv2 (RFC 1901, 1996) emerged to address some of the shortcomings of SNMPv1.

Added at least two new functions:

- *Get-bulk-request*: Access to large blocks of information in MIBs;
- *Inform-request*: Allows a manager to send relevant information directly to other managers;
- Among the novelties of SNMPv2, we highlight:
  - Management of decentralized networks, allowing the existence of more than one management station and, consequently, the exchange of information between them;
  - Possibility of transferring large blocks of information;
  - Introduction of 64-bit counters, enabling better monitoring of variables that reach their limits quickly with 32-bit counters;
  - *Improvement in error handling of variables, defining the status of success or error of the operation for each variable of the PDU and no longer for the PDU*. Thus, if one variable contains an error, the others will not be sacrificed, and the variable field in which the problem occurred is filled with an error code.

The final version of the protocol that was standardized was version 2c, which despite introducing new features such as the "GetBulkRequest" instruction, did not make any changes to the protocol's security model and the model based on community names remained.

- **SNMP v3**

This version of the protocol had as its main focus the improvement of security offered by previous versions of the SNMP protocol. Mechanisms have been developed to deal with each of the security flaws discussed so far. In this way, it became possible to use the full potential of the protocol, including the SET instructions, without compromising the security of the network. The new security model guarantees confidentiality, integrity, authentication and access control.

Generally speaking, the effective PDU that carries the SNMP instruction (either SNMPv1 or SNMPv2) is encapsulated in an SNMPv3 PDU. Esta operação provê as funções relacionadas à segurança no nível de processamento de mensagens. For this communication to be effective, both the management station and the agents must be using the same SNMP engine.

The two main modules of the SNMPv3 security model are the User-based Security Model (USM) and the View-based Access Control Model (VACM). The USM is in charge of authenticating, encrypting and decrypting SNMP packets, while the VACM is in charge of managing access to data in MIBs.

To send notifications via SNMP Trap, access the panel shown below and configure according to the fields of the interface and configuration parameters of the remote SNMP server and the version of the protocol in use.

For more information about the configuration, visit the [\[enable-snmp\]](#) page where the console command is further detailed.

For more information on Zabbix, click [here](#).

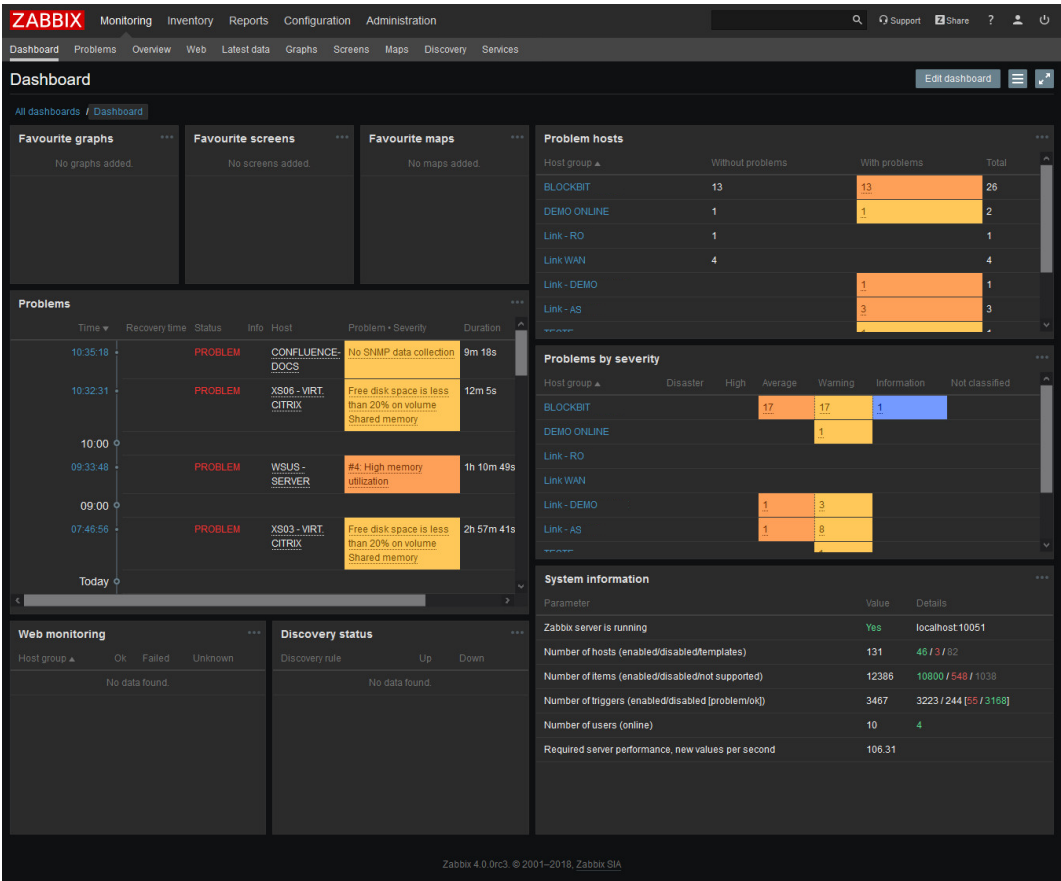
# GSM - Zabbix

Zabbix is an open source monitoring system that allows real-time monitoring of network resources. It allows you to determine thresholds to trigger events, which in addition to enabling the creation of a base of customized alerts by the user, facilitates the visualization and monitoring of the network infrastructure through the use of graphs and diagrams that are built in real time, enabling including the creation of customized graphics joining several items in a single diagram.

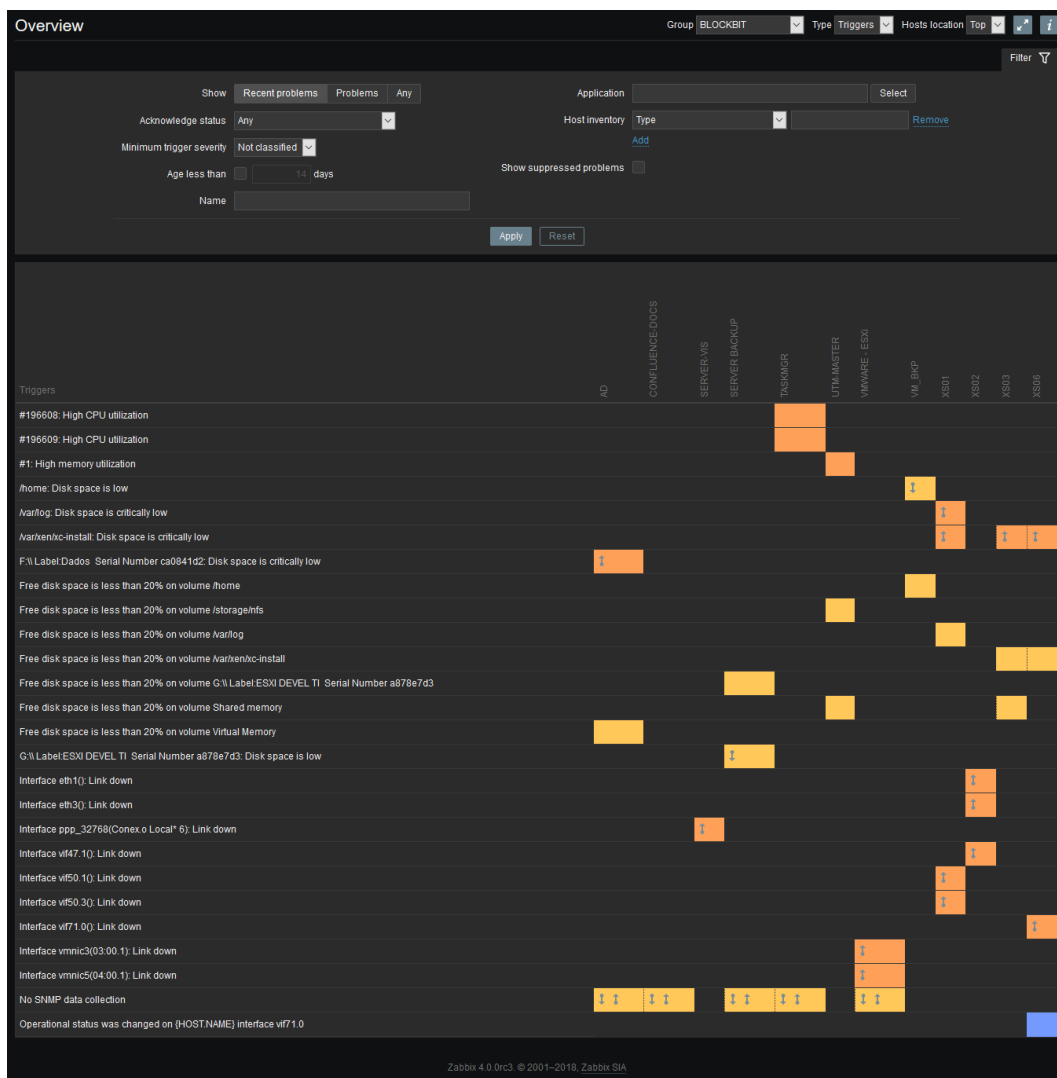
The system works by collecting data from monitored devices at configured intervals through proxy agents or the server and monitors the network infrastructure, running availability and performance tests, using the triggers determined by the user and comparing the results with the system's backend database.

Zabbix contains a very extensive range of graphical visualization generating high-level reports, history, network maps and various types of monitoring graphs created in real time based on the settings created by the user, in addition to allowing the inclusion of customized diagrams of according to the specific demands of the user's infrastructure.

Below, some examples of the resources available in Zabbix:



Zabbix - Dashboard



Zabbix - Overview

ZABBIXMonitoringInventoryReportsConfigurationAdministration

DashboardProblemsOverviewWebLatest dataGraphsScreensMapsDiscoveryServices

Screens

All screens / GSM VIOLA

From: now-1hTo: nowApply

Last 2 daysYesterdayTodayLast 5 minutesLast 7 daysDay before yesterdayToday so farLast 15 minutesLast 30 daysThis day last weekThis weekLast 30 minutesLast 3 monthsPrevious weekThis week so farLast 1 hourLast 6 monthsPrevious monthThis monthLast 3 hoursLast 1 yearPrevious yearThis month so farLast 6 hoursLast 2 yearsThis year so farLast 12 hoursLast 1 day

GSM VIOLA: Disk space usage /var

GSM VIOLA: #1: Used memory

5.9 GB5.8 GB5.7 GB5.6 GB5.5 GB

07-01 09:5610:0010:0510:1010:1510:2010:2510:3010:3510:4010:4510:5007-01 10:56

#1: Used memory [all] last: 5.86 GB min: 5.59 GB avg: 5.73 GB max: 5.86 GB

Host issues

Host	Issue	Last change	Age	Info	Ack	Actions
GSM VIOLA	Free disk space is less than 20% on volume Shared memory	2020-06-30 21:01:23	13h 54m 46s	No		

1 of 1 problem is shown Updated: 10:56:09

Host info

0 Available0 Not available1 Unknown1 Total

Group: TESTE Updated: 10:56:09

History of events

Time	Recovery time	Host	Description	Value	Severity
2020-07-01 10:52:31		XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	PROBLEM	Warning
2020-07-01 10:50:46		XS03 - VIRT. CITRIX	#1: High memory utilization	PROBLEM	Average
2020-07-01 10:35:18		CONFLUENCE-DOCS	No SNMP data collection	PROBLEM	Warning
2020-07-01 10:32:31	2020-07-01 10:51:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 10:29:46	2020-07-01 10:38:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 10:08:46	2020-07-01 10:17:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 09:59:31	2020-07-01 10:30:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 09:50:46	2020-07-01 09:56:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 09:33:48	2020-07-01 10:51:48	WSUS - SERVER	#4: High memory utilization	RESOLVED	Average
2020-07-01 09:29:46	2020-07-01 09:35:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 09:18:48	2020-07-01 09:21:48	WSUS - SERVER	#4: High memory utilization	RESOLVED	Average
2020-07-01 09:17:31	2020-07-01 09:58:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 09:14:31	2020-07-01 09:16:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 09:12:48	2020-07-01 09:15:48	WSUS - SERVER	#4: High memory utilization	RESOLVED	Average
2020-07-01 09:08:46	2020-07-01 09:14:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 09:07:31	2020-07-01 09:12:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 09:00:31	2020-07-01 09:06:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:58:31	2020-07-01 08:59:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:52:31	2020-07-01 08:54:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:47:31	2020-07-01 08:51:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:45:48	2020-07-01 09:09:48	WSUS - SERVER	#4: High memory utilization	RESOLVED	Average
2020-07-01 08:45:31	2020-07-01 08:46:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:41:46	2020-07-01 08:53:46	XS03 - VIRT. CITRIX	#1: High memory utilization	RESOLVED	Average
2020-07-01 08:41:31	2020-07-01 08:43:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning
2020-07-01 08:39:31	2020-07-01 08:40:31	XS06 - VIRT. CITRIX	Free disk space is less than 20% on volume Shared memory	RESOLVED	Warning

Updated: 10:56:10

GSM VIOLA: Interface eth0(): Network traffic

8 Kbps6 Kbps4 Kbps2 Kbps0

07-01 09:5610:0010:0510:1010:1510:2010:2510:3010:3510:4010:4510:5007-01 10:56

Interface eth0(): Bits received [avg] 7.46 Kbps min 6.43 Kbps avg 7.44 Kbps max 7.72 Ki

Interface eth0(): Bits sent [avg] 3.54 Kbps min 3.14 Kbps avg 3.67 Kbps max 5.54 Ki

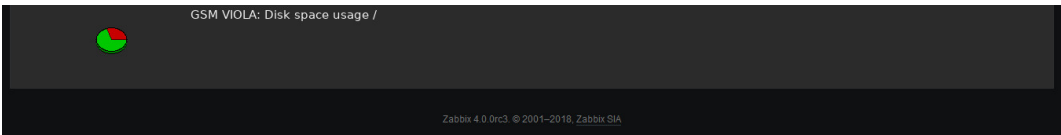
Interface eth0(): Outbound packets with errors [avg] 0 min 0 avg 0 max 0

Interface eth0(): Inbound packets with errors [avg] 0 min 0 avg 0 max 0

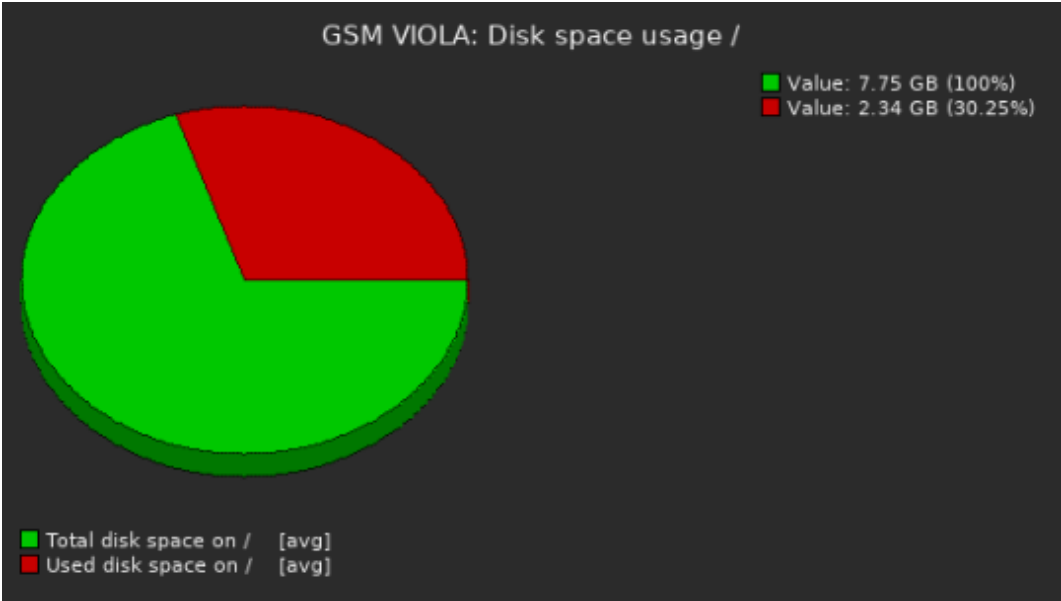
Interface eth0(): Outbound packets discarded [avg] 0 min 0 avg 0 max 0

Interface eth0(): Inbound packets discarded [avg] 0 min 0 avg 0 max 0

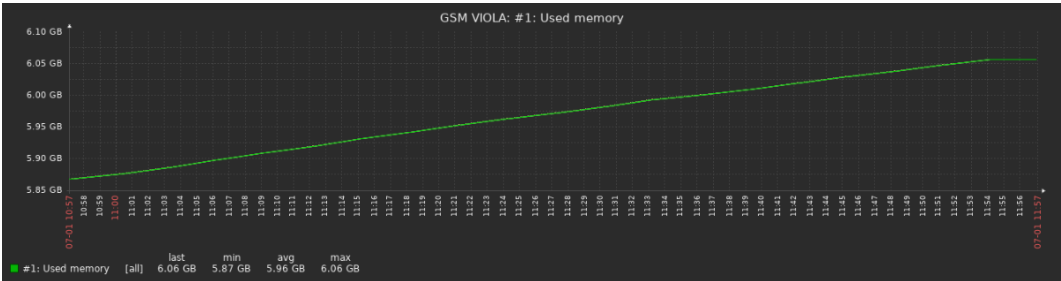
89



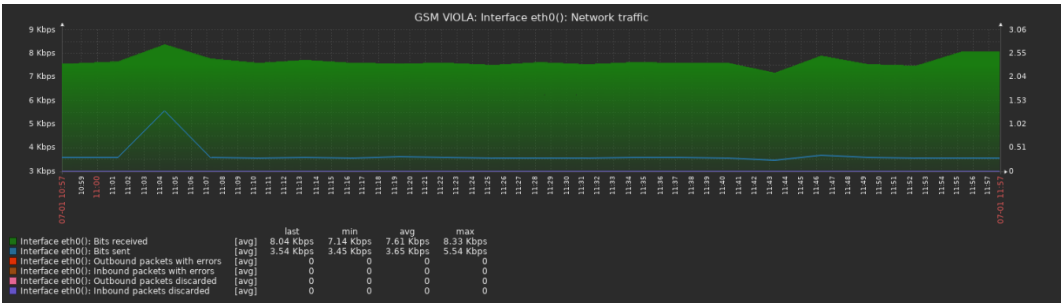
Zabbix - Screens



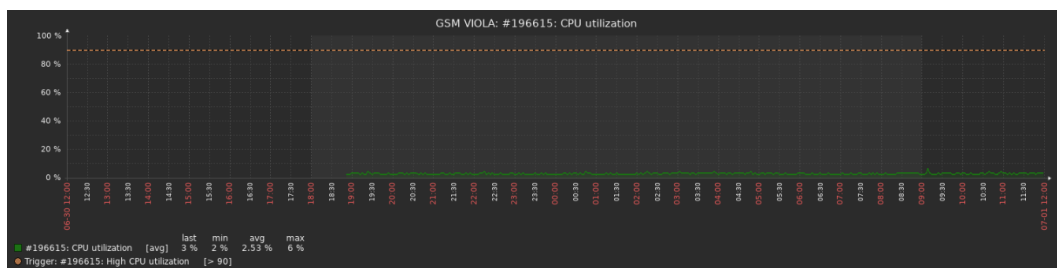
Zabbix - Disk space usage



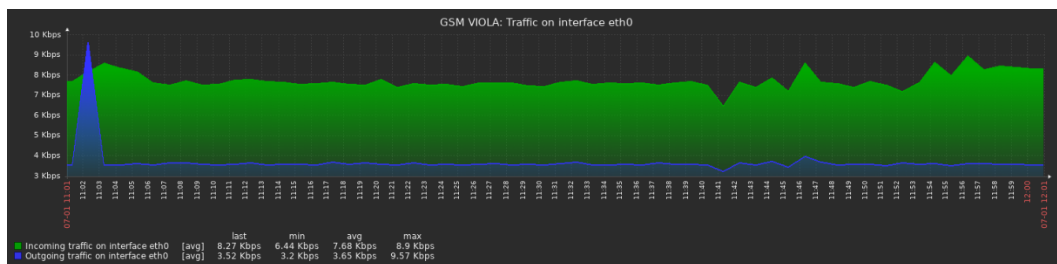
Zabbix - Used memory



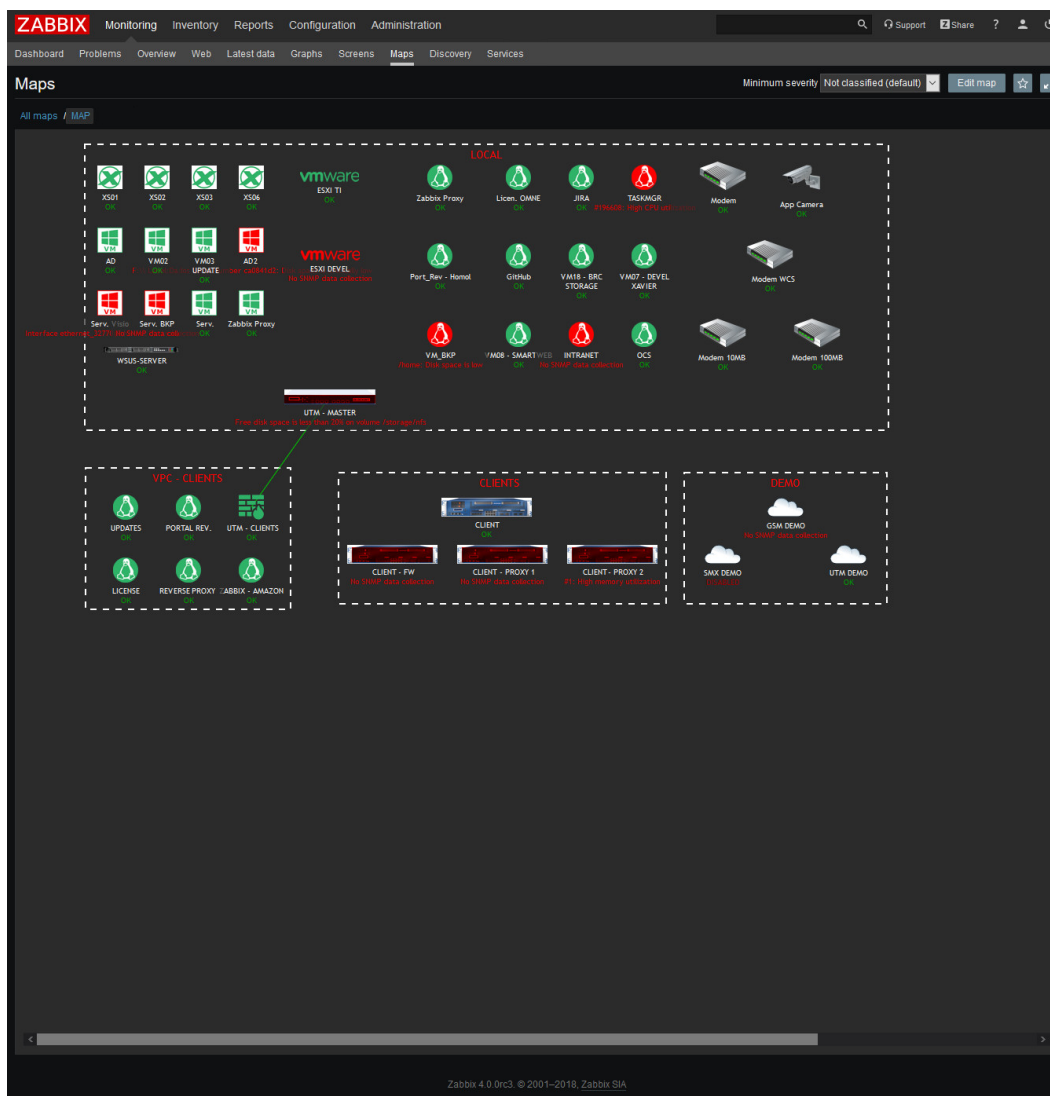
Zabbix - Network Traffic



Zabbix - CPU Utilization



Zabbix - Traffic on interface eth0



Zabbix - Network Map

## Zabbix Template

Among other resources, Zabbix also allows the use of templates to unify devices that use the same configurations, Blockbit provides the Zabbix template in XML format.

To download click this link: [Zabbix Template](#).

It is also possible to access the Resource Center home page, click on "UTM - Unified Threat Management", enter "Downloads" and download it by clicking on "Zabbix Template".



#### UTM - Unified Threat Management

UTM simplifies the administration of your network, increases the performance of your resources and raises the security level of your data, which guarantees high performance and advanced technologies against various malicious techniques and digital threats, in addition to having the best cost-benefit ratio.

#### Documentation

- › [Datasheets](#)
- › [Administrator's Guide](#)
- › [Reference Manuals](#)
- › [Release Information](#)

#### ▼ Downloads

- [Blockbit Client](#)
- [Installation Files](#)
- [Virtual Appliance](#)
- [Zabbix Template](#)

#### SD-WAN

Network adm group devices traffic, deploy security contr Secure Web C Protection, VF

#### Documentation

- › [Administ](#)
- › [Reference](#)
- › [Release In](#)
- › [Download](#)

Link to the Zabbix Template at the Resource Center PT / BR

If you need further instructions on how to use this template, consult the [official Zabbix documentation](#).

For more information on SNMP Notifications, visit this [page](#).

For more information about the configuration, visit the [\[enable-snmp\]](#) page where the console command is detailed in more depth.

# GSM - WEB INTERFACE

This section will demonstrate how to access the Blockbit GSM Web Interface.

The Blockbit GSM has a modern interface, easy to use and responsive, that is, it is able to fit the screen of any device used for access (tablets, smartphones, notebook, etc.). This ensures agility and ease for your company and can be accessed at any time and place.

To access the Blockbit GSM Web Interface, follow the guidelines.

## Accessing the Web Interface – Blockbit GSM

To access the web interface, use a recommended browser.

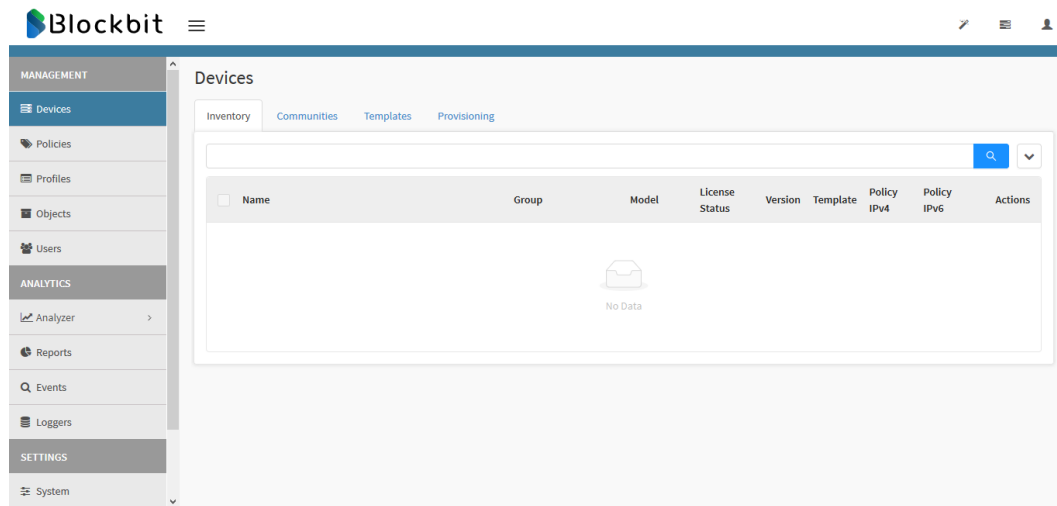
1. Connect to the web browser and access the address: <https://192.168.1.1>. If you have changed the IP address, access the new one;
2. Access the configured IP. Ex.: <https://172.16.102.235>;
3. Enter the following information:
  - **User:** Registered email. E.g.: [admin@blockbit.com](mailto:admin@blockbit.com);
  - **Password:** User's password;
  - **English:** Select the interface language. The available options are Portuguese and English.

The image shows the login screen for the Blockbit GSM web interface. At the top, the 'BLOCKBIT GSM' logo is displayed in blue and black. Below the logo, the text 'Log-in to your account' is centered. The login form consists of three input fields: 'E-mail address' with a person icon, 'Password' with a lock icon, and a language selection dropdown currently set to 'English' with a downward arrow. A large blue 'Login' button is positioned below these fields. At the bottom of the screen, the text 'BLOCKBIT© 2019' is visible. The background of the interface features a light blue sky with white clouds.

Login Screen – System Administration.

- Click on "Login" to access the Web interface.

4. This is the main screen of Blockbit GSM, also known as “Device Manager”.



Device Manager

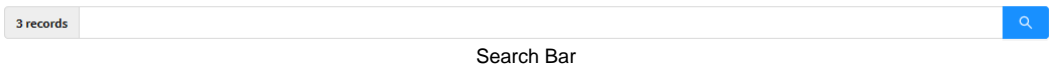
In the next chapter, all buttons and menus will be explained.

# GSM - BASIC OPERATION

Blockbit GSM is composed of some basic features that are available on several different panels, so as to make it easy to use them, here is a basic guide on how to use these features:

## Search Bar

The search bar is located at the top of the panels and makes it possible to locate specific items.



In the **records area** [ 3 records ] displayed in front of the search bar, the amount of records found by the search or present before searching is displayed.

To remove the keywords entered in the search bar, click the [ ✖ ] button; if the search bar is blank, click the **search** [ 🔍 ] button to return to the home screen.

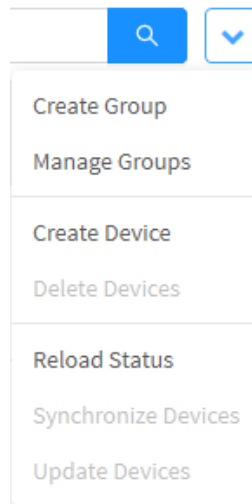
To perform the search, add the desired keyword and click the **search** [ 🔍 ] button.

## Actions menu

The action menu is allocated at the top right of panels and windows:



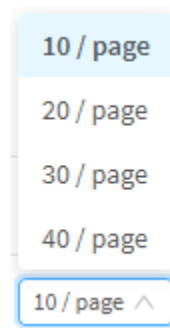
Clicking this button displays a menu with a set of contextual options for the panel where it is located, for example:



Actions menu

## Number of Results

At the bottom of the screen, you can select how many results to display per page, with a minimum of 10 and a maximum of 40 items per page.




Number of Results


Finally, about the navigation, the “Change Pages” buttons allow the user to navigate between pages.



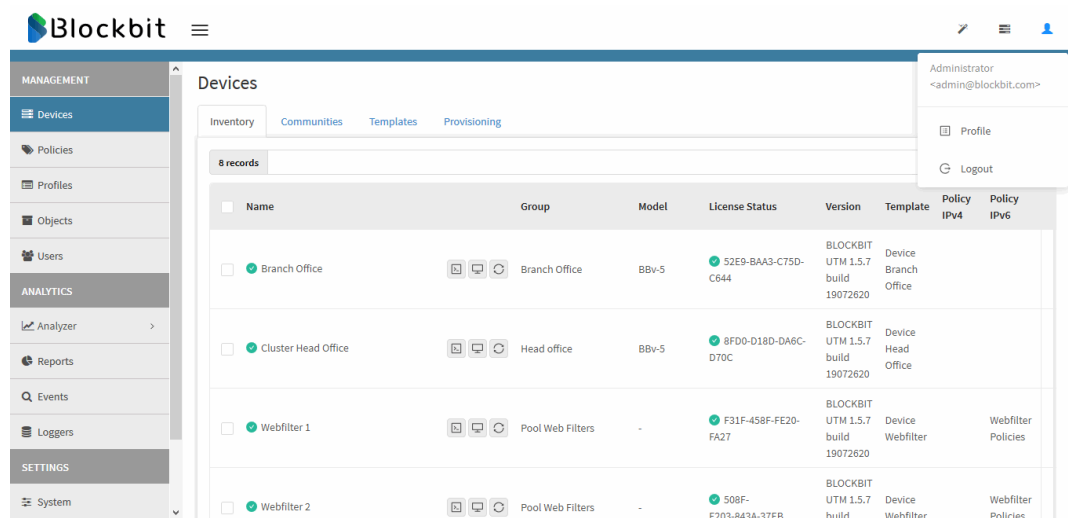
Change pages

# GSM - USER PROFILE MENU

The User profile menu is located in the upper right corner of the screen. To access just click the **user**  icon.



In the screen below the User profile menu appears with the name "admin", this is due to the name registered in the "Name" item in the [Installation Wizard chapter](#).



User profile menu

The User profile menu consists of the options:

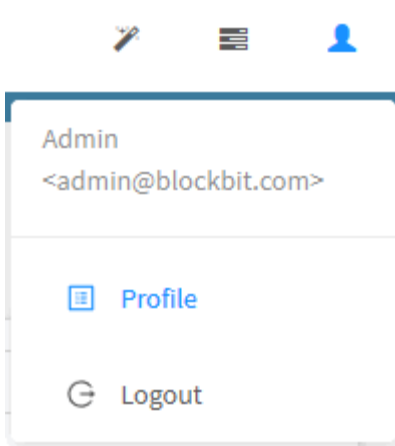
- [Profile](#);
- [Logout](#).

It will be explained in detail next.

# User Profile Menu - Profile

In the "Profile" option you can edit the user profile information. To access it, follow these steps:

1. At the right upper corner of the screen, click on "Profile";



User menu – Profile

2. Modify the profiles changes to the profile. This screen contains the following information:

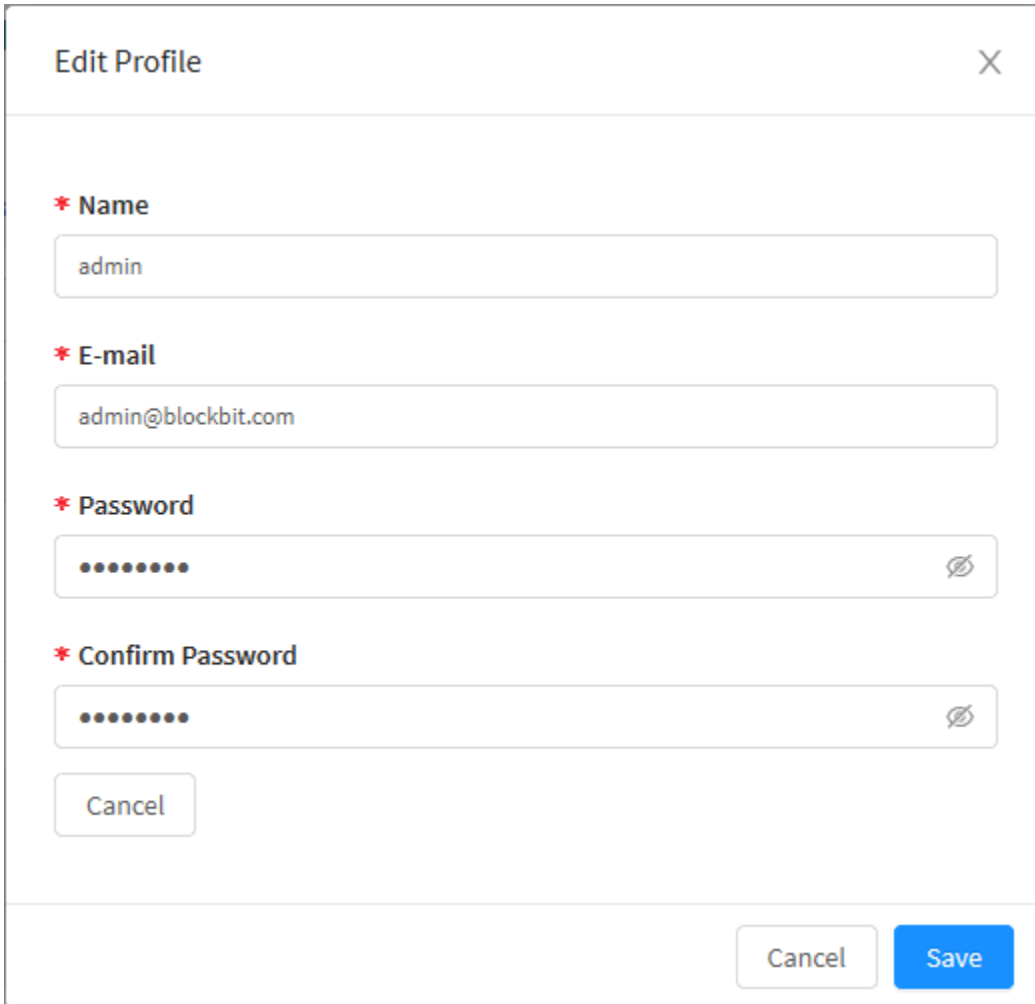
- **Name:** Enter the registered username;
- **Email:** Enter the registered user's email. This field is used to login to the Blockbit GSM;

A screenshot of a web form titled 'Edit Profile'. The form has a close button (X) in the top right corner. It contains two required fields, each marked with a red asterisk: 'Name' and 'E-mail'. The 'Name' field contains the text 'admin'. The 'E-mail' field contains the text 'admin@blockbit.com'. Below these fields is a blue button labeled 'Change Password'. At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

User Menu – Edit Profile

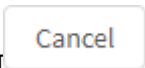

3. To change the password information, click **Change Password** 

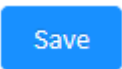
- **Password:** Enter the new password;
- **Confirm Password:** Confirm the password provided in the previous step.



The image shows a modal dialog box titled "Edit Profile" with a close button (X) in the top right corner. The dialog contains four required fields, each marked with a red asterisk: "Name" (containing "admin"), "E-mail" (containing "admin@blockbit.com"), "Password" (masked with dots and a toggle icon), and "Confirm Password" (masked with dots and a toggle icon). Below the "Confirm Password" field is a "Cancel" button. At the bottom right of the dialog are two buttons: "Cancel" and "Save".

Edit Profile – Password change

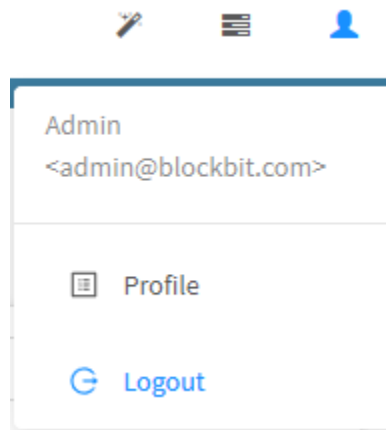
To exit this window, simply click on **Cancel** , or on the  at the top right of the screen to return to the previous window.

Click the **Save**  button to save changes, the system will update and prompt you to Login again.



# User Profile Menu – Logout

You can leave the system at any time. Just click on the "Log Out" button.



Logout

This will take the user back to the "Login" page.

# GSM - DEPLOYS PANEL

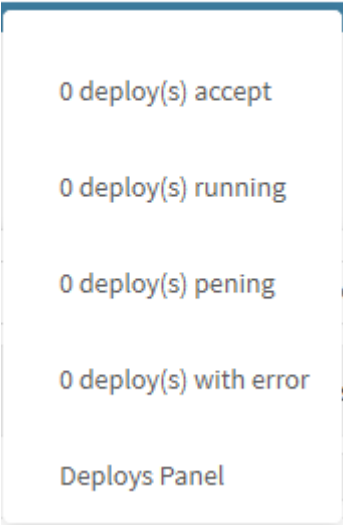
This section will demonstrate how to track and manage the **Blockbit** GSM configuration packages installations on managed devices. These packages, when requested to install, are called DEPLOYS.

To access the Deploys Panel, click on the button located at the top right of the screen, next to the user's menu:



"Deploys Panel" button

A screen will appear listing the deploy. To access the screen with filters, click on one of the four options: deploy(s) accept, deploy(s) running, deploy(s) pending and deploy(s) with an error. A new tab will open in the browser with the selected filter. If you want to access the screen without a filter, click on the "Deploys Panel" button.



Deploys Panel – List

To open Deploys Panel, select the option [ **Deploys Panel** ] from the list. The following screen will appear:

### Deploys

Scheduled	Owner	Auditor	Status	Package	
20/10/2019 ~ 19/11/2019					

Package	Auditor	Scheduled	Progress	Status	Actions
Device Communities	admin Owner: admin	25/09/2019 11:47 Created: 25/09/2019 11:47	<div><div></div></div> 0%	Cancelled	
Device Templates	admin Owner: admin	25/09/2019 11:37 Created: 25/09/2019 11:37	<div><div></div></div> 0%	Cancelled	
Policy Pack	admin Owner: admin	25/09/2019 11:00 Created: 25/09/2019 11:00	<div><div></div></div> 50%	Running	
Device Communities	admin Owner: admin	25/09/2019 09:54 Created: 25/09/2019 09:54	<div><div></div></div> 0%	Pending	
Device Templates	admin Owner: admin	25/09/2019 09:37 Created: 25/09/2019 09:37	<div><div></div></div> 0%	Error	
Device Communities	admin Owner: admin	25/09/2019 09:16 Created: 25/09/2019 09:16	<div><div></div></div> 0%	Error	
Device Templates	admin Owner: admin	25/09/2019 09:15 Created: 25/09/2019 09:15	<div><div></div></div> 0%	Cancelled	

### Deploys

The Deploys screen consists of a progress panel at the top of the screen, a search tool bar, and a six-column task list:

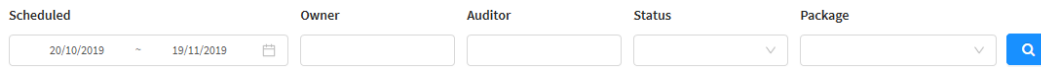
- [Package](#);
- [Auditor](#);
- [Scheduled](#);
- [Progress](#);
- [Status](#);
- [Action](#).

Next we will analyze the [Search bar and Filters](#) on this panel.

# Deploys Panel - Search and Filters

To find a specific Deploy, there is a search bar divided into: “*Scheduled*”, “*Owner*”, “*Auditor*”, “*Status*”, “*Package*” and the “*Search*” button.

In this session, we will analyze the operation of the Deploys search system.




The screenshot shows a search interface with five filter fields: 'Scheduled' (with a date range from 20/10/2019 to 19/11/2019), 'Owner' (text input), 'Auditor' (text input), 'Status' (dropdown menu), and 'Package' (dropdown menu). A blue 'Search' button with a magnifying glass icon is located to the right of the 'Package' field.

*Deploys Panel – Deploys Search.*

From left to right, we have:

- **Scheduled:** Filters by start or end date/time, referring to the date when the Deploy was scheduled;
- **Owner:** Filters by the user who created the Deploy;
- **Auditor:** Filtered by the auditor who approved the Deploy;
- **Status:** Filter by Deploy status, which can be of the following: Success, Accept, Running, Pending, Error or Canceled;
- **Package:** Filters by Deploy type, which can be: Policy Package, Device Template or Device Community.



To perform the search, click the **search**[] button.

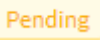





# Deploys Panel – Deploys List

In the deploy list, all the created deploys in the system are displayed.

Scheduled	Owner	Auditor	Status	Package	
20/10/2019 ~ 19/11/2019					
Package	Auditor	Scheduled	Progress	Status	Actions
Device Communities	admin Owner: admin	25/09/2019 11:47 Created: 25/09/2019 11:47	<div></div> 0%	Cancelled	
Device Templates	admin Owner: admin	25/09/2019 11:37 Created: 25/09/2019 11:37	<div></div> 0%	Cancelled	
Policy Pack	admin Owner: admin	25/09/2019 11:00 Created: 25/09/2019 11:00	<div></div> 50%	Running	
Device Communities	admin Owner: admin	25/09/2019 09:54 Created: 25/09/2019 09:54	<div></div> 0%	Pending	
Device Templates	admin Owner: admin	25/09/2019 09:37 Created: 25/09/2019 09:37	<div></div> 0%	Error	
Device Communities	admin Owner: admin	25/09/2019 09:16 Created: 25/09/2019 09:16	<div></div> 0%	Error	
Device Templates	admin Owner: admin	25/09/2019 09:15 Created: 25/09/2019 09:15	<div></div> 0%	Cancelled	

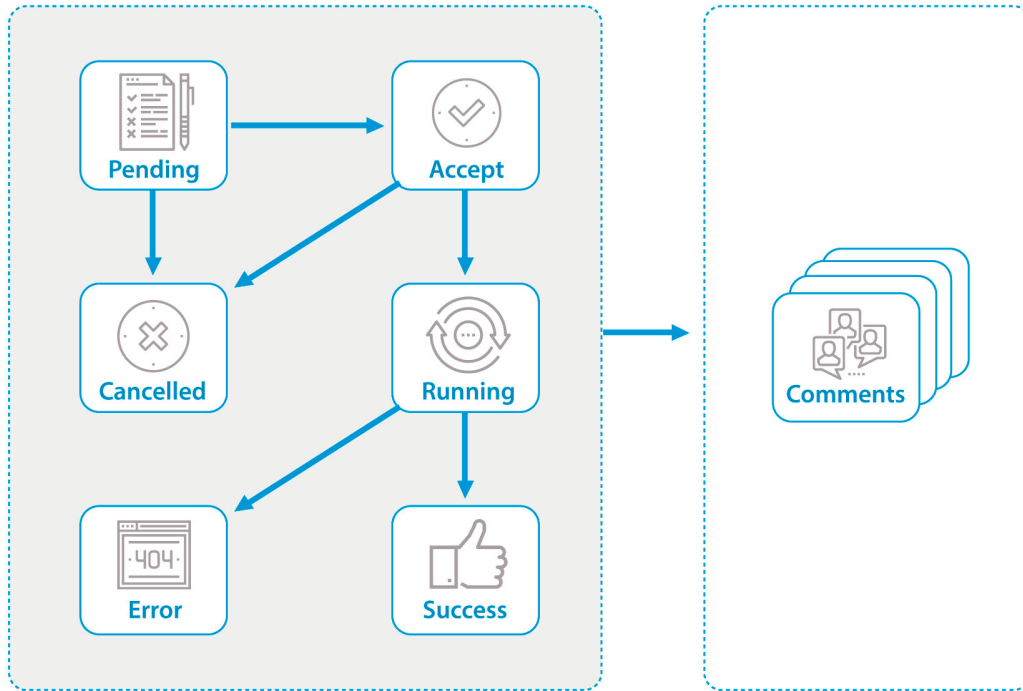
Deploys Panel – Deploy List

The deploys system has a business rule that consists of the following premises:

- The deploy list is always sorted by date of creation and in the descending order;
- The status of a deploy is classified as:
  - **Pending** : Package awaiting auditor's decision;
  - **Accept** : Package has been accepted and its deploy will start within the specified time;
  - **Running** : The package is being implemented;
  - **Success** : Package was successfully implemented;
  - **Cancelled** : Package implementation canceled;
  - **Error** : Something wrong has occurred (for more information, just click on the error icon).
- All activities within a deploy require a comment. Comments are added to the deploys "Activity" list;
- If you have a device with "Error" status, it will be the main status of the entire deploy.

Next, the deployment approval process:

## Deploys Panel



Deploys Panel - Deploys Approval Process

The deploys panel consists of the columns:

- [Package](#);
- [Auditor](#);
- [Scheduled](#);
- [Progress](#);
- [Status](#);
- [Actions](#).

Next we'll look at each column of this panel.

# Deploys Panel – Package column

The Package column displays the package name applied to deploy.

To view details of the Package applied to the deploy, click on the package name. The Task View screen appears:

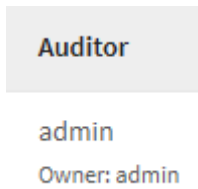


*Deploys Panel - Task view.*

To close the window, click the **Close** button or click [X] at the top of the window.

# Deploys Panel – Auditor column

The Auditor column displays the name of the Deploy Owner and the registered auditor, who is responsible for approving it.



*Deploys Panel – Auditor*



## Deploys Panel – Scheduled column

The "Scheduled" column displays information regarding the day the deploy was created and the date it's scheduled to run.

Scheduled

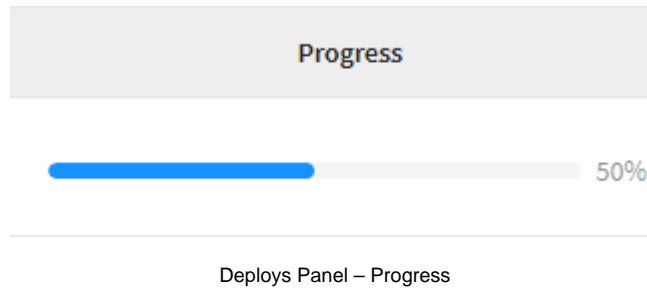
19/11/2019 14:23

Created: 19/11/2019 15:24

Deploys Panel – Scheduled

# Deploys Panel – Progress column

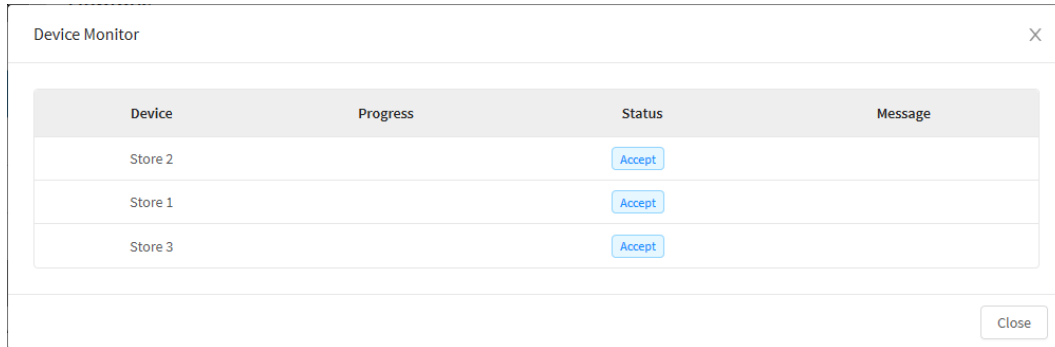
The Progress column displays a progress bar that shows you the deploy completion percentage.



# Deploys Panel – Status column

The "Status" column displays the current status of a particular deploy: Pending, Running, Canceled, Success and Error.

To display detail of the Status of each device that will be applied in a particular deploy, click on the Status name and the "Deploy Information" screen will appear:

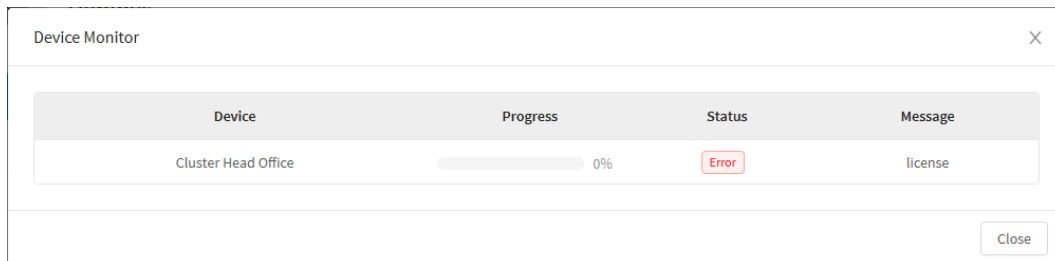


Device	Progress	Status	Message
Store 2		Accept	
Store 1		Accept	
Store 3		Accept	

*Deploys Panel – Device Status.*

The statuses displayed in this column and on this screen are identical to those [previously mentioned](#).

In the "Message" column, messages related to any failures are displayed (if the status "error" appears). The image below exemplifies the function of this column:



Device	Progress	Status	Message
Cluster Head Office	0%	Error	license

*Deploys Panel – Error Message.*

Next, we will explain the buttons and their respective statuses.

# Deploys Panel - Actions column

The action column provides some buttons with essential functionality for deploys:



There are five action buttons:

- [Accept](#);
- [Reinstall](#);
- [Cancel](#);
- [Activity](#);
- [Remove](#).

Next, we will show the features of each button.

## Deploys Panel – “Accept” button

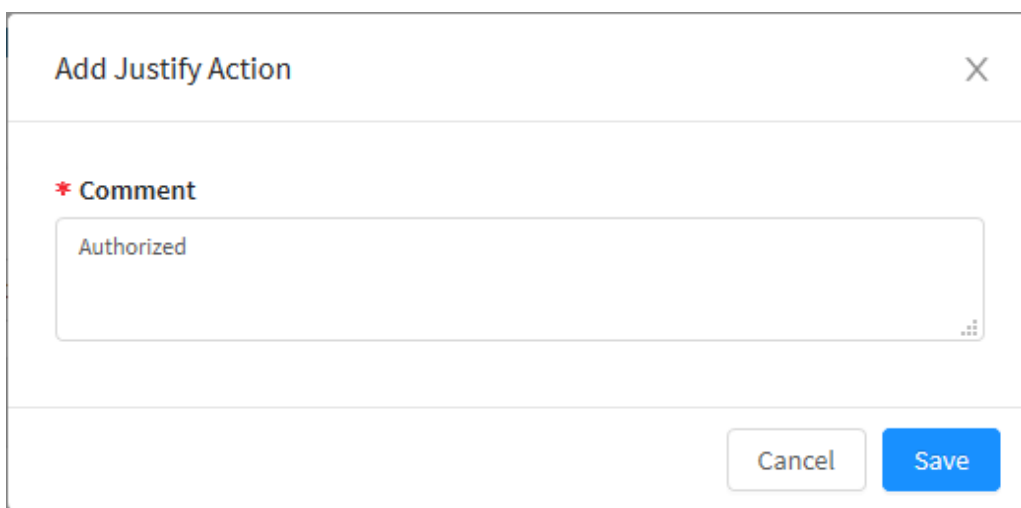
Through the "Accept" button the auditor can approve the installation of the package. It is also possible to leave a comment about the reason that justifies the approval of the Deploy.

To access, click on the "Accept" button.

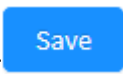
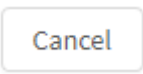


“Accept” button

The Add Justify Action screen will appear. Write the desired comment:

A dialog box titled "Add Justify Action" with a close button (X) in the top right corner. Below the title is a red asterisk followed by the text "Comment". Underneath is a text input field containing the word "Authorized". At the bottom right of the dialog are two buttons: "Cancel" and "Save".

Add Justify Action

Click on the **Save**  button to conclude the process or the **Cancel**  button to close the screen.

# Deploys Panel - "Reinstall" Button

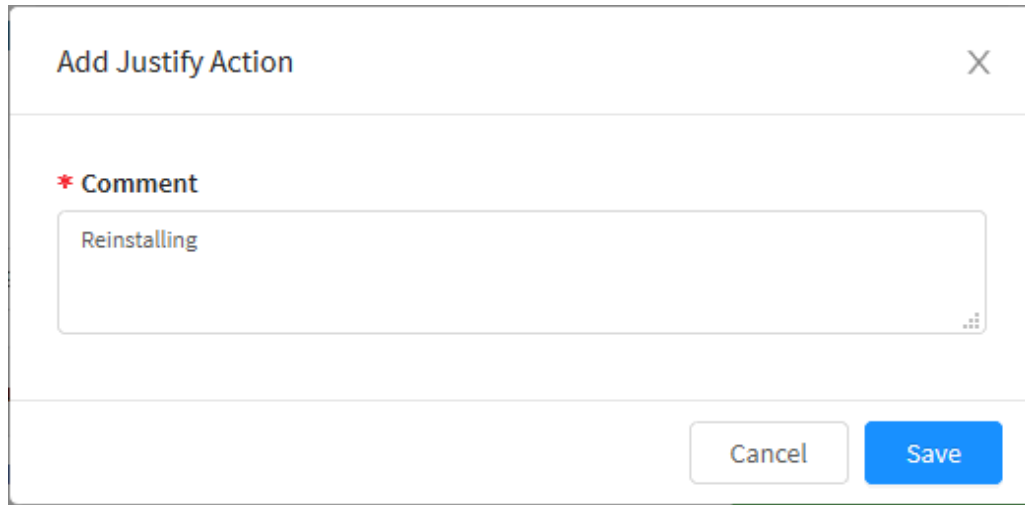
The "Reinstall" button performs the reinstallation of the packages.

To access, click on the "Reinstall" button.

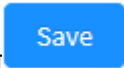



"Reinstall" button

The "Add Justify Action" screen will appear, under "Comment", write the desired comment:

A dialog box titled "Add Justify Action" with a close button (X) in the top right corner. Below the title, there is a section labeled "\* Comment" with a text input field containing the word "Reinstalling". At the bottom right of the dialog, there are two buttons: "Cancel" and "Save".

Reinstall Deploy

Click the **Save** button[] to save or **Cancel**[] to close the screen.

## Deploys Panel – “Cancel” button

Using the "Cancel" button, the auditor is able to reject the package installation. It is also possible to leave a comment with the reason for rejecting the Deploy.

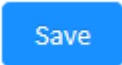
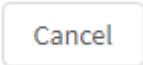
To access it, click on the "Cancel" button.



"Cancel" Button.

The Justify screen will be displayed.

Justify Action Cancellation

Click on the **Save**  to complete the procedure or **Cancel**  to close the screen.

# Deploys Panel - "Activity" button

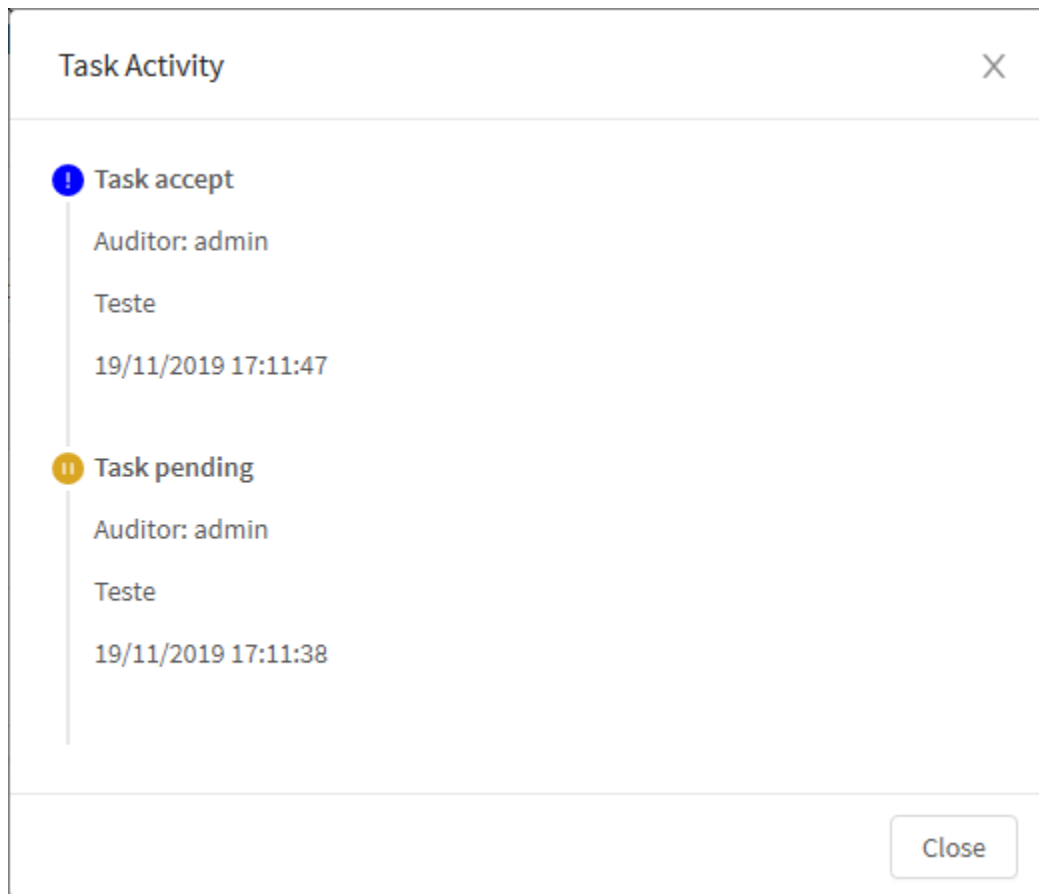
The "Activity" button displays Deploys activity history.

To access, click on the "Activity" button.



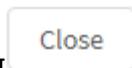
Deploys Panel Action Buttons – "Activity"

Task Activity screen will appear:



"Deploy Activity" button

Click on the **Close** button to close the screen.





# Deploys Panel - “Remove” button

The "Remove" button does exactly what the name says: It revokes the package.

To access it, click on the "Remove" button.



"Remove" Button

Delete Deploy


X

Are you sure you want to delete?

CancelDelete

Remove Deploy

Click on the **Delete** button to complete the procedure or the **Cancel** button to close the screen.

 **Deploy deleted successfully**  
Deploy deleted successfully

The deletion was successful.

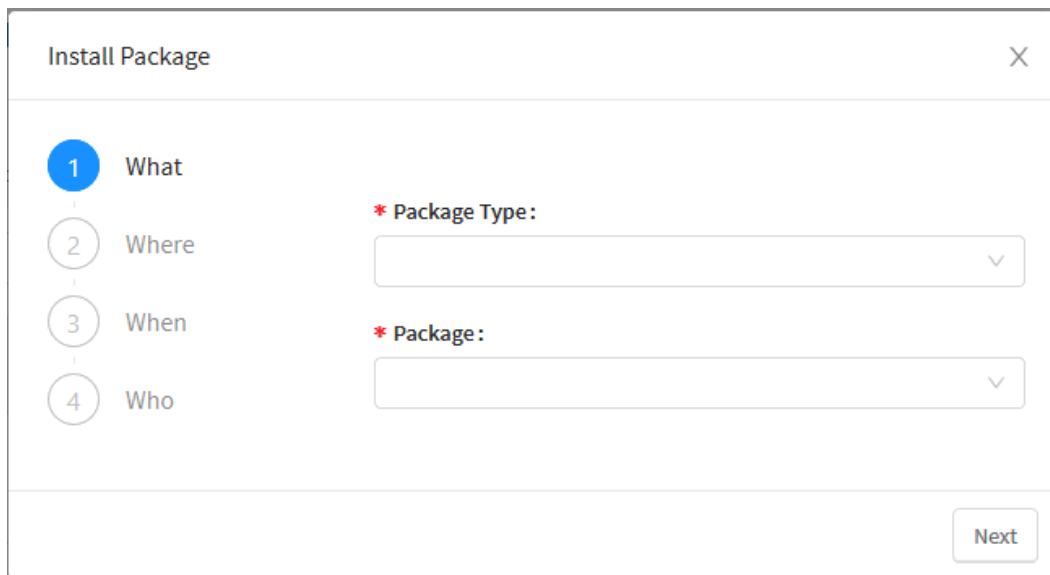
# GSM - INSTALL PACKAGE

Through the "Install Package" button, it is possible to install the configuration package for devices integrated with Blockbit GSM.



"Install Package" Button

Clicking on the button will bring up the Install Package screen:

A screenshot of the 'Install Package' window. The window has a title bar with 'Install Package' and a close button (X). On the left, there is a vertical list of four steps: '1 What' (highlighted with a blue circle), '2 Where', '3 When', and '4 Who'. To the right of the steps, there are two dropdown menus. The first is labeled '\* Package Type :' and the second is labeled '\* Package :'. Both dropdown menus have a downward arrow icon. At the bottom right of the window, there is a 'Next' button.

*Install Package.*

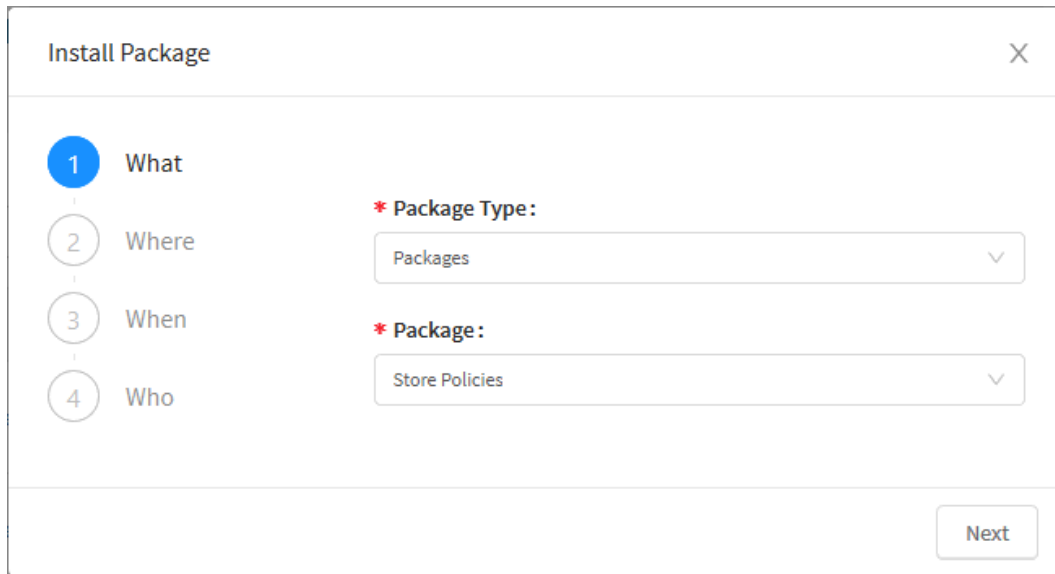
The Install Package window consists of:

- [What](#);
- [Where](#);
- [When](#);
- [Who](#).

Below we will analyze the components of the "Install Package" panel:

# What

Determines which operation will be performed, consisting of:



Install Package – What.

- **Package type:** This drop-down menu determines the type of package that will be installed, which can be of the following types:
  - **Policy Package:** With this option, you can install the packages created in "Policies", in the ["Policy Package"](#) tab;
  - **Device Template:** With this option, you can install the templates in "Device", in the ["Device Templates"](#) tab;
  - **Device Community:** Through this option, it is possible to install the communities in "Device", in the ["Device Communities"](#) tab;
- **Package:** This drop-down menu specifies the desired Policy, Device or Device Community.

The image shows a rectangular button with rounded corners and a light gray border. The word "Next" is centered inside the button in a blue, sans-serif font.

Click the next [ ] button to proceed to the [Where](#) panel and continue the procedures.

# Where

Determines where the package will be installed, consisting of:

Install Package

✓

What

2

Where

3

When

4

Who

Devices & Device group :

GROUP - Stores

X

Previous

Next

Install Package – Where.

- **Devices & Devices group:** Selects the device or device group on which packages will be installed. Select the desired option to add the item. If you chose the wrong item, click [ X ] or select the item from the list again to deselect it. Its possible to select multiple groups or devices;

To return to the [What](#) panel, click the [ 

Previous

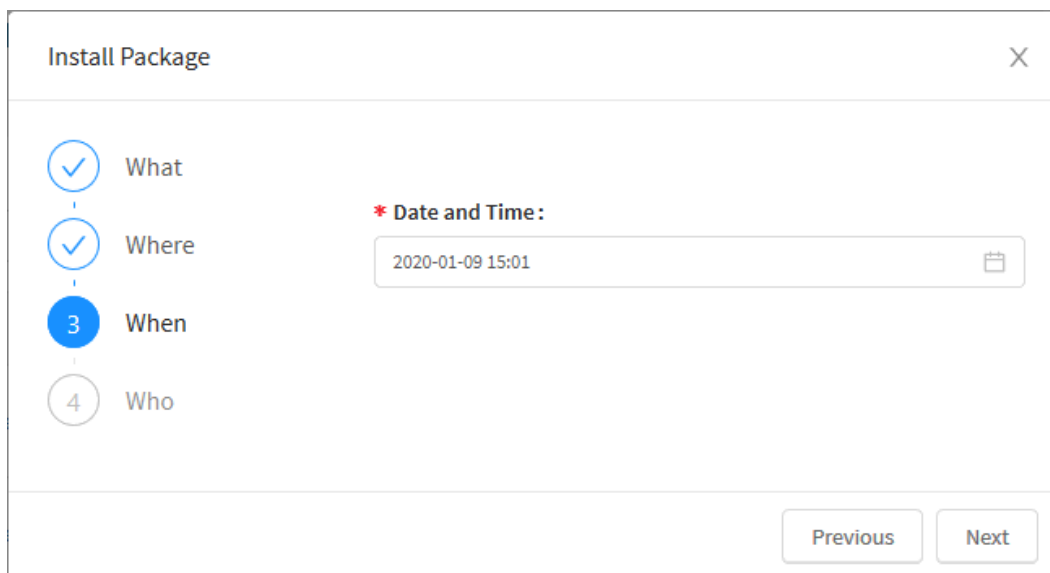
 ] button, to continue the procedures and access the [When](#) panel, click the [ 

Next

 ] button.


# When

Determines the moment at which the package will be installed, consisting of:



The screenshot shows a dialog box titled "Install Package" with a close button (X) in the top right corner. On the left side, there is a vertical list of four steps: "What", "Where", "When", and "Who". Each step is preceded by a circular icon. The "What" and "Where" steps have a checkmark icon, indicating they are completed. The "When" step has a blue circle with the number "3", indicating it is the current step. The "Who" step has a circle with the number "4", indicating it is the next step. To the right of the steps, there is a section titled "\* Date and Time:" in red. Below this title is a text input field containing the date and time "2020-01-09 15:01". To the right of the input field is a calendar icon. At the bottom right of the dialog box, there are two buttons: "Previous" and "Next".

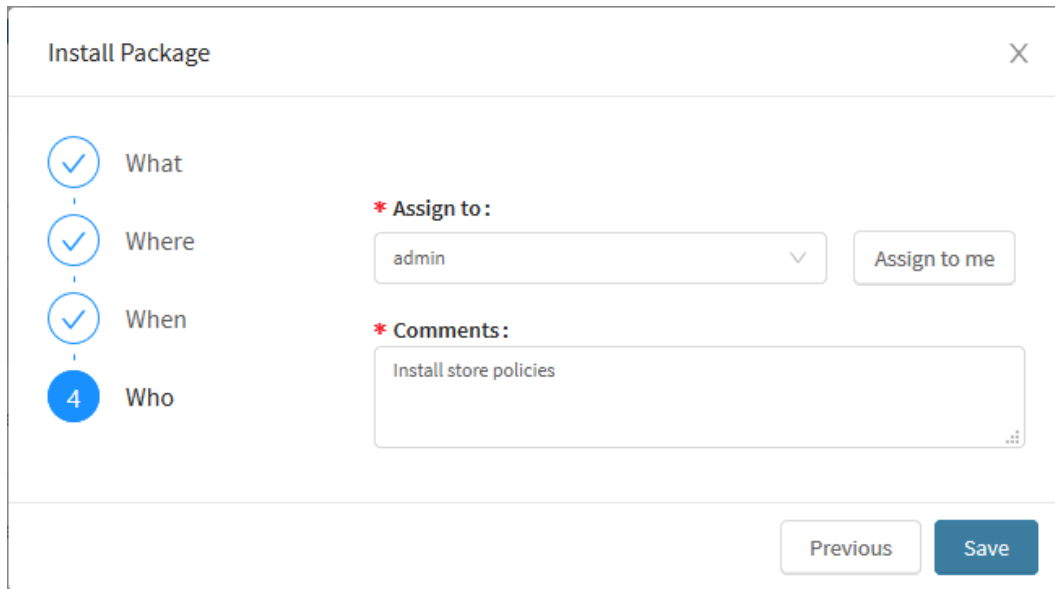
*Install Package – When.*

- **Date and Time:** Sets the desired date and time. To select the desired time, select the desired date and then click the "**select time**" option to determine the desired time. If you want to enter the current date and time, click on the "**Now**" option, finally to determine the time, just click the [  ] button.

To return to the [Where](#) panel, click the [  ] button, to continue the procedures and access the [Who](#) panel, click the [  ] button.


# Who

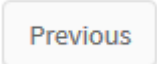

Determines who will be responsible for installing the package, consisting of:



The screenshot shows a dialog box titled "Install Package" with a close button (X) in the top right corner. On the left side, there is a vertical list of four steps: "What", "Where", "When", and "Who". Each step is preceded by a circular icon. The "What", "Where", and "When" icons contain a checkmark, while the "Who" icon contains the number "4". The "Who" step is highlighted with a blue background. To the right of the steps, there are two sections. The first section is labeled "\* Assign to:" and contains a dropdown menu with "admin" selected and a small downward arrow, followed by a button labeled "Assign to me". The second section is labeled "\* Comments:" and contains a text area with the text "Install store policies" and a small icon in the bottom right corner. At the bottom right of the dialog box, there are two buttons: "Previous" and "Save".

*Install Package – Who.*

- **Assign To:** Defines the Auditor responsible for approving the configuration installation. If you want to be responsible, click on the [  ] button. Ex.: Admin;
- **Comments:** Enter the comment to define the function of these settings, making it easier for the Auditor to understand it;

To return to the [When](#) panel, click the [  ] button, to save the setup package installation prompt click the [  ] button.

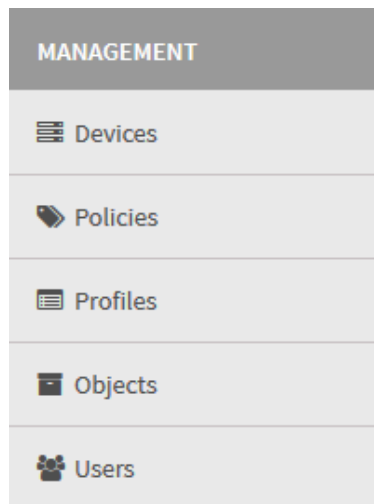
After performing these procedures, the Template installation request will have been successfully completed.

To apply these settings, see chapter [Deploys Panel](#).

# GSM - MANAGEMENT

Blockbit GSM enables the administration of multiple network devices together, providing a full perspective of the infrastructure of all organizational units, the ability to generate configuration templates and security policy packages for sharing between groups of devices and for determining the controls of access by function, is able to establish and catalog all records of connection, access to Internet applications, personal data and content of private communications in accordance with the regulations of the Civil Registry of the Internet.

Through the "Management" menu it is possible to administer the devices, policies, profiles, objects and system users.



*Menu Management.*

Contains options:

- [Devices](#);
- [Policies](#);
- [Profiles](#);
- [Objects](#);
- [Users](#).

# Devices

The Devices panel is of vital importance for the Blockbit GSM, its main function is the ability, as the name says, to manage all connected devices through a single central point, putting it in simple terms: Through this panel, Blockbit GSM manages Blockbit UTM and, in the future, other digital solutions from Blockbit.

First, when you log into Blockbit GSM, the “Inventory” tab will be automatically selected. In addition, it is possible to access the “Devices” by clicking on the button located in the vertical side menu, or by selecting the appropriate tab (if the button has already been selected).



Management – Devices

The screen below will be displayed:

Devices

Inventory Communities Templates Provisioning

8 records

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/>	Branch Office	Branch Office	BBv-5	32E9-8AA5-C7SD-C644	BLOCKBIT UTM 1.5.7 build 19072620	Device Branch Office			
<input type="checkbox"/>	Cluster Head Office	Head office	BBv-5	6FD9-D16D-D4eC-D70C	BLOCKBIT UTM 1.5.7 build 19072620	Device Head Office			
<input type="checkbox"/>	Webfilter 1	Pool Web Filters	BBv-5	F31F-466F-FE20-FA27	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 2	Pool Web Filters	BBv-5	508F-E203-843A-37EB	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 3	Pool Web Filters	BBv-5	FBA7-4F24-21F0-4060	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Store 1	Stores	BBv-5	B30D-8ED6-6C7D-543C	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		
<input type="checkbox"/>	Store 2	Stores	BBv-5	715E-69F2-CCE0-FB0F	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		
<input type="checkbox"/>	Store 3	Stores	BBv-5	D62E-61C4-25B3-751A	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		

< 1 > 10 / page

Devices - Inventory

The Devices screen has the following tabs:

- [Inventory;](#)
- [Communities;](#)
- [Templates;](#)
- [Provisioning.](#)

Next, the components of the [Inventory](#) tab will be analyzed.



# Inventory Tab

In Blockbit GSM it is possible to carry out an inventory of all your devices easily, such as: Status, License, Version and Updates of the integrated devices.

The "Inventory" tab consists of seven columns: "*Name*", "*Group*", "*Model*", "*License Status*", "*Version*", "*Template*", "*Policy IPV4*", "*Policy IPV6*" and "*Actions*". The devices are divided into groups and in addition, at the top of the screen are the [search bar](#) and in the upper right corner of the screen is the [actions menu](#).

Devices

InventoryCommunitiesTemplatesProvisioning

8 records

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPV4	Policy IPV6	Actions
<input type="checkbox"/>	Branch Office	Branch Office	BBv-5	52E9-BAA5-C79D-C644	BLOCKBIT UTM 1.5.7 build 19072620	Device Branch Office			
<input type="checkbox"/>	Cluster Head Office	Head office	BBv-5	8FD0-D18D-DA6C-D70C	BLOCKBIT UTM 1.5.7 build 19072620	Device Head Office			
<input type="checkbox"/>	Webfilter 1	Pool Web Filters	BBv-5	F31F-496F-FE20-FA27	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 2	Pool Web Filters	BBv-5	908F-E203-843A-07EB	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 3	Pool Web Filters	BBv-5	FB47-AF24-21F0-4060	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Store 1	Stores	BBv-5	B90D-8ED9-8C7D-943C	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		
<input type="checkbox"/>	Store 2	Stores	BBv-5	715E-89F2-CCED-FBDF	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		
<input type="checkbox"/>	Store 3	Stores	BBv-5	D92E-91C4-25B5-751A	BLOCKBIT UTM 1.5.7 build 19072620	Device Store	Store Policies		

< 1 > 15 / page

Inventory tab

This section will demonstrate how to:

- [Register](#), [Edit](#) and [Remove devices](#);
- [Manage groups of devices](#);
- [Synchronize devices with GSM](#);
- Etc.

Next, we'll look at the functions located at the top of this panel.

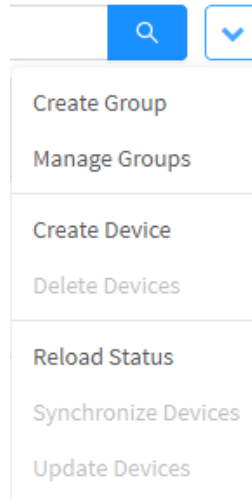
# Inventory - Actions menu

At the top right of the screen we have the actions menu:



Inventory - Actions menu button

By clicking on this button the menu below is displayed:



Inventory - Actions menu


The menu consists of the following options:

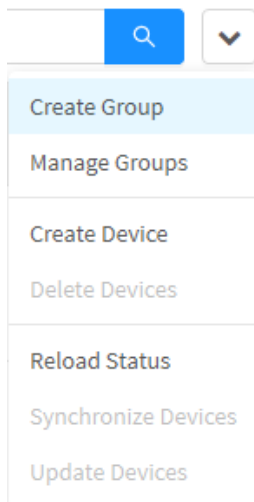
- [Create Group](#);
- [Manage Groups](#);
- [Create Device](#);
- [Delete Devices](#);
- [Reload Status](#);
- [Synchronize Devices](#);
- [Update Devices](#).

Next, each option in the action menu will be detailed.

# Inventory - Actions menu - Create Group

The groups of devices or Device Manager aim to organize the registered devices. They also facilitate the installation of configurations (deploy) for the various devices in a single action, that is, it is not necessary to apply configurations to each one of them, just select the group, and it will be displayed and in case you want to change something, all applications will be carried out in one go. To create the device groups, follow these steps:

1. Click the **Actions menu icon** [];
2. Select the "Create Group" option;



Inventory - Actions menu - Create Group

3. An "Add Group" screen will appear, allowing you to create the desired group. Fill in the fields:

Add Group
X

**\* Name**

**Description**

**Devices**

Store 1 X
Store 2 X
Store 3 X

**Logger**

Cancel
Save

Inventory – Add Group

- **Name:** Group's name. Ex.: *Stores*;
- **Description:** Description of the device group. Ex.: *Store Group*;
- **Devices:** Here it is determined which devices are part of the group being created (you can leave it blank to add the devices later in [Inventory - Actions Menu - Create Device](#), or in provisioning in the [Provisioning - Actions Menu - Create Device](#)). The devices added in this field will be inserted as tags;
- **Logger:** Its function is to determine the [logger](#) that will be used to send reports (logs) to the [analyzer](#).

If you want to cancel click on the  button. To complete the creation of the policy package click on the  button.


 **Group registered with success!**

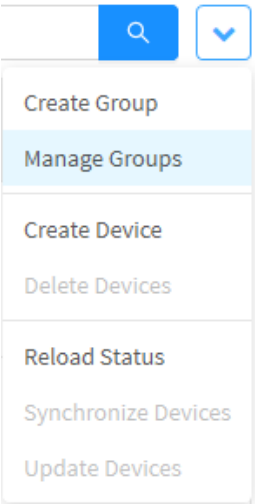
*Group registered with success*

The group was created successfully. After adding the group, it is possible to manage them in [Inventory - Actions Menu - Manage Groups](#).

# Inventory - Actions menu - Manage Groups

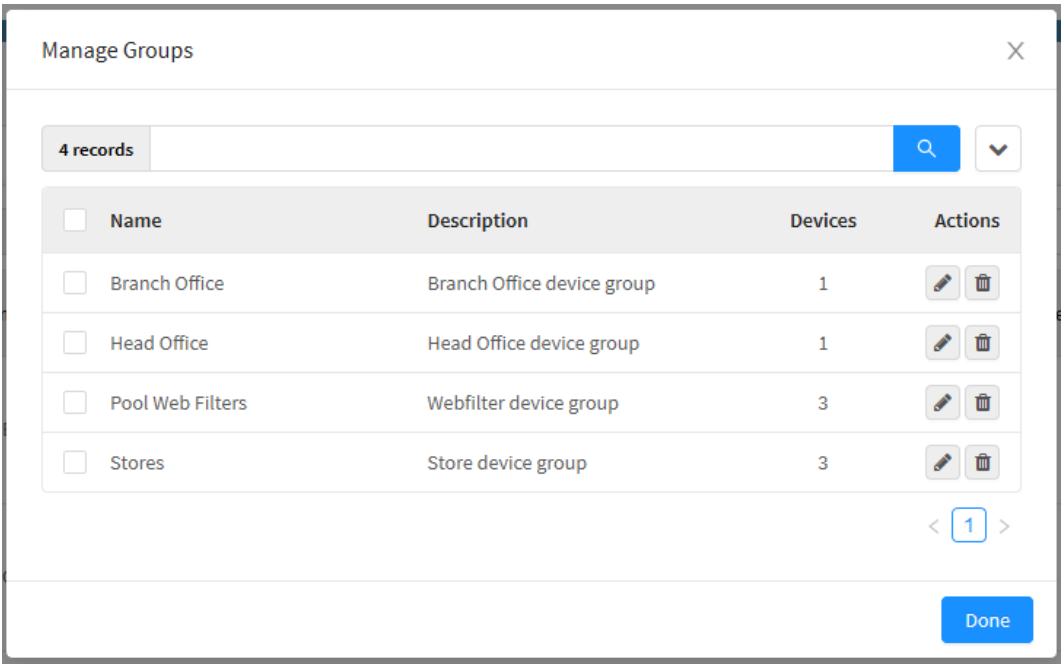
To manage device groups. Follow the steps below:

- 1. Click the **Actions Menu icon** [  ];
- 2. Click on the "Manage Groups" option;



Inventory - Actions menu - Manage Groups

- 3. The group administration screen will be displayed:



Inventory - Actions menu - Manage Groups

Next we will analyze each component of this window.

For more information about the action menu in this window, click on this [page](#).

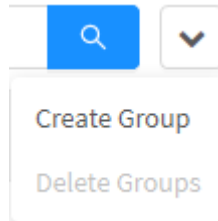
# Manage Groups - Actions menu

At the top right of the screen we have the actions menu:



Manage Groups - Actions menu button

By clicking on this button the menu below is displayed:



Manage Groups - Actions menu


The menu consists of the following options:

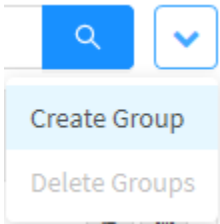
- [Create Group](#);
- [Delete Groups](#).

Next, each option in the action menu will be detailed.

# Manage Groups - Create Group

The groups of devices or Device Manager aim to organize the registered devices. They also facilitate the installation of configurations (deploy) for the various devices in a single action, that is, it is not necessary to apply configurations to each one of them, just select the group and it will be displayed and in case you want to change something, all applications will be carried out in one go. To create the device groups, follow these steps:

1. Click the Actions menu icon [  ];
2. Select the "Create Group" button;



Inventory - Actions menu - Create Group

3. The "Add Group" screen will appear, allowing you to create the desired group. Fill in the fields:

Add Group

\* Name

Stores

Description

Store device group

Devices

Store 2 XStore 1 XStore 3 X

Logger

Cancel

Save

Inventory – Add Group.

- **Name:** Group's name. Ex.: Stores;



- **Description:** Description of the device group. Ex.: *Store device group*;
- **Devices:** Here it is determined which devices are part of the group being created (you can leave it blank to add the devices later in [Inventory - Actions Menu - Create Device](#), or in provisioning in the [Provisioning - Actions Menu - Create Device](#)). The devices added in this field will be inserted as tags.
- **Logger:** Its function is to determine the [logger](#) that will be used to send reports (logs) to the [analyzer](#).



If you want to cancel click on the [ ] button. To complete the procedure, click the [ ] button.

 **Group registered with success!**

*Group registered with success*


The group was created successfully. After adding the group, it is possible to manage them in [Inventory - Actions Menu - Manage Groups](#).

For more information on how to delete groups, see this [page](#).

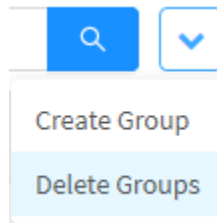
# Manage Groups - Delete Groups

In Blockbit GSM it is possible to delete device groups. Follow the steps below:

1. Select the group you want to delete by clicking on the checkbox [ ☐ ];

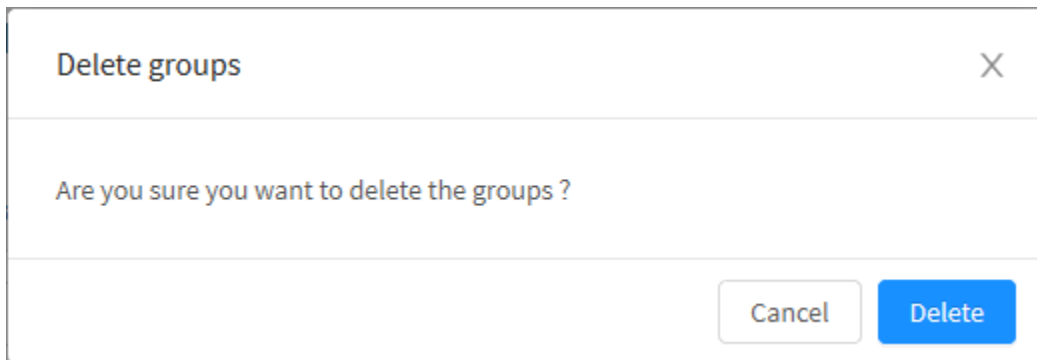
2. Click on the Actions Menu icon [  ];

3. Click on the "Delete Groups" option;

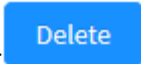
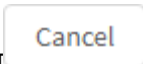



*Inventory – Actions Menu – Delete Groups.*

4. A confirmation message will appear, verifying if you want to delete the selected group:



*Inventory - Delete groups message.*

Click the [  ] button or click [  ] to return to the previous panel.

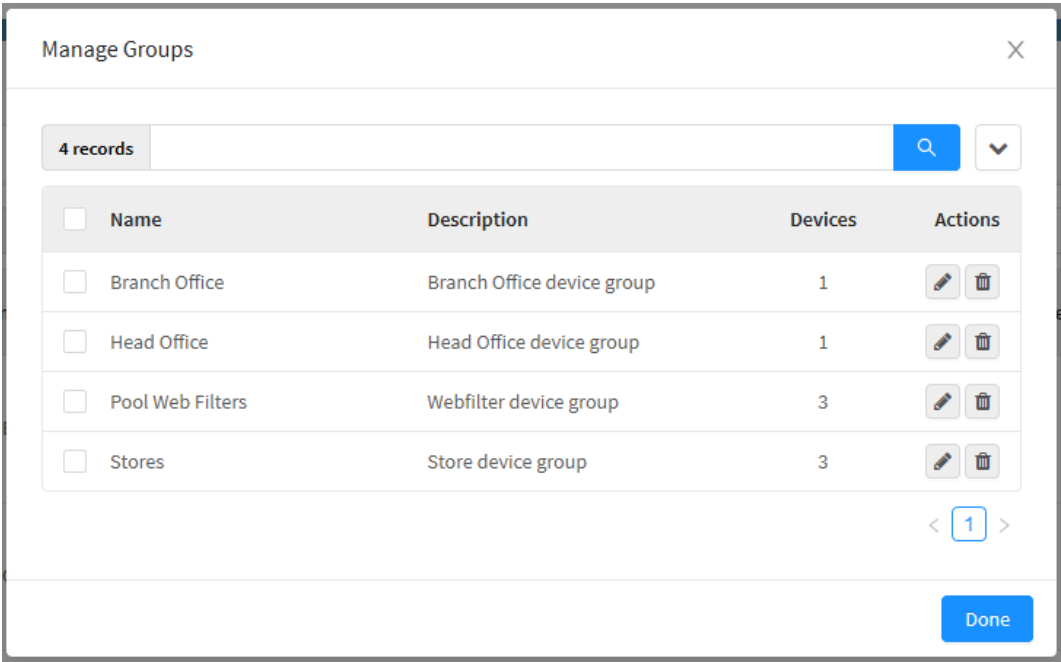
 **Group deleted successfully**  
*Group deleted successfully*

The group has been successfully removed.

Next we will analyze the components of the [columns](#).

# Manage Groups - Columns

In the following we will explain each column of the Manage Groups window:



Manage Groups - Columns

In the following we will explain each column:


- **Checkbox** [ ☐ ]: Select the group.
- **Name**: Displays the name of the registered group;
- **Description**: Displays the description of the registered group;
- **Devices**: Number of devices registered in the group;
- **Actions**: The "Actions" column consists of two buttons:
  - **Edit** [ ]: Edit registered group data;
  - **Delete** [ ]: Removes the group.

Click the [ ] button in the upper right corner or [ ] to close this window.

For more information on how to create a device, see this [page](#).

# Inventory - Actions menu - Create Device

For the integration of Blockbit GSM and Blockbit UTM it is necessary to register the devices.




The registration of devices must be carried out in the following order: first in Blockbit GSM and later in Blockbit UTM.

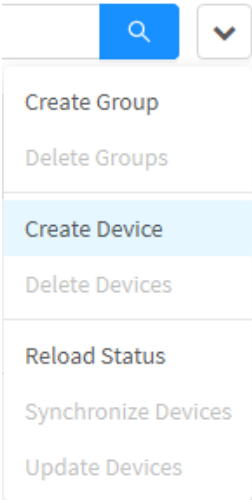
At this moment we will perform the registration of the devices. To register, it is necessary to access the Blockbit GSM Web Interface and the Blockbit UTM Web Interface. In order to facilitate understanding, a reference in bold and underlined with the name of the interface on which we are working will be described before the step-by-step begins:

**Blockbit GSM Web Interface:**

- 1. As previously mentioned, in the vertical menu on the left, initially, click on the "Devices" button and the "Inventory" tab will open automatically;



- 2. Click the Actions Menu icon [  ];
- 3. Click on the "Create Device" option;



Inventory - Actions menu - Add Device

- 4. The add device screen will appear, fill in the following fields on the "Create device" screen:

Add Device
X

\* Name

\* Company

\* Deploy Key

\* API Key

\* User Admin

Password

Device Group

Logger

Description

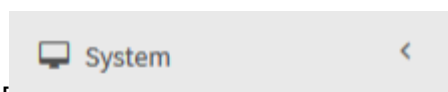
Cancel
Save

Inventory – Add Device

On this screen there are two pieces of information that were not mentioned in the previous session, they must be obtained from the Blockbit UTM Web Interface. This information are: Deploy Key and API Key.

5. Access the Blockbit UTM Interface;

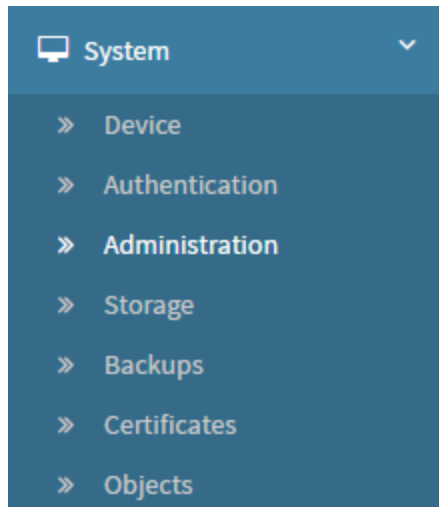
#### **Blockbit UTM Web Interface:**



6. Enter the **System Menu** [ ] located to the left of the interface;



7. Click the [ ] button;



Menu System – Administration

8. Click on the “Central Management” tab, the following interface will be displayed:

System - Administration menu - “Central Management” tab

9. Fill in the fields, as shown:


- **Enable Manager** ☒: Enables the integration module with Blockbit GSM;
- **Address**: Blockbit GSM IP Address or Hostname. Ex.: 172.16.102.235;
- **Deploy Service**: Communication port with Blockbit GSM, default value: 444;

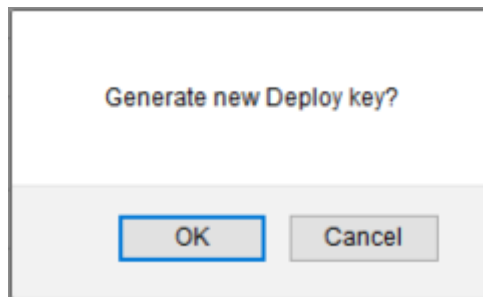


Communication is always initiated by the Blockbit UTM with the destination Blockbit GSM, on the TCP communication port 444 (Deploy port, configurable in the Blockbit GSM System Settings).

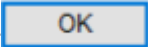


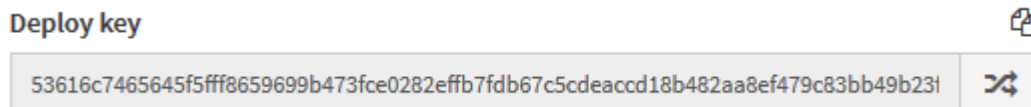
A Policy must be created allowing devices to communicate with Blockbit GSM on TCP port 444.

- **Administrator:** Selects the integration user that Blockbit GSM will use to manage Blockbit UTM. Ex.: admin;
- **Status:** Identifies the status of the communication with the Blockbit GSM. Ex.: *Offline*;
- **Deploy key:** Encryption key for communication between Blockbit UTM and Blockbit GSM. If this field is not filled out, follow the steps below:
  - To generate the “Deploy key”, click on the [  ] button. The message will appear if you want to generate a Deploy key;




Generate new deploy key

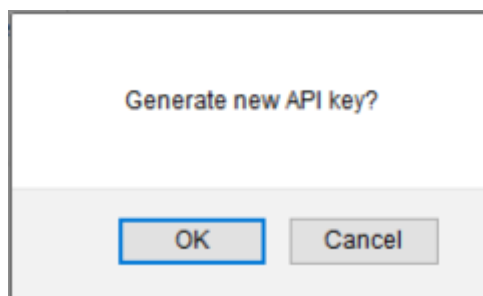
- Click the [  ] button. The system will generate the Deploy key, as shown below:



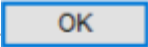
Deploy key


- **API Key:** Blockbit UTM user's cryptographic key, with administration and use permissions for the communication API with Blockbit GSM. If this field is not filled out, follow the steps below:


- To generate the API key, click on the [  ] button. The message will appear if you want to generate an API key;





Generate new API key.

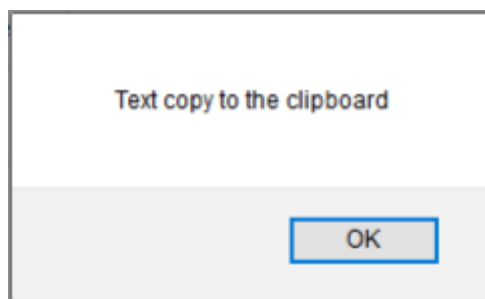
- Click the [  ] button. The system will generate the API key, as shown below:

API key


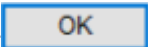
4f79bec38bd236558c5d6cb2000cd443


API key

- Click the [  ] button located in the upper right corner of the screen to save the settings;
  - Copy the Deploy key to insert in the Blockbit GSM. To copy the key, click on the Deploy Key **copy** [  ] button.
- The following message will appear:



Text copied to clipboard - Deploy Key

- Click the [  ] button.

After completing all fields, you will get the following result:

Settings
Administrators
Central Management
Audit Logs
Blocked Addresses

☒ Enable Manager

☐ Enable updates from centralized repository

Manager Address
172.31.102.235


Deploy Service
444


Administrator
admin


☐ Enable Analyzer


Analyzer Address
IP/Host

Logger Service
555

Status
Online


Deploy key
53616c7465645f548975e49e0a6cdae00c6b0a39ffe537a7d58dff98ff81a0d07c828504c56e24


API key
3b5c5b110248be11cfce27152898fe9e


Status
Offline




Complete "Central Management" tab

12. Return to the Blockbit GSM Web Interface;

**Blockbit GSM Web Interface:**

13. In the "Add Device" panel, paste the Deploy Key in the correct text box;


**\* Deploy Key**

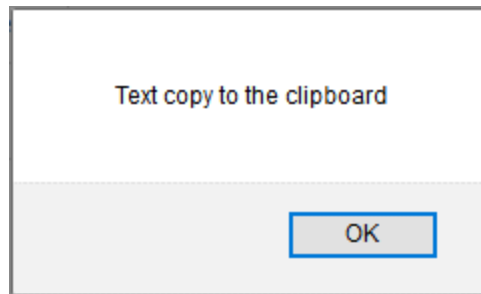
```
53616c7465645f5f1c6687a920f5d133009ea376bdb33e35327385c11b64d45fa43e6aa1d
eadf0b5e559a7c296aa6092039c0aae1ec9adb91263022d80a4339db3371a10a795c32f4
9450db14204810755cc8a8f1532658867e188df16323d33327fa80da20687dcf11db1c2a0
```

Add Device - Deploy Key

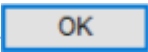
14. Return to the Blockbit UTM Web Interface;

**Blockbit UTM Web Interface**

15. Copy the API key to insert into the Blockbit GSM. To copy the key, click the **copy** [  ] button of the API key. The following message will appear:



Text copied to clipboard - API Key.

Click the [  ] button.

16. Return to the Blockbit GSM Web Interface;

**Blockbit GSM Web Interface:**

17. In the "Add Device" panel, paste the API key in the correct text box;

**\* API Key**

4f79bec38bd236558c5d6cb2000cd443

Add Device - API Key

18. Fill in the remaining data:

- **Name:** Enter the name that identifies the device in the Blockbit GSM. Ex.: *Cluster Head Office*;
- **Company:** Enter the name of the company that owns the Device. Ex.: Blockbit;
- **Model:** Select the device model. Ex.: *BB-10*;
- **User Admin:** Blockbit UTM user with administration permissions. It will be used when you want to access the Web Interface of Blockbit UTM through Blockbit GSM. Ex.: admin;
- **Password:** Blockbit UTM user password with administration permissions. If not entered, the password will be requested when accessing the device;
- **Device Group:** Select the group to which you want to add the device. Ex.: *Head Office*;
- **Logger:** It is an optional field, select from the drop-down list, which Logger will be used to generate reports. For more information, check the pages about [Loggers](#). Ex.: *Logger1*;



If you are using Logger Cluster, note that it is not possible to link a device to a logger that is not active in the cluster. For more information on how to activate manually, see this [page](#).

- **Description:** It is an optional field, type a description if necessary.

After completing all the fields, we will have arrived at a result similar to the one shown by the image below:

Add Device
X

\* Name
Cluster Head Office

\* Company
Blockbit

\* Deploy Key
53616c7465645f5f48975e49e0a6cdae00c6b0a39ffe537a7d58dff98ff81a0d07c828504c56e240bed6ece8fd5c1fbd0466bd27e2d2adc7321385449b0015329299005bd3ed6bb320f20729e4aa6ae15f0f1ed828b9287d1acec4fca0c9a2519077bd18c3888d686118434e5c0c

\* API Key
3b5c5b110248be11cfce27152898fe9e

Model
BB-5

\* User Admin
admin

Password
••••••••

Device Group
Head Office

Logger

Description
Head Office  
IP: 172.31.102.220  
Logger

Cancel Save


Inventory - Add Device - Example

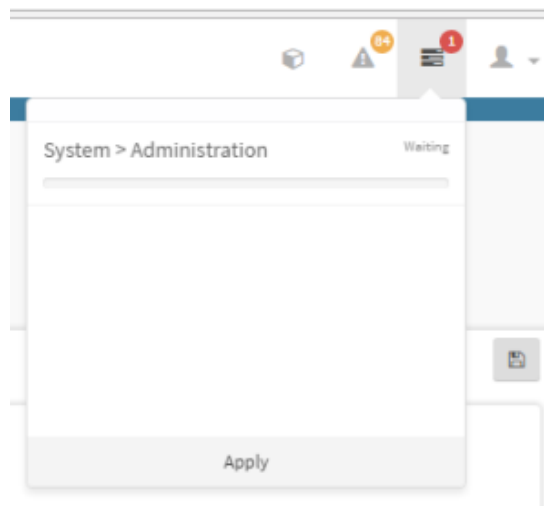
Click the [  ] button.

The device was successfully added, the Device Manager screen will appear;

19. Return to the Blockbit UTM Web Interface;

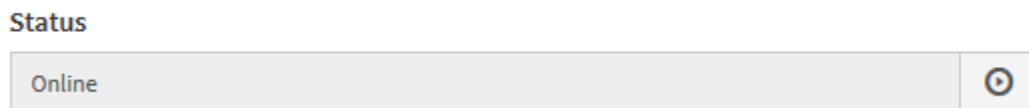
### **Blockbit UTM Web Interface**

20. Click the Saved settings queue icon [  ] to "Apply" the settings;



Saved settings queue

21. Click on the "Apply" button. Communication between Blockbit UTM and Blockbit GSM will be established and on the Central Manager screen, the Status field will be changed from "Offline" to "Online";




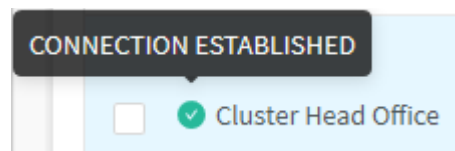
Status - Online

The device has been successfully registered with the Blockbit UTM.

22. Return to the Blockbit GSM Web Interface;

### **Blockbit GSM Web Interface**

23. On the Device Manager screen in front of the Device Name field, the online icon [  ] will appear in front of the name of the created device, informing that the communication was successfully established.



Inventory – Connection Established

If you want to register other devices, repeat the steps shown above. In our example, at the end of all necessary registrations, we will have an environment similar to this:

Devices

Inventory [Communities](#) [Templates](#) [Provisioning](#)

8 records

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/>	Branch Office	Branch Office	BBv-5	<span>52E9-BAA5-C79D-C644</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Branch Office			
<input type="checkbox"/>	Cluster Head Office	Head office	BBv-5	<span>8FD0-D18D-DA6C-D70C</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Head Office			
<input type="checkbox"/>	Webfilter 1	Pool Web Filters	BBv-5	<span>F31F-496F-FE20-FA27</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 2	Pool Web Filters	BBv-5	<span>908F-E203-843A-27EB</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Webfilter 3	Pool Web Filters	BBv-5	<span>FB47-AF24-21F0-4060</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Webfilter		Webfilter Policies	
<input type="checkbox"/>	Store 1	Stores	BBv-5	<span>B30D-8ED9-8C7D-943C</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Store		Store Policies	
<input type="checkbox"/>	Store 2	Stores	BBv-5	<span>719E-89F2-CCED-FBDF</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Store		Store Policies	
<input type="checkbox"/>	Store 3	Stores	BBv-5	<span>D92E-91C4-23B5-751A</span>	BLOCKBIT UTM 1.5.7 build 19072620	Device Store		Store Policies	


1 / 15 / page










## Device Manager - Registered Devices

Next, we'll look at how to [remove the devices](#).


# Inventory - Actions menu - Delete Devices


Through the actions menu it is possible to delete several devices at the same time. Follow the steps below:


1. Select the devices you want to delete by clicking on the checkbox [  ], located in the "Actions" column, on the right side of the trash can icon. Ex.: *Branch office 1*, *Cluster Head Office* and *Store 1*;

<input type="checkbox"/>	Name		
<input checked="" type="checkbox"/>	 Branch Office		
<input type="checkbox"/>	 Cluster Head Office		
<input checked="" type="checkbox"/>	 Webfilter 1		

Device Manager - Selected Devices

2. Click on the Actions Menu [  ];
3. Click on the "Delete Devices" option;





Create Group

Delete Groups

Create Device

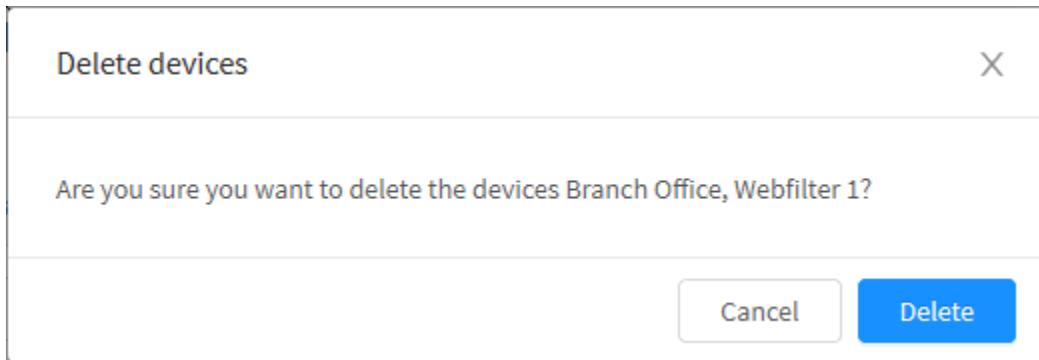
Delete Devices

Reload Status

Synchronize Devices

Update Devices

4. A screen will appear asking if you want to delete the selected device:

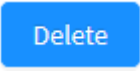
A modal dialog box titled "Delete devices" with a close button (X) in the top right corner. The main text asks, "Are you sure you want to delete the devices Branch Office, Webfilter 1?". At the bottom right, there are two buttons: "Cancel" and "Delete".


Delete devices

Are you sure you want to delete the devices Branch Office, Webfilter 1?

Cancel Delete

*Inventory – Delete Devices*


Click the [  ] button.

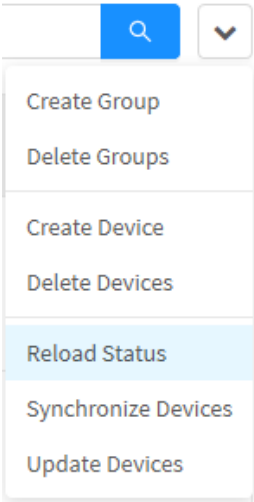
 **Device deleted successfully**  
*Device deleted successfully*

The devices have been successfully deleted.

# Inventory - Actions menu - Reload Status

Updates the status of all devices registered with GSM. To perform this operation, follow the steps:

- 1. Click on the **Actions Menu** [  ];
- 2. Click on the “Reload Status” option;



















Inventory - Actions menu - Reload Status

- 3. Wait for the panel to be available again:

Devices

Inventory Communities Templates Provisioning

8 records

Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
Branch Office	Branch Office	BBv-6	3259-BAA9-C78D-C644	BLOCKBIT UTM 1.8.7 build 19072820	Device Branch Office			 
Cluster Head Office	Head office	BBv-6	8F09-018D-046C-070C	BLOCKBIT UTM 1.8.7 build 19072820	Device Head Office			 
Webfilter 1	Pool Web Filters	BBv-6	F31F-486F-FE35-F427	BLOCKBIT UTM 1.8.7 build 19072820	Device Webfilter	Webfilter Policies		 
Webfilter 2	Pool Web Filters	BBv-6	908F-E203-843A-97E8	BLOCKBIT UTM 1.8.7 build 19072820	Device Webfilter	Webfilter Policies		 
Webfilter 3	Pool Web Filters	BBv-6	FB47-4F24-21F0-4960	BLOCKBIT UTM 1.8.7 build 19072820	Device Webfilter	Webfilter Policies		 
Store 1	Stores	BBv-6	830D-4ED9-4C7D-943C	BLOCKBIT UTM 1.8.7 build 19072820	Device Store	Store Policies		 
Store 2	Stores	BBv-6	718E-49F3-CC35-F8D8	BLOCKBIT UTM 1.8.7 build 19072820	Device Store	Store Policies		 
Store 3	Stores	BBv-6	D62E-41CA-28B9-783A	BLOCKBIT UTM 1.8.7 build 19072820	Device Store	Store Policies		 

10 / page


Inventory – Reload all devices

















After this step, the status will have been reloaded and displayed on the same panel.




# Inventory - Actions menu - Synchronize Devices

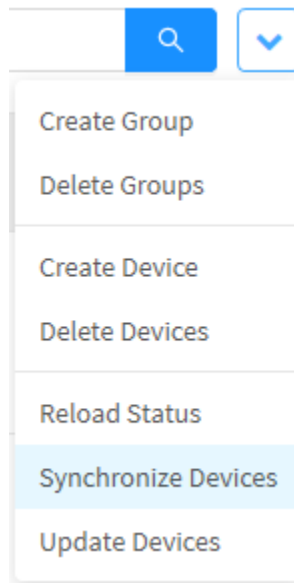
To synchronize the information of all devices registered with GSM, follow the steps:

1. Select the devices you want to delete by clicking on the checkbox , located in the "Actions" column, on the right side of the trash can icon. Ex.: *Branch office 1, Cluster Head Office* and *Store 1*;

	Name	Group
	 Branch Office	   Branch Off
	 Cluster Head Office	   Head Offic
	 Webfilter 1	   Pool Web I

Inventory - Device selected

2. Click on the Actions Menu ;
3. Click on the option "Synchronize Devices";



Inventory - Actions menu - Synchronize

All synchronizations will be successful.




Blockbit GSM automatically synchronizes information on ALL devices every 30 minutes.

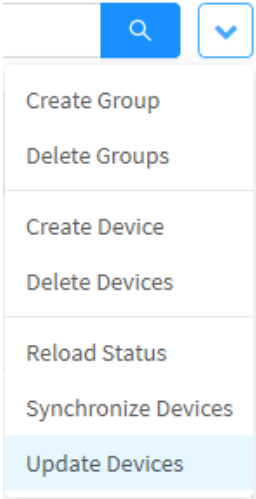
# Inventory - Actions menu- Update Devices

Performs the version update of the devices registered in the GSM. To perform this operation, follow the steps:

1. Select the desired devices by clicking on the desired ☐ check box;

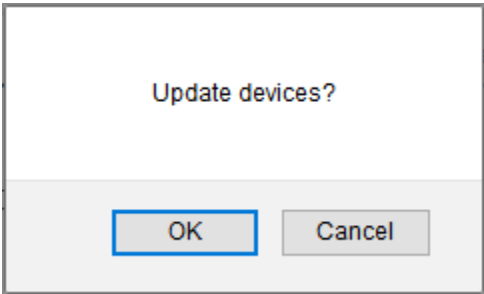
2. Click the Actions Menu ;

3. Click on the “Update Devices” option;



Inventory - Actions menu - Update Devices

4. The verification message will appear:



Update devices

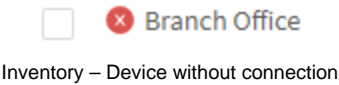
5. To update the selected devices, click , otherwise click .

# Inventory - "Name" column

The "Name" column shows the devices that were previously registered, ordered in their respective groups.

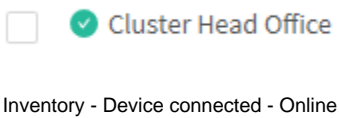
Next to the name of each registered device there is a symbol that indicates the status of the connection between Blockbit GSM and Blockbit UTM.

If the red symbol is flagged, it means that that device is not connected:



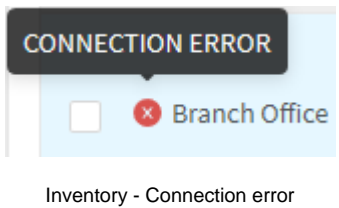
Inventory – Device without connection

If the green symbol is flagged, it means that that device is connected correctly:

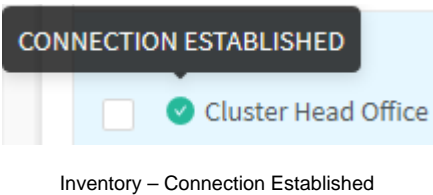


Inventory - Device connected - Online

If you want to check the status, just place the mouse over the status button for a message to be displayed:






Inventory - Connection error



Inventory – Connection Established

# Inventory - Action buttons

Also in the Device Name Column, just to the right of the device name, there are three action buttons: **Access CLI** (Command Line Interface) [  ], **Access Interface Web** [  ] and **Synchronize** [  ]:



Action buttons - Device Name.

Next we will be presenting each one of them.

- [Access CLI](#);
- [Access Interface Web](#);
- [Synchronize](#).


# Inventory - Action button - "Access CLI"

The "Access CLI" action button - Command Line Interface: accesses the text interface (shell) through the existing connection with the Blockbit GSM:



Access CLI button - Command Line Interface



Click the **Access CLI** [  ] button. It will open a new tab in the browser to access the interface via the shell.

# Inventory - Action button - "Access Interface Web"

The "Access Interface Web" action button accesses the device's web interface through the existing connection with the Blockbit GSM, that is, opens a tab in the browser to directly access the desired Blockbit UTM:



"Access Interface Web" button



Blockbit UTM can also be accessed directly from the device's IP address on TCP port 98. Ex.: <https://172.16.102.220:98>

Clicking on the "Access Interface Web" button may cause a browser pop-up. If it does, a red symbol will appear warning you that the pop-up is blocked in the upper right corner of the browser screen:



"Access Interface Web" button - Pop-up blocked

It is necessary to unblock. To do this, follow the steps:

1. Click on the pop-up blocking button located in the upper right corner of the browser;
2. The pop-up unlock screen will appear;
3. Click on the "Allow" button.

Unlock was successful. To proceed, click on the "Access Interface Web" button again. It will open a new tab in the browser with access to Blockbit UTM.

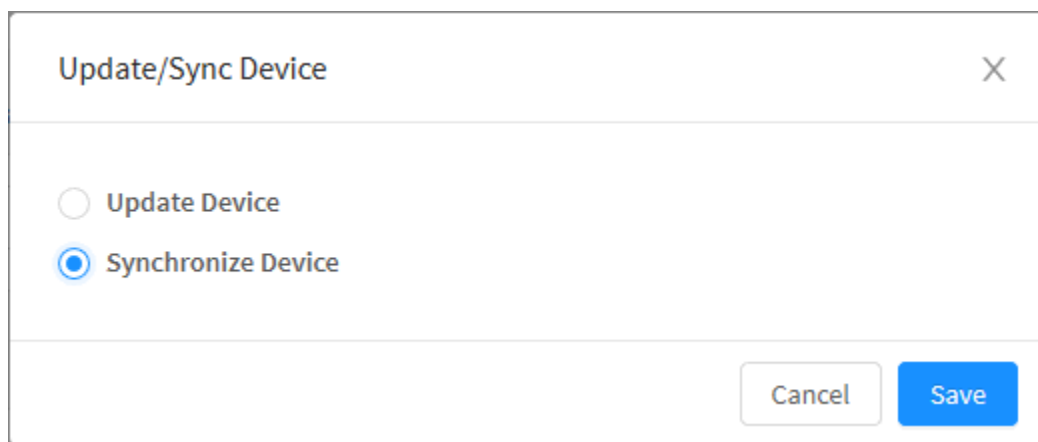
# Inventory - Action button - "Update / Synchronize"

The "Update / Synchronize" action button allows you to synchronize or update the device:



"Update / Synchronize" button

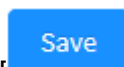
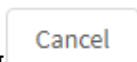
By clicking the **Update/Synchronize**  button. The following window will appear:

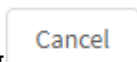
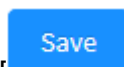
A dialog box titled "Update/Sync Device" with a close button (X) in the top right corner. It contains two radio button options: "Update Device" (unselected) and "Synchronize Device" (selected). At the bottom right, there are two buttons: "Cancel" and "Save".

Update/Sync Device

Next, we'll look at both options:

- **Update:** This option has the function of updating the device to the most current version available. Ex.: A UTM 14.6 being upgraded to a UTM 1.5.2;
- **Synchronize:** The function of this option is to synchronize the information of the device in question with the "Device Manager" tab, allowing the display of the License Status, version and several other information;



If you want to cancel click on the [  ] button. When clicking on the [  ] button the update or synchronization will be carried out.

Synchronization and update were successful.












# Inventory - "Group" column

The "Group" column shows the registered device groups.

Group
Branch Office
Head Office
Pool Web Filters

Inventory – Group

When you click on one of the groups, all appliances categorized with the group clicked will be displayed, as shown below:

3 records		group:"Stores"	
<input type="checkbox"/>	Name	Group	
<input type="checkbox"/>	✔ Store 1	  	Stores
<input type="checkbox"/>	✔ Store 2	  	Stores
<input type="checkbox"/>	✘ Store 3	  	Stores

*Inventory – Group - Selected*

If the group is clicked again, the previous screen will be displayed again.

For more information, regarding device groups, check [Inventory - Actions Menu - Manage Groups](#).

# Inventory - "Model" column













The "Model" column shows the models of the registered devices.

Model
BBv-1
BBv-5
BBv-10

Inventory – Model

When you click on one of the models, all the appliances of the clicked model will be displayed, as shown below:

# Devices

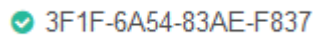
Inventory					Communities					Templates					Provisioning				
8 records					model:"BBv-5"														
<input type="checkbox"/>					Name					Group					Model				
<input type="checkbox"/>					 Branch Office					   Branch Office					BBv-5				
<input type="checkbox"/>					 Cluster Head Office					   Head office					BBv-5				
<input type="checkbox"/>					 Webfilter 1					   Pool Web Filters					BBv-5				

Inventory - Model - Selected

If the model is clicked again, the previous screen will be displayed again.





# Inventory - "License Status" column

The "License Status" column displays information regarding licenses such as: License status and license serial number.



License Status - License Number

The status icons that can be displayed are:


- **Active** : Displays whether the license is active or inactive and its respective activation date (Begin) and expiration (End);
- **Unknown** : Identifies that the license status is unknown. If a license is already active and this icon continues to appear, it is recommended to perform a [sync](#);
- **Expired** : Demonstrates that the license has expired. To reactivate it, contact Blockbit;
- **Inactive** : Demonstrates that the license is inactive.

# Inventory - "Version" column

The "Version" column shows the version information and firmware updates installed on the device. Ex.: *Blockbit UTM 1.3.0 build 17022114*.

Version
BLOCKBIT UTM 1.5.7 build 19072820
BLOCKBIT UTM 1.5.7 build 19072820
BLOCKBIT UTM 1.5.7 build 19072820

Inventory – Version



Access to Blockbit GSM allows you to manage devices in different firmware versions, however, it is highly recommended to always use the latest and most up-to-date version available.

For more information about the Blockbit GSM update process, check [System - "Update" tab](#).

# Inventory - "Template" column

The "Template" column displays the name of the settings template applied to the device.

Template
Device Branch Office
Device Head Office
Device Webfilter
Device Webfilter

Inventory – Devices Template

For more information about device templates, check the [Templates tab](#).

# Inventory - "Policy IPv4" column

The "IPv4 Policy" column displays the name of the IP policy package applied to the device. Ex.: Policies Branch Office.

Policy IPv4
Store Policies
Store Policies
Store Policies

Inventory – Policy IPv4

For more information, check the [Policies](#) section.



# Inventory - "Policy IPv6" column

The "IPv6 Policy" column displays the name of the policy package applied to the device.

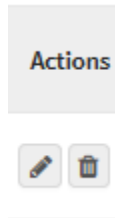
Policy IPv6
Webfilter Policies
Webfilter Policies

Inventory – Policies Head Office

For more information, check the [Policies](#) section.

# Inventory - "Actions" column

The Actions column displays the "Edit" and "Delete" buttons for each device.




Inventory - "Edit" and "Delete" buttons

Next, we will analyze the function of both buttons:

- [Edit button](#);
- [Delete button](#).

# Inventory - "Actions" column - "Edit" button

Using the **Edit**  button, it is possible to edit the device information created in the [Inventory - Actions menu - Create Device](#) or the selected group:

1. Determine which item you want to edit;


2. Click the **Edit**  button;


3. Edit the information you want;

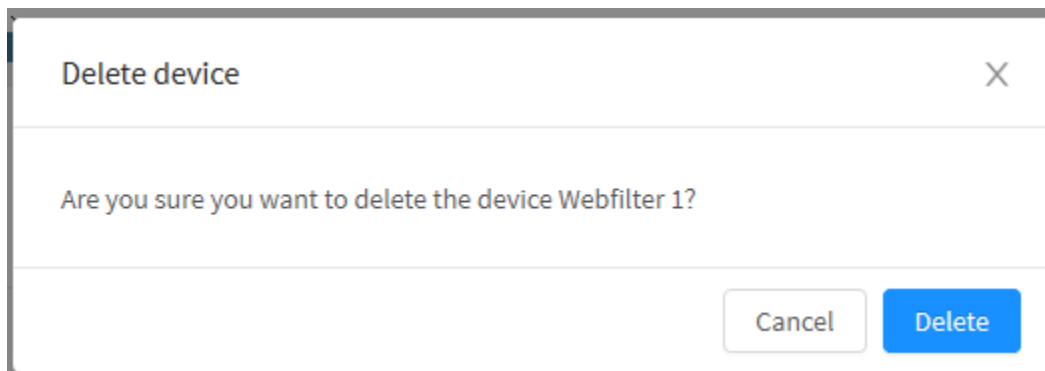
4. *If you want to cancel the changes made, click the [  ] button.* To complete the edited changes, click the [  ] button.

The edits were successful.

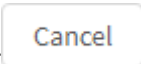
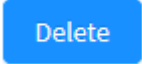
# Inventory - "Actions" column - "Delete" button


Through the **Delete**  button, it is possible to remove the registered device or group.

1. Determine which item you want to delete;
2. Click the **Delete**  button;
3. A screen will appear asking if you want to delete the selected item:



Inventory – *Delete device.*

If you want to cancel click on the  button. To complete the removal, click the  button.

 **Device deleted successfully**  
*Device deleted successfully*

The removal was successful.

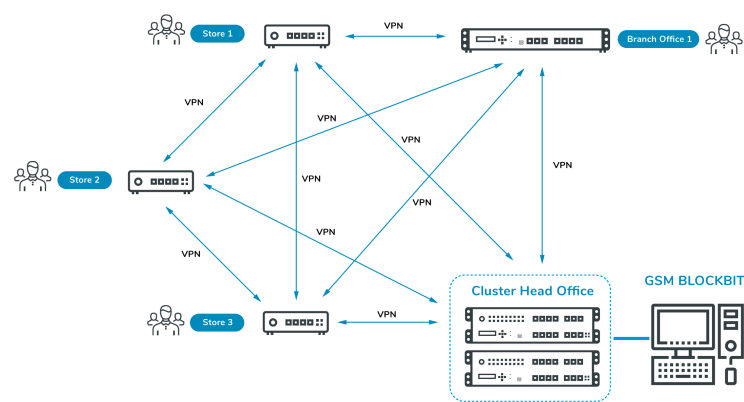
# Communities Tab

This section will demonstrate how to create VPN - Virtual Private Network communities on Blockbit GSM. These settings allow secure, fast and encrypted communication to occur between devices.

Blockbit GSM allows you to configure two topology modes to create communities: Full Meshed and Star:

- **Full Meshed:** All devices establish communication with each other. The following is the example of the Full Meshed Topology:

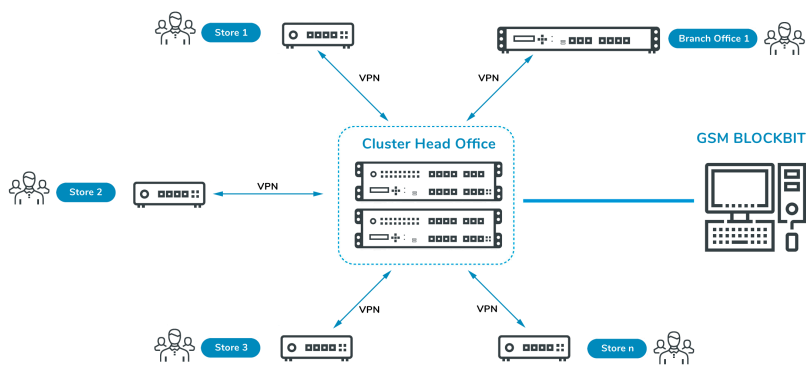
## Device Communities Topology Full Meshed



Device - Communities – Topology Full Meshed

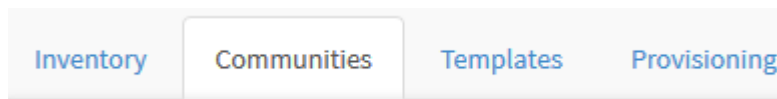
- **Star:** All devices establish communication with a HUB (usually the company's headquarters), and this allows communication between devices, however, in a controlled manner. The following is an example of Star Topology.

## Device Communities Topology Star



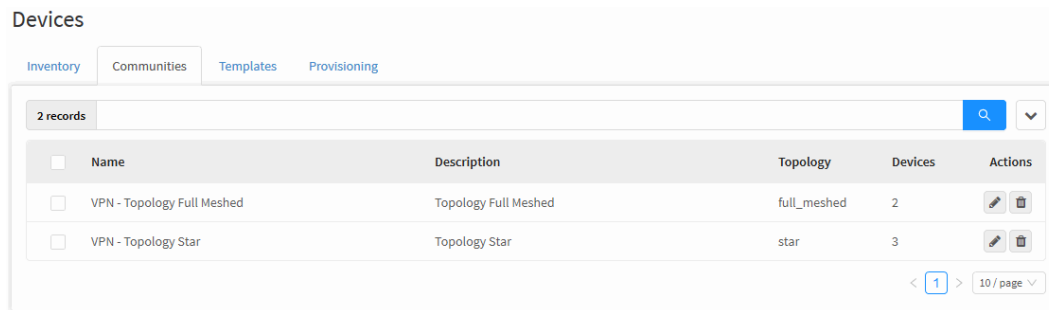
Device - Communities – Topology Star

To access the Communities screen, click on the tab as shown below.



Communities tab

The Communities Screen will appear. It consists of five columns: "Name", "Description", "Topology", "Devices" and "Actions". In addition, the [search bar](#) is located at the top of the screen and in the upper right corner of the screen is the [actions menu](#).



Devices - Communities

This section will demonstrate how:

- [Create](#) and [delete](#) VPN communities;
- [Add](#) and [remove](#) devices to VPN communities;
- Etc.

In the following we will explain each component of this panel.

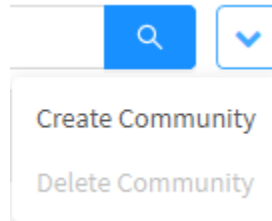
# Communities - Actions menu

At the top right of the screen we have the actions menu:



Communities - Actions Menu button

By clicking on this button the menu below is displayed:



Communities - Actions menu


The menu consists of the following options:

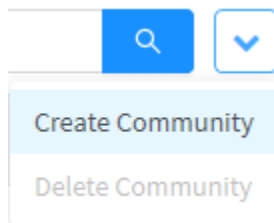
- [Create Community](#);
- [Delete Community](#).

Next, each option in the action menu will be detailed.

# Communities - Actions menu - Create Community

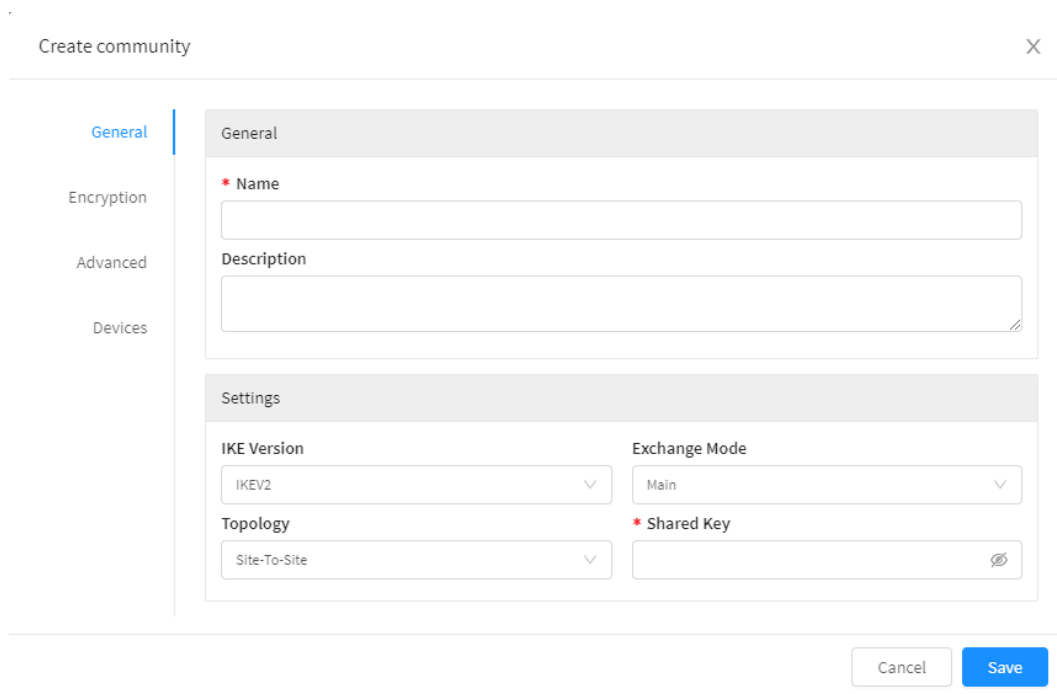
To create Community, follow these steps:

1. Click on the **actions menu** [  ];
2. Click on the "Create Community" option;



Communities - Actions menu - Create Community

3. The "Create Community" panel will be displayed. With the "General" side flap pre-selected.

A screenshot of a web application window titled 'Create community'. The window has a close button (X) in the top right corner. On the left side, there is a vertical sidebar with four tabs: 'General' (selected and highlighted in blue), 'Encryption', 'Advanced', and 'Devices'. The main content area is divided into two sections. The top section is titled 'General' and contains two text input fields: 'Name' (marked with a red asterisk) and 'Description'. The bottom section is titled 'Settings' and contains four fields: 'IKE Version' (a dropdown menu with 'IKEV2' selected), 'Exchange Mode' (a dropdown menu with 'Main' selected), 'Topology' (a dropdown menu with 'Site-To-Site' selected), and 'Shared Key' (marked with a red asterisk, with a copy icon to its right). At the bottom right of the window, there are two buttons: 'Cancel' and 'Save'.

Communities – Create Community - General

The "Create community" panel is made up of tabs:

- [General](#);
- [Encryption](#);
- [Advanced](#);
- [Devices](#).

Next, we'll look at the "[Create community](#)" panel in detail.



# Communities - Actions menu - Create Community - General

In the “General” section there are the following fields:

- **Name:** Device Community name. Ex.: VPN – *Topology Full Meshed*;
- **Description:** Description of Device Community. Ex.: *FULL MESHED*.

In Settings, the fields below are displayed:

- **IKE Version:** Determines the version of IKE that will be used;
- **Exchange Mode:** IKE key negotiation method;
- **Topology:** Defines which topology is chosen in the Topology field. Ex.: *Site-To-Site*;
- **Shared Key:** It is a key shared between the devices. This key is used in the authentication process by the IKE protocol. Ex.: “q1Q!q1Q!”. To view the key entered, click the view [👁] icon.

Create community

X

General

Encryption

Advanced

Devices

General

\* Name

Description

Settings

IKE Version

IKEV2

Exchange Mode

Main

Topology

Site-To-Site

\* Shared Key

Cancel

Save

Communities – Create Community - General

# Communities - Actions menu - Create Community - Encryption

The side tab "Encryption" is divided into two panels: "Phase 1 (IKE)" and "Phase 2 (ESP)".

In "Phase 1 (IKE)" the following fields are displayed:

- **Encryption Algorithms:** Determines which encryption algorithm will be used by the VPN community;
- **Authentication Algorithms:** Determines the authentication algorithm that will be used by the VPN community;
- **Diffie-Hellman (DH) Group:** Determines the level of complexity in the exchange of keys, the higher the value of the Diffie-Hellman Group, the greater the level of security but the more time it takes to process the key.

In "Phase 2 (IKE)" the following fields are displayed:

- **ESP Encryption Algorithms:** Determines which encryption algorithm for the ESP protocol will be used by the VPN community;
- **ESP Authentication Algorithms:** Determines the authentication algorithm of the ESP protocol that will be used by the VPN community;
- **Perfect Forward Secrecy (PFS) Group:** Determines the level of complexity in the exchange of keys, the higher the value of the Perfect Forward Secrecy Group, the greater the level of security but the more time it takes to process the key.

Create community

General

Encryption

Advanced

Devices

Phase 1 (IKE)

Encryption Algorithms

aes256

Authentication Algorithms

sha256

Diffie-Hellman (DH) Group

DH Group 2: 1024-bit group

Phase 2 (ESP)

ESP Encryption Algorithms

aes256

ESP Authentication Algorithms

sha256

Perfect Forward Secrecy (PFS) Group

PFS Group 2: 1024-bit group

Cancel

Save

Communities – Create Community - Encryption.

# Communities - Actions menu - Create Community - Advanced

Follow the fields displayed in the "Advanced" tab:

The screenshot shows the 'Create community' dialog box with the 'Advanced' tab selected. The 'Advanced' tab contains the following settings:

- IKE lifetime (s):** 28800
- Key lifetime (s):** 3600
- Keying Tries:** 5
- Rekey margin (s):** 5
- DPD Action:** Restart (dropdown menu)
- DPD delay (s):** 101
- DPD timeout (s):** 30
- Re-Auth:** ☐
- Fragmentation:** ☐
- Compression:** ☐
- NAT-T:** ☐

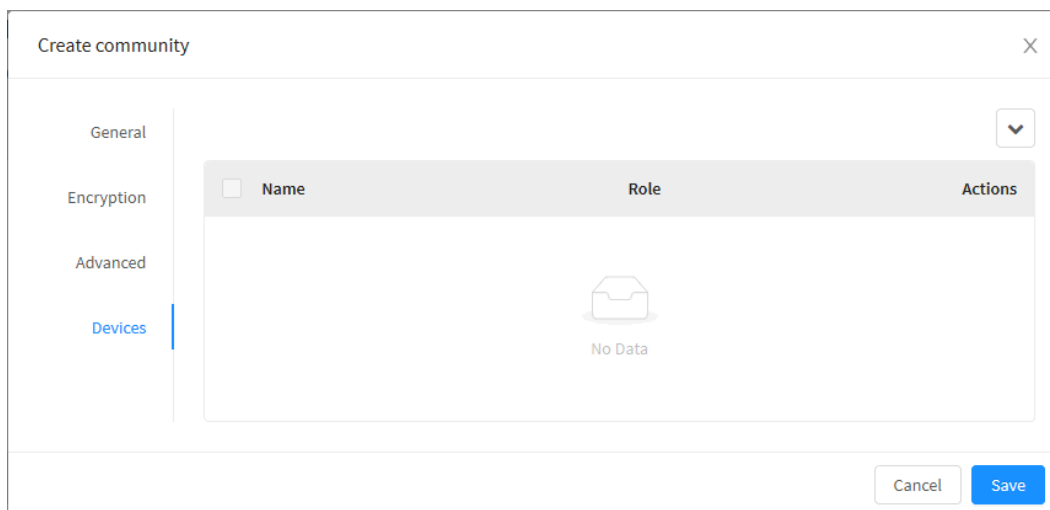
At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Communities – Create Community - Advanced.

- **IKE lifetime (s):** Determines the lifetime that the protocol will wait to renegotiate the SA, is determined in seconds;
- **Key lifetime (s):** Determines the validity time of the successful negotiation key, is determined in seconds;
- **Keying Tries:** This is the number of times that the VPN points will renegotiate the tunnel or try to re-authenticate after the key expires;
- **Rekey margin (s):** Determines how long before the connection expires the VPN points and initiates the renegotiation of the tunnel keys;
- **DPD Action:** Controls the use of the lost VPN points detection protocol. Follows the operation of each option:
  - The "Clear" action closes, or closes the connection without taking any previous steps;
  - The "Hold" action sets up a strategic policy that captures traffic and tries to renegotiate the connection on demand;
  - The action "Restart" immediately initiates an attempt to renegotiate the connection;
  - The default is "None" or none, disables automatic sending of DPD messages.
- **DPD delay (s):** Defines the time interval or period in which informational IKE v1 and IKE v2 exchange messages are sent to VPN points. It is determined in seconds;
- **DPD timeout (s):** Sets the timeout interval for sending messages to IKE v1 after all connections to a VPN point are lost in the event of inactivity. It is determined in seconds;
- **Re-Auth [ ☐ ]:** This check box allows you to enable the reauthentication process. This feature has the function of renegotiating the IKE keys and checking the validity of the credentials, if this check box is disabled, the connection will remain active even if the certificate has expired;
- **Fragmentation [ ☐ ]:** By enabling this checkbox, very long IKEv2 messages are fragmented into a set of smaller messages, which in turn are individually encrypted;
- **Compression [ ☐ ]:** This checkbox enables the use of the IPComp protocol to compress the contents of IP packets in conjunction with IPsec encryption;
- **NAT-T [ ☐ ]:** Enable the NAT-T (NAT Transversal) item if one of the VPN sites is behind an address translation (NAT) server "Firewall".



# Communities - Actions menu - Create Community - Devices

In the "Devices" tab, the following fields are displayed:



Name	Role	Actions
No Data		

Communities – Create Community - Devices.

- **Name:** Where the device name is displayed;
- **Role:** Where the role of the device used by the VPN is displayed, it can be Hub or Spoke;
- **Actions:** In this column there are two action buttons:
  - **Edit** : This button allows you to edit and edit the settings of the devices added in the [Add device](#) option of the actions menu;
  - **Delete** : This button removes the device.



**ATENÇÃO:** When adding devices, if one of them is configured as a hub, a [site-to-site Star](#) topology will automatically be created. However, if all devices are configured as spoke, a [site-to-site full-meshed](#) topology will be automatically created.

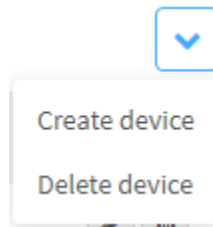
# Communities - Actions menu - Create Community - Devices - Actions menu

At the top right of the screen we have the actions menu:



Devices - Actions menu button

By clicking on this button the menu below is displayed:



Devices - Actions menu


The menu consists of the following options:

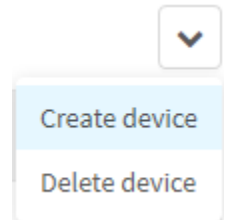
- [Create device](#);
- [Remove devices](#).

Next, each action menu option will be detailed.

# Communities - Actions menu - Create Community - Devices - Actions menu - Create device

To add a new device. Follow the steps below:

1. Click the Action Menu [  ] button:



*Devices - Create Device*

2. Click on the **Create Device** option, the following window will be displayed:

Create Device

X

\* Device

\* Local Host

\* Local ID

Network

+

^

▼

-

Role

Hub

▼

☐ Dynamic


Cancel

Save

Device - Create Device

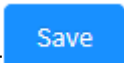
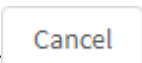
- **Device:** Select the desired device from the list. Ex.: Store 1;
- **Local Host:** Communication address of the LOCAL VPN point to establish the tunnel. It must be identified by: "IP address" or "Hostname (FQDN)". Ex.: 172.31.102.222;
- **Local ID:** IP address of the selected device used to establish the VPN. Ex.: 172.31.102.222;

- **Networks:** This text field allows adding networks to the list. Click [  ] to add the selected item. If you have entered the wrong item, select

the item and click [  ] to remove it from the list. In this list are located the local networks of the selected device that will be accessible to other devices after the establishment of the VPN. Ex.: 172.31.102.0/24;

- **Role:** It is the role of the device used by the VPN, it can be Hub or Spoke. Ex.: Hub;

- **Dynamic** ☐: When activating the checkbox the IPs of the eth interfaces of the UTM's members of this community will be dynamic.

Click [  ] to register the device or click [  ] to close this panel.



Device added successfully

*Device added successfully*

After these steps the devices will have been successfully added.







To add the other devices, repeat the steps above. After adding all devices we will have the following screen:

General

Encryption

Advanced

Devices

<input type="checkbox"/>	Name	Role	Actions
<input type="checkbox"/>	Store 1	hub	 
<input type="checkbox"/>	Store 2	spoke	 
<input type="checkbox"/>	Store 3	spoke	 

Device - Added Devices



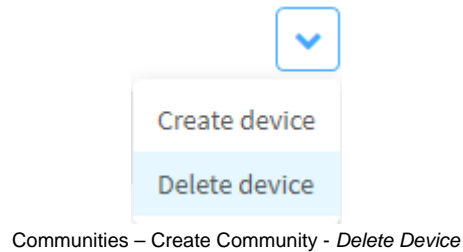
# Communities - Actions menu - Create Community - Devices - Actions menu - Delete device

To delete devices. Follow the steps below:

1. Select the device you want to delete by clicking on the **selection** ;

2. Click on the **Actions Menu**  icon;



3. Click on the "Delete Devices" option;

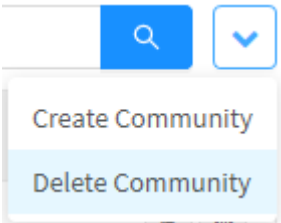


If you want to remove a device just click on the checkbox and select all the desired devices and in the action menu click on "Delete device".

# Communities - Actions menu - Delete Community

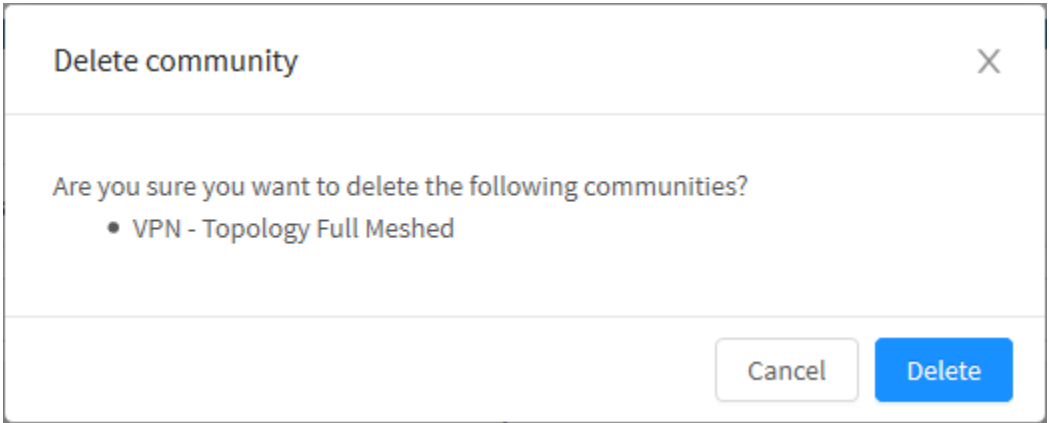
To delete communities. Follow the steps below:

- 1. Select the community you want to delete by clicking on the **selection** [  ];
- 2. Click on the **Actions Menu icon** [  ];
- 3. Click on the "Delete Community" option;

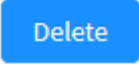
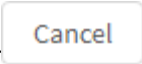


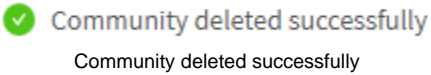
Communities – Menu de ações – Delete Community.

- 4. A confirmation message will appear, verifying if you want to delete the selected community:



Communities - Delete community.

Click the [  ] button or click [  ] to return to the previous panel.



The community has been successfully removed.

# Communities - Columns

In the following we will explain each column of the Communities tab:

Devices

InventoryCommunitiesTemplatesProvisioning



2 records

<input type="checkbox"/>	Name	Description	Topology	Devices	Actions
<input type="checkbox"/>	VPN - Topology Full Meshed	Topology Full Meshed	full_meshed	2	<div><div></div><div></div></div>
<input type="checkbox"/>	VPN - Topology Star	Topology Star	star	3	<div><div></div><div></div></div>

<1>

10 / page

Communities

- **Select** [ ☐ ]: Allows you to select a community.
- **Name**: Displays the name of the registered Community;
- **Description**: Displays the description of the registered Community;
- **Topology**: Displays the type of registered topology;
- **Devices**: Displays the number of devices within the Community;
- **Actions**: Provides the following essential actions:
  - **Edit** [  ]: Allows you to edit the community settings added in the [Create Community](#) option of the actions menu;
  - **Delete** [  ]: Lets you remove a community.

# Communities - Communities Examples

Next, we will exemplify the registration of some device communities in order to demonstrate in practice how GSM automatically creates VPN topologies on devices:

We will carry out the demonstration using the following topologies:

- [Topology Star](#);
- [Topology Full-Mesh](#).

We will start the examples with the star topology:

## Topology Star

This demonstration will take into account the following structure:

*Topology Star - IP addressing*

Device	IP	Papel
UTM204	204.204.204.0	Hub
UTM206	206.206.206.0	Spoke
UTM8	108.108.108.0	Spoke

Before creating communities, in Inventory [add the Devices](#) according to their structure, in this example we will use:

Devices

InventoryCommunitiesTemplatesProvisioning

3 records

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/>	<div><div>UTM204</div></div>	<div><div></div><div></div><div></div></div> No Group	BBv-100	<div><div></div><div>4336-D46C-5D19-B506</div></div>	BLOCKBIT UTM 2.0.6 build 20102607		Policies 2.0 IPv4	Policies 2.0 IPv6	<div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>UTM206</div></div>	<div><div></div><div></div><div></div></div> No Group	BBv-1000	<div><div></div><div>E593-8A8D-F033-C4AA</div></div>	BLOCKBIT UTM 2.0.6 build 20102607			Policies 2.0 IPv6	<div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>UTM8</div></div>	<div><div></div><div></div><div></div></div> No Group	BBv-5	<div><div></div><div>E828-E23A-BFF0-44A5</div></div>	BLOCKBIT UTM 1.5.14 build 20102611		Policies 1.5 IPv6		<div><div></div><div></div></div>

<1>10 / page

Example - Devices Tab

Back in the communities tab, [create a new community](#) and configure it, as shown below:

Edit community

X

General

Encryption

Advanced

Devices

General

\* Name

Device Community

Description

Device Community

Settings

IKE Version

IKEV2

Exchange Mode

Main

Topology

Site-To-Site

\* Shared Key

...

Cancel

Save

Example - Create Community

- **Name:** Device Community;
- **Description:** Device Community;
- **IKE Version:** IKEV2;
- **Exchange Mode:** Main;
- **Topology:** Site-to-site;
- **Shared Key:** q1Q!q1Q!.

The settings on the side tabs Encryption and Advanced will remain the same. Select the [Devices](#) tab and create the Hubs and Spokes as shown:

## UTM204

Configure the UTM204 device as a Hub, as shown below:

Edit Device

X

\* Device

UTM204

\* Local Host

204.204.204.0

\* Local ID

204.204.204.0

Network

+

192.168.204.0/24

^

↓

-

Role

Hub

↓

☐ Dynamic

Cancel

Save

Example - Create Community - Create Device

- **Device:** UTM204;
- **Local Host:** 204.204.204.0;
- **Local ID:** 204.204.204.0;
- **Network:** 192.168.204.0/24;
- **Role:** Hub.

## UTM206

Configure the UTM206 device as a Spoke, as shown below:

Edit Device

X

\* Device

UTM206

\* Local Host

206.206.206.0

\* Local ID

206.206.206.0

Network

+

192.168.206.0/24

^

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

Save

Example - Create Community - Create Device

- **Device:** UTM206;
- **Local Host:** 206.206.206.0;
- **Local ID:** 206.206.206.0;
- **Network:** 192.168.206.0/24;
- **Role:** Spoke.

## UTM8

Configure the UTM8 device as a Spoke, as shown below:

Edit Device

X

\* Device

UTM8

\* Local Host

108.108.108.0

\* Local ID

108.108.108.0

Network

+

192.168.108.0/24

^

1

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

Save

Example - Create Community - Devices - Create Device

- **Device:** UTM8;
- **Local Host:** 108.108.108.0;
- **Local ID:** 108.108.108.0;
- **Network:** 192.168.108.0/24;
- **Role:** Spoke.

After these steps, we will arrive at this result:



Edit community

General

Encryption

Advanced

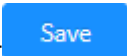

Devices

Name	Role	Actions
UTM204	hub	
UTM206	spoke	
UTM8	spoke	

Cancel

Save

Example - Create Community - Devices

Finally, click , *install package* and *deploy*. Then, access the IP of one of the Spokes or in Inventory click on the icon .

Devices

Inventory

Communities

Templates

Provisioning

4 records

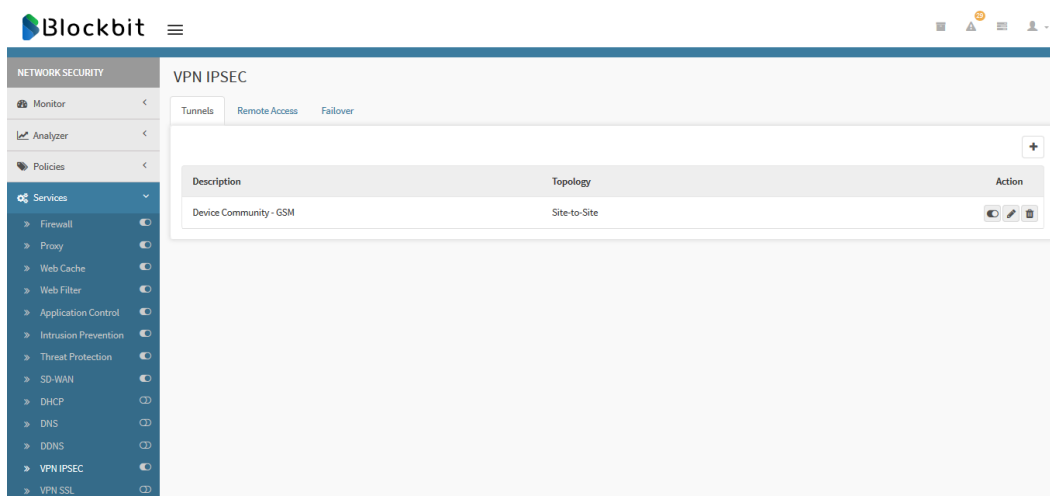
Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
UTM14	No Group	-	8F97-46F9-C2D3-7422	BLOCKBIT UTM 1.5.14 build 20102611	Template 1.5	Políticas 1.5 IPv4		
UTM204	No Group	BBv-100	4336-D46C-5D19-B506	BLOCKBIT UTM 2.0.6 build 20102707	Template 2.0	Políticas 2.0 IPv4	Políticas 2.0 IPv6	
UTM206	No Group	BBv-1000	E593-8A8D-F033-CA4A	BLOCKBIT UTM 2.0.6 build 20102707			Políticas 2.0 IPv6	
UTM8	No Group	BBv-5	E828-E23A-BFF0-44A5	BLOCKBIT UTM 1.5.14 build 20102611		Políticas 1.5 IPv4		

< 1 >

10 / page

Exemplo - Inventory - Connect

At UTM, access the Services menu, click on the IPSEC VPN option.



Example - UTM - Services - VPN IPSEC - Tunnels - Spokes

In the tunnels tab, we can see that, because we have configured a Hub in Devices Communities, only one tunnel was created automatically, which communicates with the centralizer, generating a Star topology. If we had connected to the Hub, two tunnels would be displayed, communicating with the Spokes, as shown below:



Example - UTM - Services - VPN IPSEC - Tunnels - Hub

This completes the configuration of a Star topology. Next, we will exemplify the Full-Mesh topology.

## Topology Full-Mesh

This demonstration will take into account the following structure:

Topology Star - IP Addressing

Device	IP	Role
UTM204	204.204.204.0	Spoke
UTM206	206.206.206.0	Spoke
UTM8	108.108.108.0	Spoke

Before creating the communities, in Inventory [add the Devices](#) according to their structure, in this example we will use:

Devices

Inventory

Communities

Templates

Provisioning

3 records

UTM204

No Group

BBv-100

4336-D46C-5D19-B506

BLOCKBIT UTM 2.0.6  
build 20102607

Policies 2.0  
IPv4

Policies 2.0  
IPv6

UTM206

No Group

BBv-1000

E593-8A8D-F033-CA4A

BLOCKBIT UTM 2.0.6  
build 20102607

Policies 2.0  
IPv6

UTM8

No Group

BBv-5

E828-E23A-BFF0-44A5

BLOCKBIT UTM 1.5.14  
build 20102611

Policies 1.5  
IPv6

<

1

>

10 / page

Example - Devices Tab

Back in the communities tab, [create a new community](#) and configure it, as shown below:

Edit community

General

Encryption

Advanced

Devices

General

\* Name

Device Community

Description

Device Community

Settings

IKE Version

IKEV2

Exchange Mode

Main

Topology

Site-To-Site

\* Shared Key

...

Cancel

Save

Example - Create Community

- **Name:** Device Community;
- **Description:** Device Community;
- **IKE Version:** IKEV2;
- **Exchange Mode:** Main;
- **Topology:** Site-to-site;
- **Shared Key:** q1Q!q1Q!.

The settings on the side tabs Encryption and Advanced will remain the same. Select the [Devices](#) tab and create the Spokes as shown:

## UTM204

Configure the UTM204 device as a Spoke, as shown below:

Edit Device

X

\* Device

UTM204

\* Local Host

204.204.204.0

\* Local ID

204.204.204.0

Network

+

192.168.204.0/24

^

1

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

Save

Example - Create Community - Create Device

- **Device:** UTM204;
- **Local Host:** 204.204.204.0;
- **Local ID:** 204.204.204.0;
- **Network:** 192.168.204.0/24;
- **Role:** Spoke.

## UTM206

Configure the UTM206 device as a Spoke, as shown below:

Edit Device

X

\* Device

UTM206

\* Local Host

206.206.206.0

\* Local ID

206.206.206.0

Network

+

192.168.206.0/24

^

1

▼

-

Role

Spoke

▼

☐ Dynamic

Cancel

Save

Example - Create Community - Create Device

- **Device:** UTM206;
- **Local Host:** 206.206.206.0;
- **Local ID:** 206.206.206.0;
- **Network:** 192.168.206.0/24;
- **Role:** Spoke.

## UTM8

Configure the UTM8 device as a Spoke, as shown below:

Edit Device

X

\* Device

UTM8

\* Local Host

108.108.108.0

\* Local ID

108.108.108.0

Network

+

192.168.108.0/24

^

↓

-

Role

Spoke

↓

☐ Dynamic

Cancel

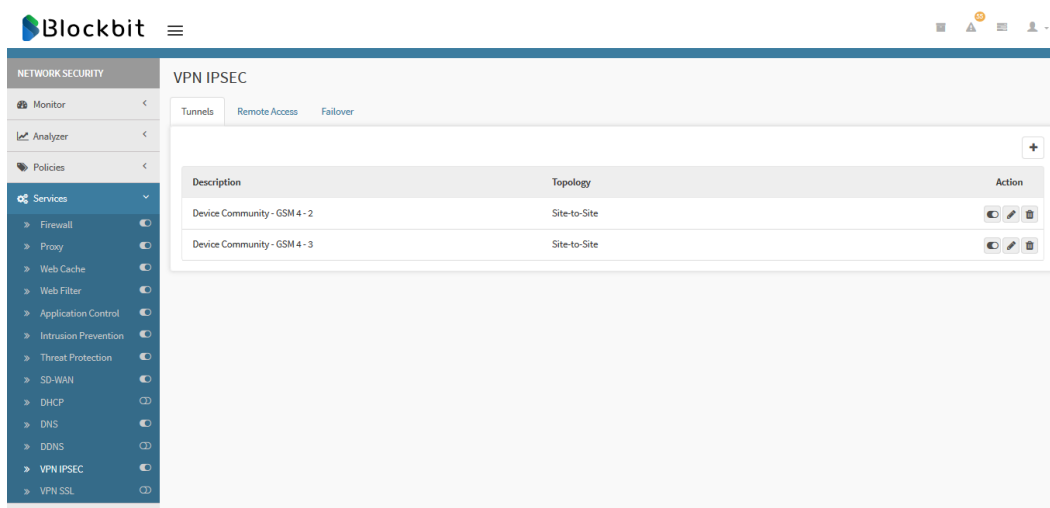
Save

Example - Create Community - Devices - Create Device

- **Device:** UTM8;
- **Local Host:** 108.108.108.0;
- **Local ID:** 108.108.108.0;
- **Network:** 192.168.108.0/24;
- **Role:** Spoke.

After these steps, we will arrive at this result:





Example - UTM - Services - VPN IPSEC - Tunnels

In the tunnels tab we can see that because we have configured several Spokes and no Hub in the Device Communities, a tunnel was automatically created for each Spoke, generating a Full Mesh topology.

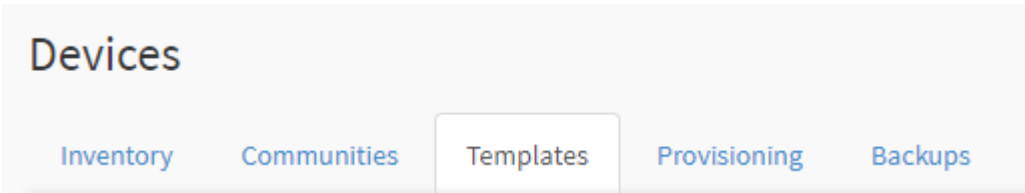
This completes the configuration of the examples, for more information on device communities, see this [page](#).



# Templates tab

Templates are a set of general settings for Blockbit NGFW devices. With this set of configurations, it is possible to initialize the devices with the global configurations in a fast, practical and error-free way, decreasing the TCO, maximizing the performance of the IT team and avoiding configuration errors.

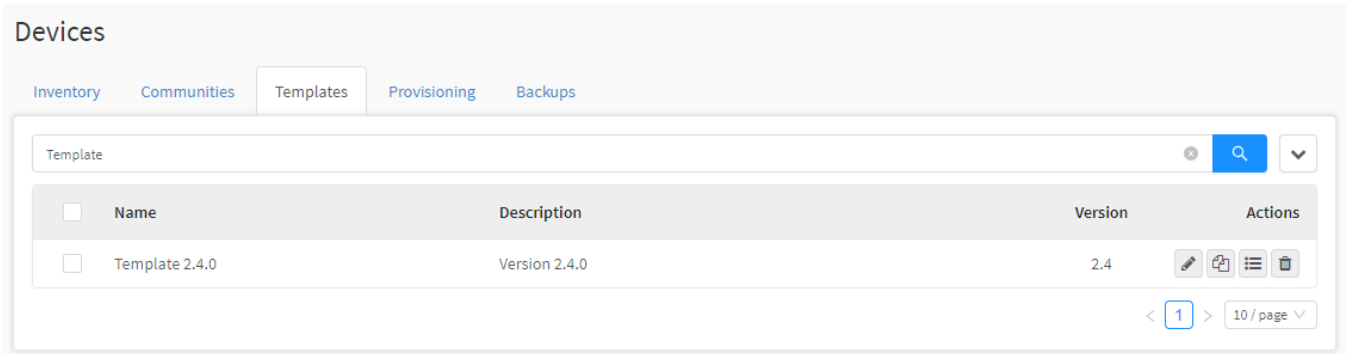
To access the Templates screen, click on the tab as shown below.



Templates tab

The Templates Screen will appear. It consists of four columns: "Name", "Description", "Versions" and "Actions". In addition, the search bar is located at the top of the screen and in the upper right corner of the screen is the **actions menu** [  ].

The screen below will be displayed:



Devices - Templates

This section will demonstrate how:

- Create, clone and delete Templates;
- Configure the created Templates;
- Etc.

Next, we'll look at the functions at the top of this table.

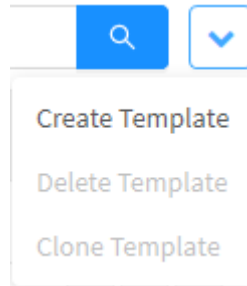
# Templates - Actions menu

At the top right of the screen we have the actions menu:



Templates - Actions menu button

By clicking on this button the menu below is displayed:



Templates - Actions menu

The menu consists of the following options:

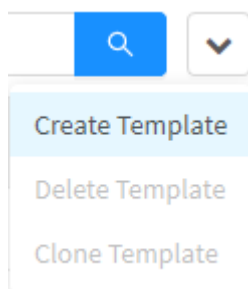
- [Create Template](#);
- [Delete Templates](#);
- [Clone Template](#).

Next, each action menu option will be detailed.

# Templates - Actions menu - Create Template

Through the button "Create Template" it is possible to create a new Template. To access, follow the steps below:

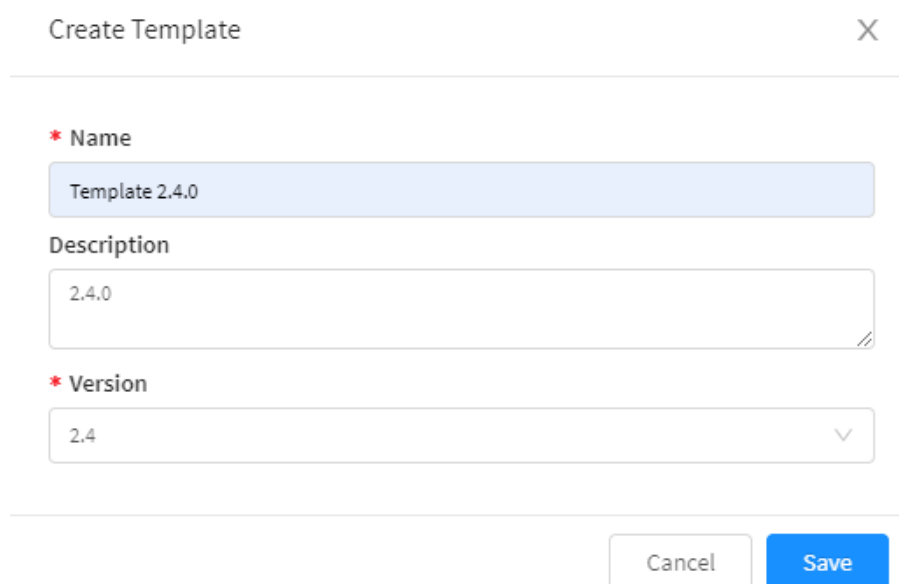
1. Click on the "Create Template" option;



Templates – Create Template


2. Fill in the "Create Templates" screen:

- **Name:** Template Name. Ex.: *Devices Store*;
- **Description:** Template Description. Ex.: *Basic Stores Settings*;
- **Version:** Select the correct version according to the NGFW that will be used. It is important to keep in mind that if you select a different version, the template will not work.


A screenshot of a 'Create Template' dialog box. The title bar says 'Create Template' with a close button (X) on the right. The form has three main sections: 1. 'Name' with a red asterisk, a text input field containing 'Template 2.4.0'. 2. 'Description' with a text area containing '2.4.0'. 3. 'Version' with a red asterisk, a dropdown menu showing '2.4'. At the bottom right are two buttons: 'Cancel' and 'Save'.

Templates – Create Template

3. To save changes, click [  ], otherwise click [  ] to close the window.

 **Saved successfully**  
Saved successfully

After performing these procedures, the "Template" of the device was successfully created.

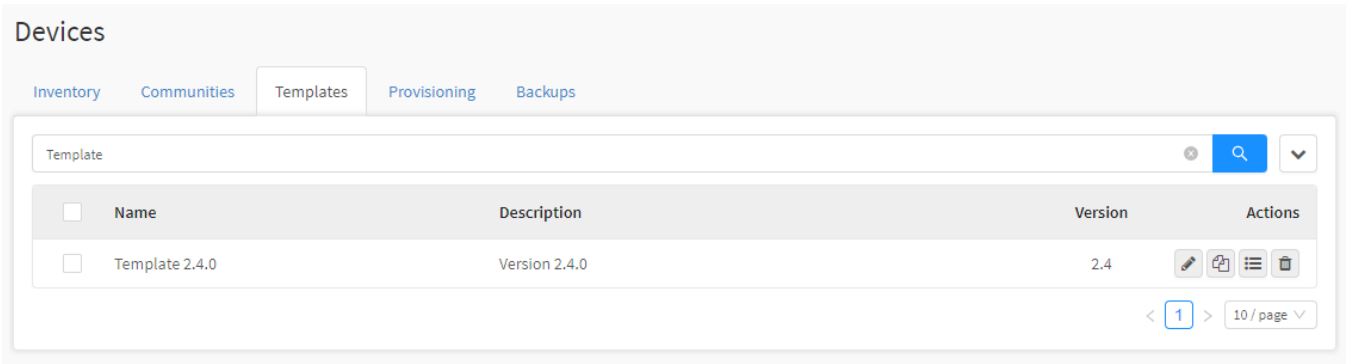
Finally, after registering the name and description of the Template, it will be necessary to click on detail [  ] to display the "Config Template" screen and finalize the template configuration;

For more information access the chapter [Templates - Config Template](#);


# Templates - Actions menu - Delete Templates

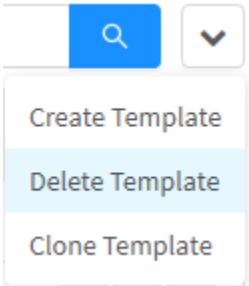
Through the "Delete Templates" button it is possible to delete several Templates at the same time. To delete via the actions menu, follow these steps:

- 1. Select [  ] which Templates you want to delete;



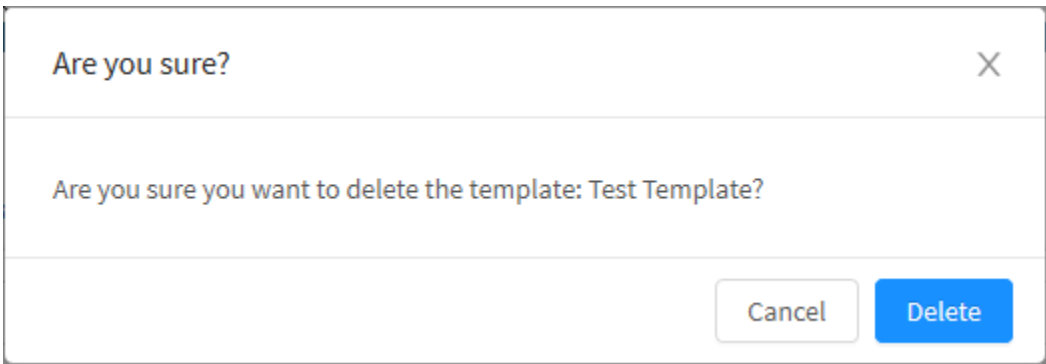
Templates – Selection of Templates to be deleted

- 2. Enter the Actions Menu [  ] and click on the "Delete Template" option;

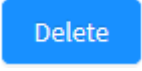


Templates – Delete Template

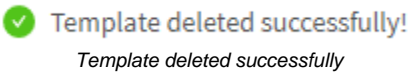
- 3. The message will appear if you really want to delete the selected items;



Templates – Delete Template




If you want to cancel click on the [ ] button. To finish, click the [ ] button.

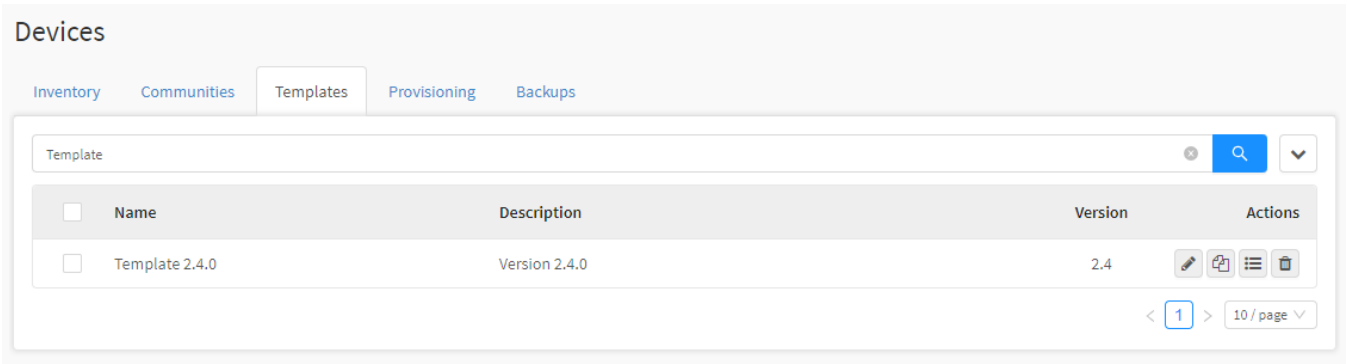


After performing these procedures, the Templates will be successfully deleted.

# Templates - Actions menu - Clone Template

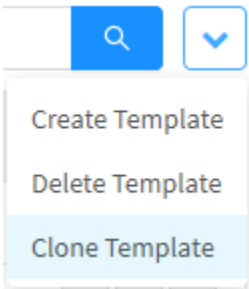
Through the “Clone Template” option it is possible to replicate a *Template*.

1. Select [  ] which Template you want to clone. Ex .: Devices Branch office;



Templates - Selection of the Templates to be cloned

2. In the Actions menu [  ],, click on the option “Clone Template” ;

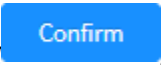


Clone template

3. The message will appear if you really want to clone the selected items;



Templates – Clone Template.



If you want to cancel click on the [ ] button. To finish, click the Confirm [ ] button.



It's also possible to clone a Template by clicking the Clone button [ ].

 Template cloned successfully!

Template successfully cloned

The templates were successfully cloned.















# Templates - Columns

Below we will explain each column of the Templates tab:

Devices




InventoryCommunitiesTemplatesProvisioning

4 records

Name	Description	Version	Actions
<input type="checkbox"/> Device Branch Office	Template for Branch Office	1.5	  
<input type="checkbox"/> Device Head Office	Template for Head Office	1.5	  
<input type="checkbox"/> Device Store	Template for Store Device	1.5	  
<input type="checkbox"/> Device Webfilter	Template for Webfilter Devices	1.5	  

< 1 > 10 / page

Templates

- **Name:** Displays the name of the registered Template;
- **Description:** Displays the registered Template description;
- **Version:** Displays the version in which the Template was created;
- **Actions:** The “Actions” menu consists of several buttons:
  - **Edit** : Allows you to edit the settings of the Template added in the Create Template option of the action menu;
  - **View** : Allows you to view, edit and add more specific Template options, for more information, visit the chapter [Templates - Config Template](#);
  - **Delete** : Delete the Template;
  - **checkbox** ☐: Select the Template.

# Templates - Config Template

By clicking on the detail button [  ] it is possible to configure the template;

In this panel it is possible to make the general configurations and activate which modules will be used in this template.

Config Template

X

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

General

Name

Template 2.4.0

Description

Version 2.4.0

Version

2.4

Modules

Custom

UTM

IPS

ATP

SWG

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Cancel

Save

Config Templates – Edit Template.

## General

In "General" we have the following text boxes:

206

General

\* Name

Template 2.4.0

Description

Version 2.4.0

Version

2.4

Configuration - General.

- **Name:** The template name. Ex.: *Device Head Office*;
- **Description:** The template description. Ex.: *Template for Head Office*;
- **Version:** The version used by the template. It can be 2.3 or 2.4. This option is determined only when the template is created. For more information, check [Templates - Actions menu - Create Template](#).

## Modules

In "Modules" we have the following options:

Modules

☐ Custom
 ☒ UTM
 ☐ IPS
 ☐ ATP
 ☐ SWG

☒ Firewall
 ☒ Intrusion Prevention

☒ Proxy
 ☒ Threat Protection

☒ Web Cache
 ☒ SD-WAN

☒ Web Filter
 ☒ DNS

Configuration - Modules.

The modules arranged in the checkboxes will be enabled or disabled according to the selection of these options:

- **Custom** ☐: If this option is selected, the user has the option to customize which modules will be enabled;
- **UTM** ☒: If this option is selected, all modules commonly used by the NGFW will be enabled;
- **IPS** ☐: If this option is selected, all modules commonly used by the IPS will be enabled: The "Firewall" and "Deep Inspection" modules will be enabled;
- **ATP** ☐: If this option is selected, all modules commonly used by the ATP will be enabled: The "Firewall", "Proxy", "Antimalware" and "Deep Inspection" modules will be enabled;

- **SWG** ☐: If this option is selected, all modules commonly used by the SWG will be enabled: The "Firewall", "Proxy", "Web Cache", "Web Filter" and "Antimalware" modules will be enabled.

By checking the checkboxes it is possible to enable and disable the configuration of the NGFW modules. The available modules are:

- **Firewall** ☐: In this module it is possible to manage the services, security settings and Zone Protection. For more information on these features, check [Firewall](#);
- **Proxy** ☐: This module makes it possible to manage the configurations of HTTP, FTP, SMTP and POP3. For more information on these features, check [Proxy](#);
- **Web Cache** ☐: In this module it is possible to edit the Cache settings. For more information on these features, check [Web Cache](#);
- **Web Filter** ☐: This module makes it possible to customize the blocking page, Google domains and Safe Search settings. For more information on these features, check the [Web Filter](#);
- **Threat Protection** ☐: In this module it is possible to manage the general settings of Threat Protection. In version 1.5 this field is named "Antimalware". For more information on these features, check [Threat Protection](#);
- **Intrusion Prevention** ☐: This module makes it possible to manage the profiles, Whitelist and Blacklist of Intrusion Prevention. In version 1.5 this field is named "DPI". For more information on these features, check [Intrusion Prevention](#);
- **SD-WAN** ☐: In this module it is possible to manage SD-WAN profiles and services. For more information on these features, check [SD-WAN](#);
- **DHCP** ☐: This module makes it possible to manage the DHCP servers, Ranges and Relay. For more information on these features, check [DHCP](#);
- **DNS** ☐: In this module it is possible to edit the settings and DNS redirection. For more information on these features, check [DNS](#);
- **DDNS** ☐: This module makes it possible to manage dynamic hosts. For more information on these features, check [DDNS \(DynDns\)](#).



Note that: When deploying a Firewall (Zone Protection), with authentication by users / groups:

Only users / groups will be listed, if the NGFW already has them, since the GSM does not create users;

If the NGFW does not have users / groups, a rule will be created only with authentication enabled (without considering users / groups).




For more information on each configuration, please refer to the Blockbit NGFW manual.


# Templates - Config Template - Custom Branding


Through this tab it is possible to use GSM as a customization platform for Firewall devices, being possible to change the product title, icon, background image, menu colors etc. Using these options, it is possible to create firewall customization templates according to the visual identity used by the user's own company. This template, in turn, can be applied to multiple devices when deploying the device template (allowing you to select a group of devices that select the same customization).

The customization of appliances is controlled through a license, therefore, this option will only be available if the user has a valid active customization license. If the GSM license allows customization, the custom brand tab will be available in the templates configuration. If the subscription is expired and the user tries to apply a template already configured, the deploy system will present a license error.

This feature works by customizing the appliances even before they are installed on the network.

 If you want to customize the GSM itself, see this [page](#).

To enable customization, click **Enabled** ;

 When activating Custom Branding, references to "Blockbit" in the UTM layout will be automatically hidden, effectively making the appliances a white-label product.

However, note that there are some exceptions:

- Windows and panels where the appliance model is displayed;
- The content of the terms of use;
- Any configuration or component that is only accessible via the root user;
- Zero Touch Provisioning settings;

Config Template

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Custom Branding

Custom


☒ Enabled

Restore Default


\* Page Title

BLOCKBIT | UTM


\* Favicon



\* Logo




\* Background



Preview

BLOCKBIT | UTM

https://172.31.240.35/devices/templates



NETWORK SECURITY

Monitor

Dashboard

Live Sessions

Analyzer

\* Section

#999999

\* Selected

#3C7C9F

\* Open

#356B89

\* Open Font

#CCCCCC

\* Menu

#E9E9E9

\* Base

#E9E9E9

\* Section Font

#FFFFFF

\* Selected Font

#FFFFFF

\* Open F Hover

#FFFFFF

\* Menu Font


#4E4E4E

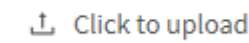



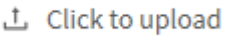


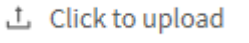


Cancel

Save

Config Template - Custom Brand

209

- **Enabled** : It is necessary to activate this check box to enable the customization of the template, if it is disabled, the customization of the template will be disabled;
- **Page title**: Defines the name that will be displayed in the title bar in the system window. Ex.: UTM;
- **Section**: This option customizes the color of the GSM sections (where "Management", "Analytics" and "Settings" appears), this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Section Font**: In this option, the font color of the GSM sections is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #FFFFFF;
- **Selected**: In this option, the color of the selected menus and the top bar of the GSM is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #ccb516;
- **Selected Font**: In this option, the font color of the selected menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Open**: In this option, the color of the open menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #f3dc3a;
- **Open Font**: In this option, the font color of the open menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Open F Hover**: In this option, the highlighted color of the font of the open menus is customized when the mouse passes over them, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with field RGBA. Ex.: #ffec6c;
- **Menu**: In this option, the color of the menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #bd9700;
- **Menu Font**: In this option, the color of the menu fonts is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Base**: In this option, the base color of the panel where the menus are located is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;

- **Favicon**: Clicking the  button allows you to upload the page's favicon. If you want to view the added image, click , to download click , to delete, click . The format needs to be PNG or ICO, the minimum dimensions are 24x24, there is no maximum size, it is only necessary that the image has the same height and width (need to be a square);
- **Logo**: Clicking the  button allows you to upload the logo used at the top of the menus. If you want to view the added image, click , to delete, click . The format needs to be SVG of dimensions 300x65. There is no maximum size, it is only necessary that the image has different height and width (need to be rectangular);
- **Background**: Clicking the  button allows you to upload an image that is used as a background on the initial login screen. If you want to view the added image, click , to delete, click . The format needs to be PNG or JPG of dimensions 1920x1080;
- **Preview**: Demonstrates the changes that were made to the options above in a preview for checking before actually applying them.



To assist in defining colors:

It is possible to create or consult a color palette on the website <https://colors.co/generate> that provides coloring information at: Color Name, HEX, RGB, HSB, HSL, CMYK, LAB, RAL, HKS, Copic and Prismacolor.

If it is necessary to convert from Pantone to RGB, CMYK or HEX, see the converter on the official website at this link: <https://www.pantone.com/color-finder>.

Here is an example of a template with customization already applied:

Config Template

×

Configuration

Firewall

Proxy

Web Cache

Web Filter

Intrusion Prevention

Threat Protection

SD-WAN

DNS

Custom Branding

Custom


Enabled

Restore Default


\* Page Title

UTM


\* Favicon ⓘ



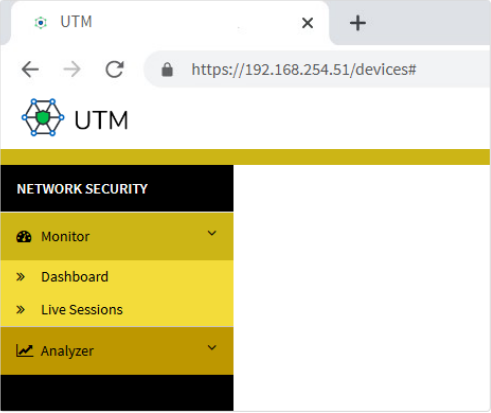
\* Logo ⓘ



\* Background ⓘ



Preview



\* Section

#000000

#FFFFFF

\* Selected

#ccb516

#000000

\* Open

#f3dc39

#FFFFFF

\* Open Font

#000000

#FFFFFF

\* Menu

#bd9700

#000000

\* Base

#000000

#000000

Cancel

Save



Config Template - Custom Brand - Edited Template

When applying custom branding on UTM it may be necessary to clear the browser cache to view the changes.

To access the cache deletion window just use the command "ctrl + shift + del".

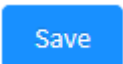
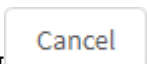
The caption "Powered by Blockbit" below the logo is not customizable.

Restore Default

If you are not satisfied with the changes made, click [  ] to restore the default settings or disable the **Enabled**  check box and deploy the template again to return to the factory defaults.

Save

Cancel

To save changes, click [  ], otherwise, click [  ] to close the window.

Saved successfully

Saved successfully

211

After performing these procedures, the firewall customization was successful.



# Provisioning tab

The Zero Touch Provisioning feature has the function of facilitating and speeding up the implementation of new Blockbit UTM to be managed by GSM. This functionality automates the process of installing and configuring new appliances, requiring only a valid connection to be made available during the first access.

After making the [addition](#) and connection of the appliance, when turning it on for the first time, the UTM will be installed, all settings of the UTM installation wizard will be detected and carried out automatically, the certificate will be valid, any device template that has been configured will be implemented and any policy package that has been pre-configured will be applied automatically.

Through Zero Touch Provisioning the operational cost, technical level and the possibility of human error are drastically reduced, since at the physical point of the network it is not necessary to do anything more than just connect the appliance and turn it on.

It is possible to provision a specific device and also a [batch of multiple devices](#).



## Important

### For the GSM (Global Security Management):

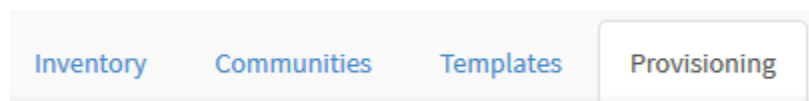
- The following TCP ports has to be accessible to the Blockbit GSM:
  - Port 80
  - Port 22
  - Port 443
  - Port 444
  - Port 555

### For the NGFW (Next-Generation Firewall):

- Internet access is essential to reach <https://license.blockbit.com> using the TCP port 443.
- Make sure the following ports are accessible by the Blockbit GSM public IP address.
  - Port 80
  - Port 22
  - Port 443
  - Port 444
  - Port 555

Make sure the network is configured correctly.

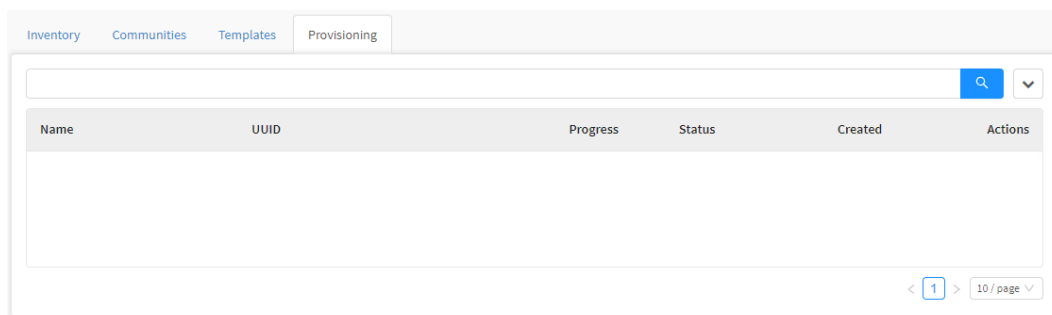
To access the Provisioning screen, click on the tab as shown below.



Provisioning tab

The Provisioning screen will be displayed. It consists of the columns: "Name", "Identification", "Progress", "Status", "Connected" and "Actions". In addition, the [search bar](#) is located at the top of the screen and in the upper right corner of the screen is the [actions menu](#).

The screen below will be displayed:



Devices - Provisioning

This section will demonstrate:

- How to [create devices](#) for provisioning;
- [How to use the Batch provisioning feature](#).

Next, we'll look at the functions at the top of this table.

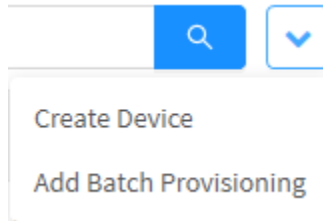
# Provisioning - Actions menu

At the top right of the screen we have the actions menu:



*Provisioning – Actions menu button*

By clicking on this button the menu below is displayed:



Provisioning - Actions menu

The menu has options:

- [Create Device](#),
- [Add Batch Provisioning](#).

Next, we will detail each menu option.

# Provisioning - Actions menu - Create Device

To perform Zero Touch provisioning, the device must be properly licensed, the license is always linked to a company's e-mail and to a UUID, this step is essential because the approval and confirmation of the provisioning is sent by e-mail, in addition because all provisioning is tied to the UUID of an appliance.

In addition, for Zero Touch provisioning to work, it is mandatory to have a valid link configured in order to reach the Blockbit license portal in order to validate this license.

Before you configure provisioning, you must have created a [Device Template](#) or [Policy Package](#) to add to the device during provisioning.



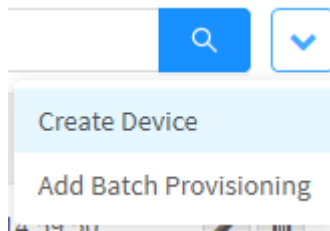
As the GSM policies that are in the header have priority over those of the UTM, It is recommended that when creating a policy package to be used in provisioning, that they are created in the footer for security so that they do not overwrite important permissions of the UTM policies.



When deploying using a policy that uses QoS, it will be necessary to activate the WAN interface in [Network - Traffic Shaping](#), otherwise the policy will not work.

Through the button "Create Device" it is possible to create a new device for provisioning. To access, follow the steps below:

1. Click on the "Create Device" option;



*Provisioning – Create Device*

2. The "Device" window is made up of the "General", "Network" and "Certificate" tab. When adding a device for provisioning fill the fields with the device settings, basically as if you were going to install a UTM normally. Complete the fields as shown below:

Device

General

Network

Certificate

\* Name

\* Company

\* User Admin

Password

Device Template

Policy Package

\* UUID

Description

Cancel

Save

Create Device – Device - General

- **Name:** Device Name. Ex.: Provisioned Device;
- **Company:** Defines the company name. Ex.: Blockbit;
- **User Admin:** Enter the same administrator user that was registered during the installation of UTM. Ex.: admin;
- **Password:** Enter the password registered during the installation of UTM. This password must be at least eight characters long, contain upper and lower case letters and special characters. Ex.: q1W@e3R\$;
- **Device Template:** Through this field, it is possible to add the templates created in [Device Template](#) for this device;
- **Policy Package:** Through this field, it is possible to add the policy packages created in [Policy Package](#) for this device;
- **UUID:** Enter the UTM's unique identification code, it can be found on the Dashboard - System in the widget license;
- **Description:** Device description. Ex.: Provisioned Device Settings.

3. After filling in the fields on the "General" tab, fill in the fields on the "Network" tab, as shown below:

Device

General

Network

Certificate

\* Hostname

\* Language

\* Timezone

\* Gateway

\* Suffix DNS

\* DNS Server

\* NTP Server

ETH0

1.1.1.1

255.255.255.255

DHCP Server

ETH1

1.1.1.1

255.255.255.255

DHCP Server

ETH2

1.1.1.1

255.255.255.255

DHCP Server

Cancel

Save

Create Device – Device - Network

- **Hostname:** Defines the Hostname. It can be anyone as long as it complies with the FQDN - Fully Qualified Domain Name. Ex.: GSM;
- **Language:** Select the default language. Ex.: *English*;
- **Timezone:** Select the time zone. Ex.: *America/Sao\_Paulo*;
- **Gateway:** Sets the default route for the network. Ex.: 176.16.102.1;
- **Suffix DNS:** Determines the domain of the network. Ex.: *blockbit.com*;
- **DNS Server:** Defines the network or internet DNS server. Ex.: 176.16.102.161;
- **NTP Server 1:** Sets the clock synchronization server. Ex.: *a.ntp.br*;
- **ETH** ☒: Activate the desired network interfaces by checking the checkbox;
  - **IP Address:** Inform which network address the settings will be applied to;
  - **Net Mask:** Inform which will be the netmask;
  - **Network zone:** Determine the Network Zone. By default, the default options are: LAN, WAN and DMZ;
  - **DHCP Server** ☒: Enable this checkbox to distribute IP addresses as network devices request connection.



If an IP is defined on the eth0 port, when performing the UTM provisioning, the IP change will be applied replacing DHCP, thus requiring the user to access the IP defined on port 98.

4. After completing the fields on the "Network" tab, complete the fields on the "Certificate" tab, as shown below:

Device

General

Network

Certificate

\* Country

Abbreviation of two letters. Ex.: US

\* State

Full Ex.: New York

\* City

Full Ex.: New York

\* Organization

Company name

\* E-mail

admin@domain

\* Organizational Unit

Ex.: Department

\* Expires (years)

Years

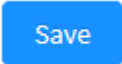
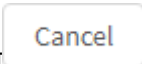
\* Hostname


Cancel

Save

Create Device – Device - Certificate

- **Country:** Defines the country. Ex.: BR;
- **State:** Sets the state. Ex.: Sao Paulo;
- **City:** Defines the city. Ex.: Sao Paulo;
- **Organization:** Defines the company name. Ex.: Blockbit;
- **E-mail:** Sets the administrator email. Ex.: user@blockbit;
- **Organizational Unit:** Defines the department. Ex.: QA;
- **Expires (years):** Defines the validity time of the certificate. Ex.: 10;
- **Hostname:** Sets the FQDN for the certificate. Ex.: [utm.blockbit.com](http://utm.blockbit.com).

5. To save changes, click [  ], otherwise click [  ] to close the window.

 **Saved successfully**  
Saved successfully

When saving the settings, a confirmation email will be sent to the address that is registered on the Blockbit License Portal. You will need to click on the link that will appear in the body of the email to actually start provisioning itself.



Provisioning - Confirmation email

A confirmation email will be sent when authorizing provisioning, as shown below:



Provisioning - Provisioning confirmation

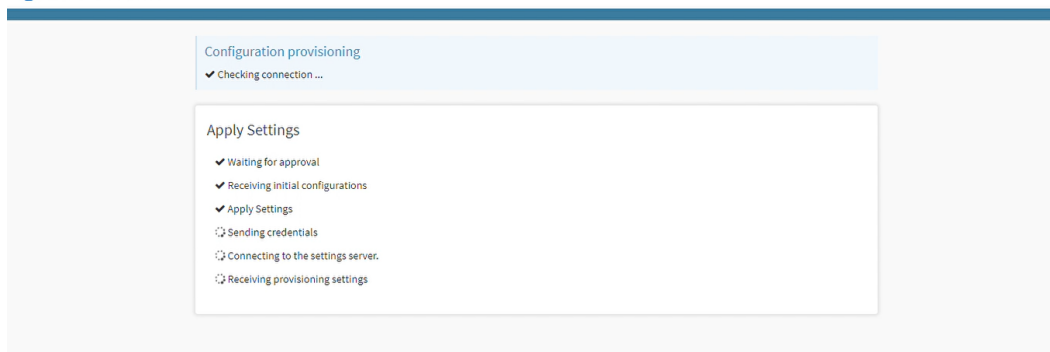
It is possible to track the progress of provisioning through the Status and Progress column in the [Provisioning tab](#) of the GSM, as shown below:

Devices					
<a href="#">Inventory</a> <a href="#">Communities</a> <a href="#">Templates</a> <a href="#">Provisioning</a>					
<div>1 records</div> <div> <input type="text"/> <input type="button" value="Search"/> <input type="button" value="Filter"/> </div>					
Name	UUID	Progress	Status	Created	Actions
Provisioned Device	564DD38E-BB9D-7B6F-7754-463B86696040	<div> <div></div> 50% </div>	<span>Sending deploy</span>	August 19th 2020 - 11:31:55	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<div> <div>&lt; 1 &gt;</div> <div>10 / page</div> </div>					

Provisioning - Provisioning progress

It is also possible to see the provisioning progress through the UTM interface that will be provisioned. As shown in the following image:



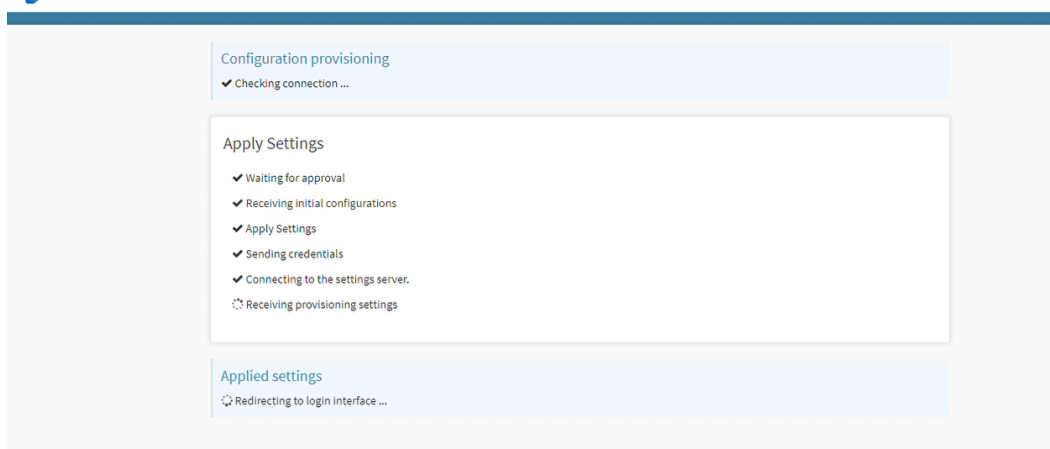


Provisioning - Provisioning in progress



This screen will be displayed in Portuguese or English according to the user's browser settings.

If provisioning is completed successfully, an automatic redirection to the login screen will occur, as shown below:



Provisioning - Redirect

When directed to the Login screen, it will probably not be possible to access the system immediately thanks to the completion of the provisioning settings, wait until the access has been released. During this stage it is extremely important not to disconnect the device. *If the settings are still being made, a notification will be displayed blocking access when trying to log in.* For a more accurate view of the progress of provisioning, check the Status and Progress column on the [Provisioning tab](#) of the GSM.



**ATTENTION:** When performing Zero Touch provisioning, DO NOT turn off the device before you are actually able to log into UTM. Check the Status and Progress column on the GSM [Provisioning tab](#) to get a more accurate view of the progress of the procedure. If there is a power outage at any time during provisioning, it is recommended to remove the provisioning that was made in GSM, access the CLI and use the [rewizard](#) command on the appliance, so that provisioning is restarted from the initial step and also to restart all installation settings that will be made in the UTM.

If provisioning is successful, the device will be displayed in the [Inventory tab](#), in the same way as a manually linked device.

Devices

Inventory Communities Templates Provisioning

2 records

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/>	NGFW Branch NY	No Group	BBv-10	3AFC-DB25-2434-2F93	BLOCKBIT UTM 2.0.0 build 20030507		Policy 2.0		
<input type="checkbox"/>	UTM23	No Group	BBv-5	09B6-536E-E1BD-5FDE	BLOCKBIT UTM 2.0.0 build 20030216				

< 1 > 10 / page

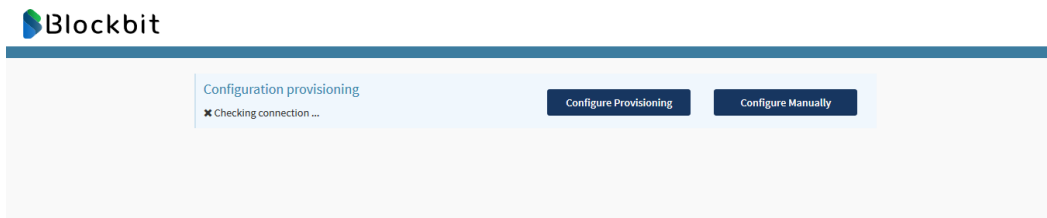
Provisioning - Device moved to Inventory tab

Upon successful completion of Zero Touch Provisioning, UTM will also automatically have the license validated, being administered by GSM in Central Management, with the deployment of [Device Templates](#) and [Policy Packages](#) defined in GSM applied.



After finishing configuring Zero Touch Provisioning, if you need to send logs to GSM, access the Settings menu, Administration option, Central Management tab in UTM, check the Enable Manager ☒ checkbox and configure the Manager Address field with the IP of the GSM logger.

If provisioning is not completed successfully, a panel with two buttons will appear:



Provisioning - Configure Provisioning

If provisioning does not occur because the DNS is unable to provide a valid path to the Blockbit License Portal, click on the button [

**Configure Provisioning**

] so that the panel illustrated below is displayed, it is possible to configure a valid IP so that the UTM can properly license.

Configuration provisioning

✖ Checking connection ...

Configure Provisioning

Configure Manually

General

IP Address

Mask

255.255.255.255

Gateway

DNS

Save

© BLOCKBIT 2020

Provisioning - Add a valid IP

### Configure Manually

Through the option [ ] it is possible to make the configuration manually, when selecting this option you will be directed to the standard Wizard. This will also happen if the license has expired or expired, the user will be notified and directed to the normal Wizard. For more information on how to configure it, see the UTM Wizard configuration [page](#).

If it is necessary to use the [rewizard](#) command on a machine that has already been provisioned, you must first remove it from the GSM [Inventory](#) tab.

That done, it will be necessary to create a new provisioning for the machine that has gone through the rewizard.

After these steps, the process is the same.

For more information about the columns on the Provisioning tab click this [link](#) for more information about batch provisioning, see this [page](#).

# Provisioning - Actions Menu - Add Batch Provisioning

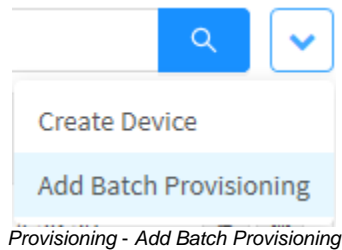
The main benefit of the batch provisioning function is the agility with which the administrator is able to implement and configure services and policies, using pre-defined settings in device templates and policy packages, as well as facilitating the process of approval and error checking in this process (in case of possible inconsistencies in the code for example). In addition to all these benefits, the batch provisioning process is relatively simple and transparent, and can easily be followed by the panel on the Provisioning tab through the progress bar and status icons.

Batch provisioning works using a CSV file as a template, it basically contains all fields in the Zero Touch Provisioning window and acts in the same way: Gathering all the information necessary for the implementation of a new device.

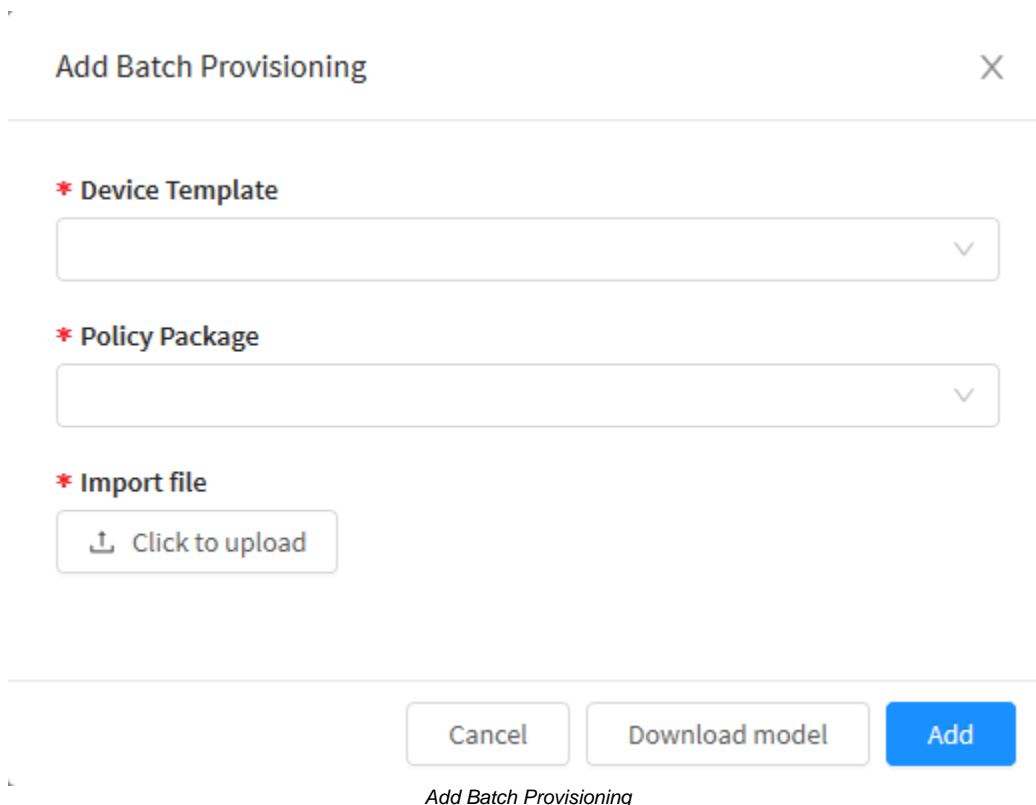
After completing the CSV, the user simply needs to determine which template and policy package will be applied to this list of devices, after adding the devices to be provisioned, just wait for the receipt of the batch provisioning email and click on the confirmation link.

If any inconsistency is detected, the batch implementation is not performed, the confirmation email will only be received if the entire batch is in compliance on the Blockbit licensing portal and if the CSV file is correctly configured.

To perform batch provisioning, click on the actions menu [  ] and select the option "Add Batch Provisioning";



The window below will appear:

A screenshot of a web form titled "Add Batch Provisioning". The form has a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk: "Device Template", "Policy Package", and "Import file". Each field has a dropdown arrow icon. The "Import file" field has a "Click to upload" button. At the bottom of the form, there are three buttons: "Cancel", "Download model", and "Add". The "Add" button is highlighted in blue. Below the form, the text "Add Batch Provisioning" is visible.

Download model

Before completing the form, click [ ] to download the template in CSV.



The CSV file is available according to the interface language. For example, if you have selected the language "Portuguese" when logging in, all CSV fields will be in this language (en-US).

The data of this model represents the fields of the form in [Zero Touch Provisioning](#) therefore, complete the CSV as needed and save it, there is no obligation for the file to be with the same name as when the download was made, just being necessary to configure it correctly and use the file extension (CSV).



When editing the CSV the field language, ntp server and timezone must use the correct information among those provided by GSM (see [creation of single device](#)). For example, the only supported languages are "pt\_BR" or "en-US", if another value is added in this field, the file will be considered invalid.

For more information about the Time Zone syntax in CSV visit this [page](#).



If you are using Microsoft Excel to edit the CSV file, you can use the "Get Text / CSV data" function to facilitate data interpretation. This feature uses delimiters as columns, making it easy to view the file.

Click to upload

When you are finished completing the CSV, click [ ] to upload the batch of devices.



Note that if the CSV is too long, it is natural that the system takes time to upload and read the file.

After uploading, make selections on the form as needed:

- **Device Template:** Select the Device Template that will be applied to all appliances in the batch, if you need more information on how to create one see this [page](#);
- **Policy Package:** Select the Policy Package that will be applied to all appliances in the batch, if you need more information on how to create one, see this [page](#).



As [Custom Branding](#) is part of the Device Template, it is possible to customize UTMs during this process.



It is not necessary to select a Device Template and a Policy Package, it is mandatory to select at least one of them. If the user prefers to select only one of the two, provisioning will proceed normally.

After completing the form the window should look like the example below:

Add Batch Provisioning

X

Device Template

Teste de Device Template 2.x v1

Policy Package

Policy Package

\* Import file

Click to upload



provisioning\_model.csv

Cancel

Download model

Add

Add Batch Provisioning - Example

Click  to batch provision or  to close the window.



Provisioning is only possible when the clients linked to the UUID are the same, if there are differences, the error will be displayed, informing that such UUIDs do not belong to the same client.

If a device in the CSV file has an incorrect data, a window is displayed informing the error and the line where the correction must be made.

## Error import batch



Invalid fields / Line 1

UUID: as-CF90-4436-D105-0B15CC47F036

Invalid fields / Line 2

UUID: dad-26E5-1213-B4B0-6AC5B4E0C327

Invalid fields / Line 3

UUID: adsadassa-EA0F-D4A9-E500-4FED55BD1E28

Invalid fields / Line 4

UUID: adasd-2E32-3650-3AFA-D9AEA13C9FF7

Duplicate name / Line 5

Name: Lote2

Invalid fields / Line 5

UUID: asdsadas-D46F-0D90-995A-20158F17AF74

Close

Error Import Batch



In order to ensure the completeness of the batch, if any error is detected, the entire batch will be discarded.

Close



Make the indicated corrections and try again. To close this window, click the [Close] or [X] button.

In addition to the validation of the CSV itself, batch provisioning can also be canceled due to errors in the UUID, for more information, see this [page](#).

Add

If all devices are correctly configured, clicking [Add] will save the settings and a confirmation email will be sent to the address registered in the Blockbit License Portal. You will need to click on the link that will appear in the body of the email to actually start provisioning itself.

The confirmation email sent when authorizing provisioning is shown below:



Batch Provisioning - Confirmation email

From this stage onwards, the process will be identical to the provisioning of a single device being possible to follow the progress in the [Provisioning tab](#) of the GSM, in addition, it is also possible to see the progress through the UTM interface itself. For more information, see this [page](#).

After provisioning has been successfully completed, devices will be displayed in the [Inventory tab](#), as shown below:

Devices

Inventory Communities Templates Provisioning

5 records

Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/> Batch1	No Group	BBv-1000	BEB0-56CC-FFE6-0440	BLOCKBIT UTM 2.0.5 build 20080307	Test			
<input type="checkbox"/> Batch2	No Group	BBv-100	6350-104F-3158-200F	BLOCKBIT UTM 2.0.5 build 20080307	Test			
<input type="checkbox"/> Batch3	No Group	BBv-1000	545F-A663-0918-7C0B	BLOCKBIT UTM 2.0.5 build 20080307	Test			
<input type="checkbox"/> Batch4	No Group	BBv-100	47D2-96A6-4F28-4246	BLOCKBIT UTM 2.0.5 build 20080307	Test			
<input type="checkbox"/> Batch5	No Group	BBv-100	15F2-B9B6-0CF3-56C0	BLOCKBIT UTM 2.0.5 build 20080307	Test			

< 1 > 10 / page

Devices - Inventory - Provisioned Devices

For more information about the columns on the Provisioning tab, click on this [link](#), regarding Zero Touch Provisioning, see this [page](#).



# Possible errors in provisioning

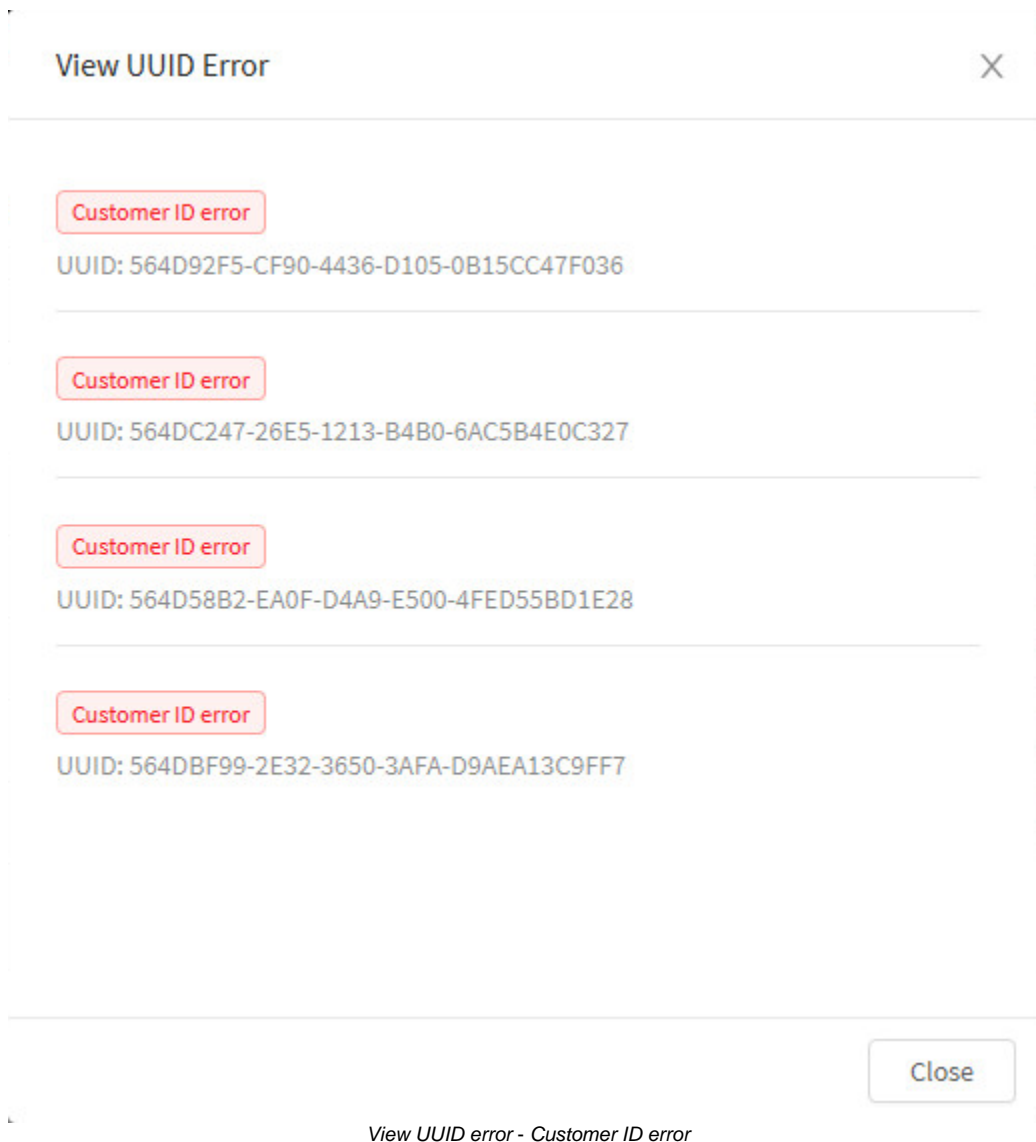
In addition to CSV validation itself, batch provisioning can also be canceled in the following cases:

- [Incorrect Customer ID](#);
- [License in use](#);
- [Expired license](#);
- [License not found](#);
- [Inactive license](#).

To see more details about these errors, just click on the [ **Error batch** ] icon in the status column.

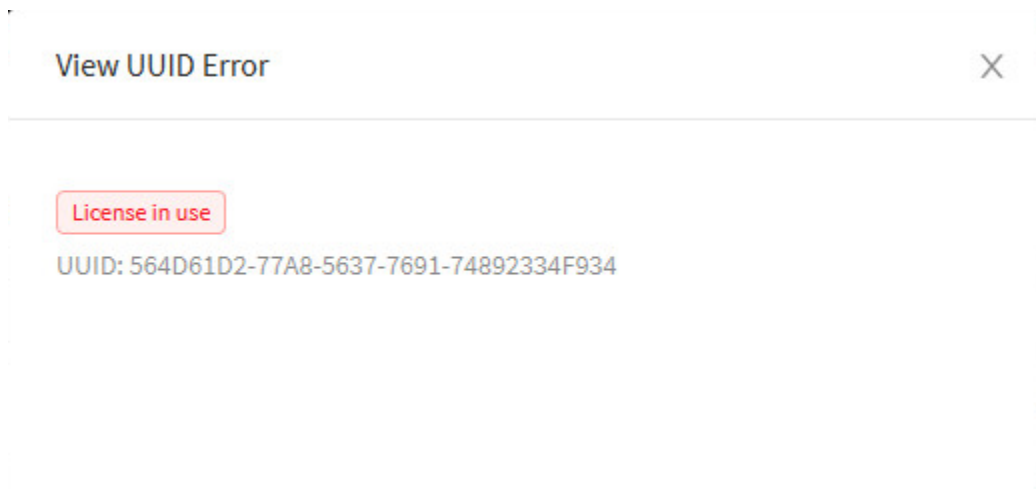
Next we will demonstrate the window that is displayed when viewing these errors.

## Incorrect Customer ID



This error is displayed if the UUID used in the Lot is linked to another user. Provisioning is only possible when the customer linked to the UUID is the same, if there are any differences this error will be presented, informing that the UUIDs do not belong to the same customer.

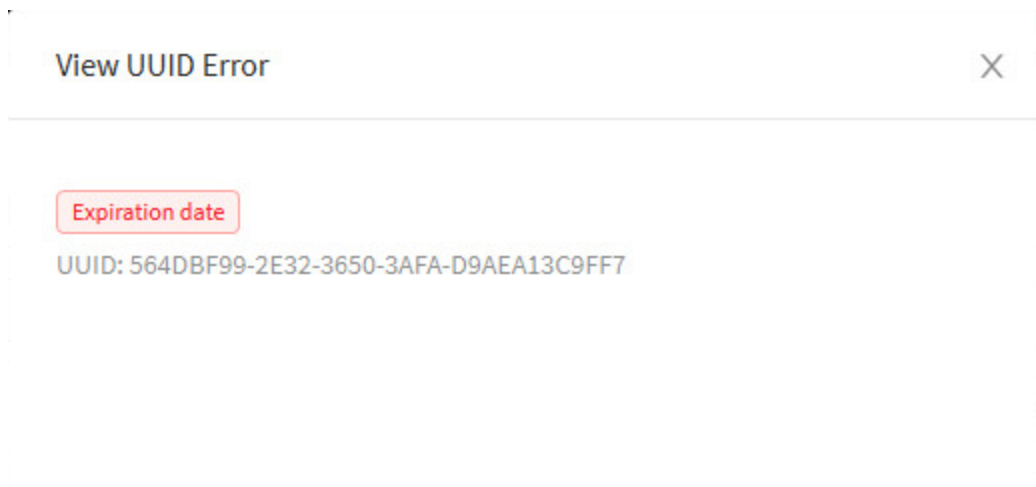
## License in use



*View UUID error - License in Use*

This error is displayed if the license used in the Batch is already in use by another device. If this UUID refers to a device provisioned by GSM, it is recommended to check the [Inventory](#) tab, where it will be possible to manage and remove it.

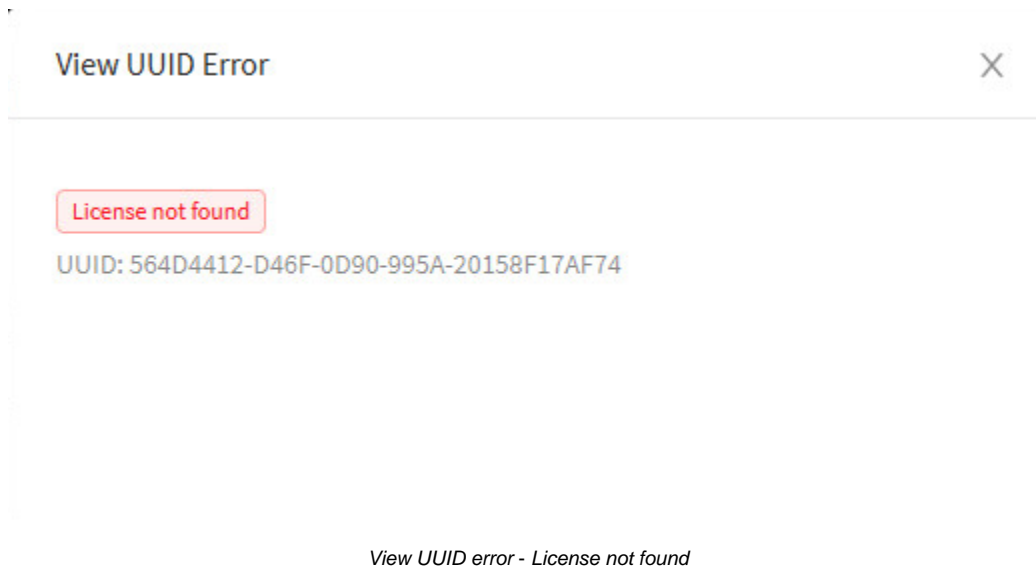
## Expired license



*View UUID error - Expiration Date*

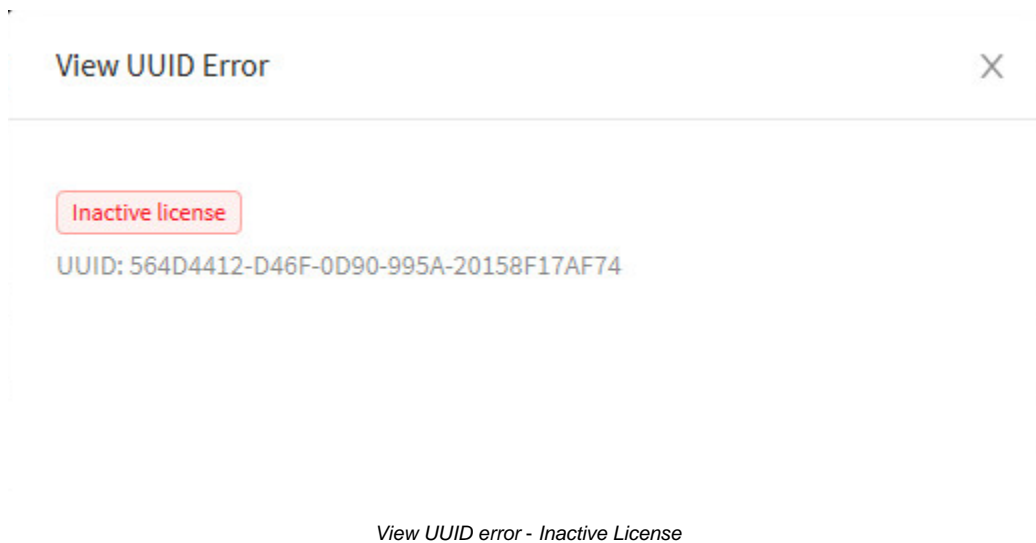
This error is displayed if the license used in the Batch is expired. In this case, contact Blockbit to regularize your situation.

## License not found



This error is displayed if the license has not been found on the portal. In this case, contact Blockbit to regularize your situation.

## Inactive license



This error is displayed if the license is inactive. In this case, contact Blockbit to regularize your situation.

Therefore, ensure that the licenses for all devices to be carried out in batch provisioning are valid and that the CSV data has been completed correctly before performing batch provisioning..

For more information on batch provisioning, see this [page](#).

# Time Zone Syntax in CSV

In order to facilitate the editing of the CSV, a table with all the time zones accepted in the UTM and the equivalent value to be added in the CSV follows:

Timezone	Value
Africa/Abidjan	Africa/Abidjan
Africa/Accra	Africa/Accra
Africa/Addis_Ababa	Africa/Addis_Ababa
Africa/Algiers	Africa/Algiers
Africa/Asmara	Africa/Asmara
Africa/Bamako	Africa/Bamako
Africa/Bangui	Africa/Bangui
Africa/Banjul	Africa/Banjul
Africa/Bissau	Africa/Bissau
Africa/Blantyre	Africa/Blantyre
Africa/Brazzaville	Africa/Brazzaville
Africa/Bujumbura	Africa/Bujumbura
Africa/Cairo	Africa/Cairo
Africa/Casablanca	Africa/Casablanca
Africa/Ceuta - Ceuta, Melilla	Africa/Ceuta
Africa/Conakry	Africa/Conakry
Africa/Dakar	Africa/Dakar
Africa/Dar_es_Salaam	Africa/Dar_es_Salaam
Africa/Djibouti	Africa/Djibouti
Africa/Douala	Africa/Douala
Africa/El_Aaiun	Africa/El_Aaiun
Africa/Freetown	Africa/Freetown
Africa/Gaborone	Africa/Gaborone
Africa/Harare	Africa/Harare
Africa/Johannesburg	Africa/Johannesburg
Africa/Juba	Africa/Juba
Africa/Kampala	Africa/Kampala
Africa/Khartoum	Africa/Khartoum
Africa/Kigali	Africa/Kigali
Africa/Kinshasa - Dem. Rep. of Congo (west)	Africa/Kinshasa
Africa/Lagos	Africa/Lagos
Africa/Libreville	Africa/Libreville
Africa/Lome	Africa/Lome
Africa/Luanda	Africa/Luanda
Africa/Lubumbashi - Dem. Rep. of Congo (east)	Africa/Lubumbashi
Africa/Lusaka	Africa/Lusaka
Africa/Malabo	Africa/Malabo

Africa/Maputo	Africa/Maputo
Africa/Maseru	Africa/Maseru
Africa/Mbabane	Africa/Mbabane
Africa/Mogadishu	Africa/Mogadishu
Africa/Monrovia	Africa/Monrovia
Africa/Nairobi	Africa/Nairobi
Africa/Ndjamena	Africa/Ndjamena
Africa/Niamey	Africa/Niamey
Africa/Nouakchott	Africa/Nouakchott
Africa/Ouagadougou	Africa/Ouagadougou
Africa/Porto-Novo	Africa/Porto-Novo
Africa/Sao_Tome	Africa/Sao_Tome
Africa/Tripoli	Africa/Tripoli
Africa/Tunis	Africa/Tunis
Africa/Windhoek	Africa/Windhoek
America/Adak - Aleutian Islands	America/Adak
America/Anchorage - Alaska (most areas)	America/Anchorage
America/Anguilla	America/Anguilla
America/Antigua	America/Antigua
America/Araguaina - Tocantins	America/Araguaina
America/Argentina/Buenos_Aires - Buenos Aires (BA, CF)	America/Argentina/Buenos_Aires
America/Argentina/Catamarca - Catamarca (CT); Chubut (CH)	America/Argentina/Catamarca
America/Argentina/Cordoba - Argentina (most areas: CB, CC, CN, ER, FM, MN, SE, SF)	America/Argentina/Cordoba
America/Argentina/Jujuy - Jujuy (JY)	America/Argentina/Jujuy
America/Argentina/La_Rioja - La Rioja (LR)	America/Argentina/La_Rioja
America/Argentina/Mendoza - Mendoza (MZ)	America/Argentina/Mendoza
America/Argentina/Rio_Gallegos - Santa Cruz (SC)	America/Argentina/Rio_Gallegos
America/Argentina/Salta - Salta (SA, LP, NQ, RN)	America/Argentina/Salta
America/Argentina/San_Juan - San Juan (SJ)	America/Argentina/San_Juan
America/Argentina/San_Luis - San Luis (SL)	America/Argentina/San_Luis
America/Argentina/Tucuman - Tucuman (TM)	America/Argentina/Tucuman
America/Argentina/Ushuaia - Tierra del Fuego (TF)	America/Argentina/Ushuaia
America/Aruba	America/Aruba
America/Asuncion	America/Asuncion
America/Atikokan - EST - ON (Atikokan); NU (Coral H)	America/Atikokan
America/Bahia - Bahia	America/Bahia
America/Bahia_Banderas - Central Time - Bahia de Banderas	America/Bahia_Banderas
America/Barbados	America/Barbados
America/Belem - Para (east); Amapa	America/Belem
America/Belize	America/Belize
America/Blanc-Sablon - AST - QC (Lower North Shore)	America/Blanc-Sablon

America/Boa_Vista - Roraima	America/Boa_Vista
America/Bogota	America/Bogota
America/Boise - Mountain - ID (south); OR (east)	America/Boise
America/Cambridge_Bay - Mountain - NU (west)	America/Cambridge_Bay
America/Campo_Grande - Mato Grosso do Sul	America/Campo_Grande
America/Cancun - Eastern Standard Time - Quintana Roo	America/Cancun
America/Caracas	America/Caracas
America/Cayenne	America/Cayenne
America/Cayman	America/Cayman
America/Chicago - Central (most areas)	America/Chicago
America/Chihuahua - Mountain Time - Chihuahua (most areas)	America/Chihuahua
America/Costa_Rica	America/Costa_Rica
America/Creston - MST - BC (Creston)	America/Creston
America/Cuiaba - Mato Grosso	America/Cuiaba
America/Curacao	America/Curacao
America/Danmarkshavn - National Park (east coast)	America/Danmarkshavn
America/Dawson - Pacific - Yukon (north)	America/Dawson
America/Dawson_Creek - MST - BC (Dawson Cr, Ft St John)	America/Dawson_Creek
America/Denver - Mountain (most areas)	America/Denver
America/Detroit - Eastern - MI (most areas)	America/Detroit
America/Dominica	America/Dominica
America/Edmonton - Mountain - AB; BC (E); SK (W)	America/Edmonton
America/Eirunepe - Amazonas (west)	America/Eirunepe
America/El_Salvador	America/El_Salvador
America/Fort_Nelson - MST - BC (Ft Nelson)	America/Fort_Nelson
America/Fortaleza - Brazil (northeast: MA, PI, CE, RN, PB)	America/Fortaleza
America/Glace_Bay - Atlantic - NS (Cape Breton)	America/Glace_Bay
America/Godthab - Greenland (most areas)	America/Godthab
America/Goose_Bay - Atlantic - Labrador (most areas)	America/Goose_Bay
America/Grand_Turk	America/Grand_Turk
America/Grenada	America/Grenada
America/Guadeloupe	America/Guadeloupe
America/Guatemala	America/Guatemala
America/Guayaquil - Ecuador (mainland)	America/Guayaquil
America/Guyana	America/Guyana
America/Halifax - Atlantic - NS (most areas); PE	America/Halifax
America/Havana	America/Havana
America/Hermosillo - Mountain Standard Time - Sonora	America/Hermosillo
America/Indiana/Indianapolis - Eastern - IN (most areas)	America/Indiana/Indianapolis
America/Indiana/Knox - Central - IN (Starke)	America/Indiana/Knox
America/Indiana/Marengo - Eastern - IN (Crawford)	America/Indiana/Marengo

America/Indiana/Petersburg - Eastern - IN (Pike)	America/Indiana/Petersburg
America/Indiana/Tell_City - Central - IN (Perry)	America/Indiana/Tell_City
America/Indiana/Vevay - Eastern - IN (Switzerland)	America/Indiana/Vevay
America/Indiana/Vincennes - Eastern - IN (Da, Du, K, Mn)	America/Indiana/Vincennes
America/Indiana/Winamac - Eastern - IN (Pulaski)	America/Indiana/Winamac
America/Inuvik - Mountain - NT (west)	America/Inuvik
America/Iqaluit - Eastern - NU (most east areas)	America/Iqaluit
America/Jamaica	America/Jamaica
America/Juneau - Alaska - Juneau area	America/Juneau
America/Kentucky/Louisville - Eastern - KY (Louisville area)	America/Kentucky/Louisville
America/Kentucky/Monticello - Eastern - KY (Wayne)	America/Kentucky/Monticello
America/Kralendijk	America/Kralendijk
America/La_Paz	America/La_Paz
America/Lima	America/Lima
America/Los_Angeles - Pacific	America/Los_Angeles
America/Lower_Princes	America/Lower_Princes
America/Maceio - Alagoas, Sergipe	America/Maceio
America/Managua	America/Managua
America/Manaus - Amazonas (east)	America/Manaus
America/Marigot	America/Marigot
America/Martinique	America/Martinique
America/Matamoros - Central Time US - Coahuila, Nuevo Leon, Tamaulipas (US border)	America/Matamoros
America/Mazatlan - Mountain Time - Baja California Sur, Nayarit, Sinaloa	America/Mazatlan
America/Menominee - Central - MI (Wisconsin border)	America/Menominee
America/Merida - Central Time - Campeche, Yucatan	America/Merida
America/Metlakatla - Alaska - Annette Island	America/Metlakatla
America/Mexico_City - Central Time	America/Mexico_City
America/Miquelon	America/Miquelon
America/Moncton - Atlantic - New Brunswick	America/Moncton
America/Monterrey - Central Time - Durango; Coahuila, Nuevo Leon, Tamaulipas (most areas)	America/Monterrey
America/Montevideo	America/Montevideo
America/Montserrat	America/Montserrat
America/Nassau	America/Nassau
America/New_York - Eastern (most areas)	America/New_York
America/Nipigon - Eastern - ON, QC (no DST 1967-73)	America/Nipigon
America/Nome - Alaska (west)	America/Nome
America/Noronha - Atlantic islands	America/Noronha
America/North_Dakota/Beulah - Central - ND (Mercer)	America/North_Dakota/Beulah
America/North_Dakota/Center - Central - ND (Oliver)	America/North_Dakota/Center
America/North_Dakota/New_Salem - Central - ND (Morton rural)	America/North_Dakota/New_Salem
America/Ojinaga - Mountain Time US - Chihuahua (US border)	America/Ojinaga

America/Panama	America/Panama
America/Pangnirtung - Eastern - NU (Pangnirtung)	America/Pangnirtung
America/Paramaribo	America/Paramaribo
America/Phoenix - MST - Arizona (except Navajo)	America/Phoenix
America/Port_of_Spain	America/Port_of_Spain
America/Port-au-Prince	America/Port-au-Prince
America/Porto_Velho - Rondonia	America/Porto_Velho
America/Puerto_Rico	America/Puerto_Rico
America/Punta_Arenas - Region of Magallanes	America/Punta_Arenas
America/Rainy_River - Central - ON (Rainy R, Ft Frances)	America/Rainy_River
America/Rankin_Inlet - Central - NU (central)	America/Rankin_Inlet
America/Recife - Pernambuco	America/Recife
America/Regina - CST - SK (most areas)	America/Regina
America/Resolute - Central - NU (Resolute)	America/Resolute
America/Rio_Branco - Acre	America/Rio_Branco
America/Santarem - Para (west)	America/Santarem
America/Santiago - Chile (most areas)	America/Santiago
America/Santo_Domingo	America/Santo_Domingo
America/Sao_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)	America/Sao_Paulo
America/Scoresbysund - Scoresbysund/Itoqqortoormiit	America/Scoresbysund
America/Sitka - Alaska - Sitka area	America/Sitka
America/St_Barthelemy	America/St_Barthelemy
America/St_Johns - Newfoundland; Labrador (southeast)	America/St_Johns
America/St_Kitts	America/St_Kitts
America/St_Lucia	America/St_Lucia
America/St_Thomas	America/St_Thomas
America/St_Vincent	America/St_Vincent
America/Swift_Current - CST - SK (midwest)	America/Swift_Current
America/Tegucigalpa	America/Tegucigalpa
America/Thule - Thule/Pituffik	America/Thule
America/Thunder_Bay - Eastern - ON (Thunder Bay)	America/Thunder_Bay
America/Tijuana - Pacific Time US - Baja California	America/Tijuana
America/Toronto - Eastern - ON, QC (most areas)	America/Toronto
America/Tortola	America/Tortola
America/Vancouver - Pacific - BC (most areas)	America/Vancouver
America/Whitehorse - Pacific - Yukon (south)	America/Whitehorse
America/Winnipeg - Central - ON (west); Manitoba	America/Winnipeg
America/Yakutat - Alaska - Yakutat	America/Yakutat
America/Yellowknife - Mountain - NT (central)	America/Yellowknife
Antarctica/Casey - Casey	Antarctica/Casey
Antarctica/Davis - Davis	Antarctica/Davis



Antarctica/DumontD'Urville - Dumont-d'Urville	Antarctica/DumontD'Urville
Antarctica/Macquarie - Macquarie Island	Antarctica/Macquarie
Antarctica/Mawson - Mawson	Antarctica/Mawson
Antarctica/McMurdo - New Zealand time - McMurdo, South Pole	Antarctica/McMurdo
Antarctica/Palmer - Palmer	Antarctica/Palmer
Antarctica/Rothera - Rothera	Antarctica/Rothera
Antarctica/Syowa - Syowa	Antarctica/Syowa
Antarctica/Troll - Troll	Antarctica/Troll
Antarctica/Vostok - Vostok	Antarctica/Vostok
Arctic/Longyearbyen	Arctic/Longyearbyen
Asia/Aden	Asia/Aden
Asia/Almaty - Kazakhstan (most areas)	Asia/Almaty
Asia/Amman	Asia/Amman
Asia/Anadyr - MSK+09 - Bering Sea	Asia/Anadyr
Asia/Aqtau - Mangghystau/Mankistau	Asia/Aqtau
Asia/Aqtobe - Aqtobe/Aktobe	Asia/Aqtobe
Asia/Ashgabat	Asia/Ashgabat
Asia/Atyrau - Atyrau/Atirau/Gur'yev	Asia/Atyrau
Asia/Baghdad	Asia/Baghdad
Asia/Bahrain	Asia/Bahrain
Asia/Baku	Asia/Baku
Asia/Bangkok	Asia/Bangkok
Asia/Barnaul - MSK+04 - Altai	Asia/Barnaul
Asia/Beirut	Asia/Beirut
Asia/Bishkek	Asia/Bishkek
Asia/Brunei	Asia/Brunei
Asia/Chita - MSK+06 - Zabaykalsky	Asia/Chita
Asia/Choibalsan - Dornod, Sukhbaatar	Asia/Choibalsan
Asia/Colombo	Asia/Colombo
Asia/Damascus	Asia/Damascus
Asia/Dhaka	Asia/Dhaka
Asia/Dili	Asia/Dili
Asia/Dubai	Asia/Dubai
Asia/Dushanbe	Asia/Dushanbe
Asia/Famagusta - Northern Cyprus	Asia/Famagusta
Asia/Gaza - Gaza Strip	Asia/Gaza
Asia/Hebron - West Bank	Asia/Hebron
Asia/Ho_Chi_Minh	Asia/Ho_Chi_Minh
Asia/Hong_Kong	Asia/Hong_Kong
Asia/Hovd - Bayan-Olgii, Govi-Altai, Hovd, Uvs, Zavkhan	Asia/Hovd
Asia/Irkutsk - MSK+05 - Irkutsk, Buryatia	Asia/Irkutsk

Asia/Jakarta - Java, Sumatra	Asia/Jakarta
Asia/Jayapura - New Guinea (West Papua / Irian Jaya); Maluku/Moluccas	Asia/Jayapura
Asia/Jerusalem	Asia/Jerusalem
Asia/Kabul	Asia/Kabul
Asia/Kamchatka - MSK+09 - Kamchatka	Asia/Kamchatka
Asia/Karachi	Asia/Karachi
Asia/Kathmandu	Asia/Kathmandu
Asia/Khandyga - MSK+06 - Tomponsky, Ust-Maysky	Asia/Khandyga
Asia/Kolkata	Asia/Kolkata
Asia/Krasnoyarsk - MSK+04 - Krasnoyarsk area	Asia/Krasnoyarsk
Asia/Kuala_Lumpur - Malaysia (peninsula)	Asia/Kuala_Lumpur
Asia/Kuching - Sabah, Sarawak	Asia/Kuching
Asia/Kuwait	Asia/Kuwait
Asia/Macau	Asia/Macau
Asia/Magadan - MSK+08 - Magadan	Asia/Magadan
Asia/Makassar - Borneo (east, south); Sulawesi/Celebes, Bali, Nusa Tenggara; Timor (west)	Asia/Makassar
Asia/Manila	Asia/Manila
Asia/Muscat	Asia/Muscat
Asia/Nicosia - Cyprus (most areas)	Asia/Nicosia
Asia/Novokuznetsk - MSK+04 - Kemerovo	Asia/Novokuznetsk
Asia/Novosibirsk - MSK+04 - Novosibirsk	Asia/Novosibirsk
Asia/Omsk - MSK+03 - Omsk	Asia/Omsk
Asia/Oral - West Kazakhstan	Asia/Oral
Asia/Phnom_Penh	Asia/Phnom_Penh
Asia/Pontianak - Borneo (west, central)	Asia/Pontianak
Asia/Pyongyang	Asia/Pyongyang
Asia/Qatar	Asia/Qatar
Asia/Qostanay - Qostanay/Kostanay/Kustanay	Asia/Qostanay
Asia/Qyzylorda - Qyzylorda/Kyzylorda/Kzyl-Orda	Asia/Qyzylorda
Asia/Riyadh	Asia/Riyadh
Asia/Sakhalin - MSK+08 - Sakhalin Island	Asia/Sakhalin
Asia/Samarkand - Uzbekistan (west)	Asia/Samarkand
Asia/Seoul	Asia/Seoul
Asia/Shanghai - Beijing Time	Asia/Shanghai
Asia/Singapore	Asia/Singapore
Asia/Srednekolymsk - MSK+08 - Sakha (E); North Kuril Is	Asia/Srednekolymsk
Asia/Taipei	Asia/Taipei
Asia/Tashkent - Uzbekistan (east)	Asia/Tashkent
Asia/Tbilisi	Asia/Tbilisi
Asia/Tehran	Asia/Tehran
Asia/Thimphu	Asia/Thimphu

Asia/Tokyo	Asia/Tokyo
Asia/Tomsk - MSK+04 - Tomsk	Asia/Tomsk
Asia/Ulaanbaatar - Mongolia (most areas)	Asia/Ulaanbaatar
Asia/Urumqi - Xinjiang Time	Asia/Urumqi
Asia/Ust-Nera - MSK+07 - Oymyakonsky	Asia/Ust-Nera
Asia/Vientiane	Asia/Vientiane
Asia/Vladivostok - MSK+07 - Amur River	Asia/Vladivostok
Asia/Yakutsk - MSK+06 - Lena River	Asia/Yakutsk
Asia/Yangon	Asia/Yangon
Asia/Yekaterinburg - MSK+02 - Urals	Asia/Yekaterinburg
Asia/Yerevan	Asia/Yerevan
Atlantic/Azores - Azores	Atlantic/Azores
Atlantic/Bermuda	Atlantic/Bermuda
Atlantic/Canary - Canary Islands	Atlantic/Canary
Atlantic/Cape_Verde	Atlantic/Cape_Verde
Atlantic/Faroe	Atlantic/Faroe
Atlantic/Madeira - Madeira Islands	Atlantic/Madeira
Atlantic/Reykjavik	Atlantic/Reykjavik
Atlantic/South_Georgia	Atlantic/South_Georgia
Atlantic/St_Helena	Atlantic/St_Helena
Atlantic/Stanley	Atlantic/Stanley
Australia/Adelaide - South Australia	Australia/Adelaide
Australia/Brisbane - Queensland (most areas)	Australia/Brisbane
Australia/Broken_Hill - New South Wales (Yancowinna)	Australia/Broken_Hill
Australia/Currie - Tasmania (King Island)	Australia/Currie
Australia/Darwin - Northern Territory	Australia/Darwin
Australia/Eucla - Western Australia (Eucla)	Australia/Eucla
Australia/Hobart - Tasmania (most areas)	Australia/Hobart
Australia/Lindeman - Queensland (Whitsunday Islands)	Australia/Lindeman
Australia/Lord_Howe - Lord Howe Island	Australia/Lord_Howe
Australia/Melbourne - Victoria	Australia/Melbourne
Australia/Perth - Western Australia (most areas)	Australia/Perth
Australia/Sydney - New South Wales (most areas)	Australia/Sydney
Europe/Amsterdam	Europe/Amsterdam
Europe/Andorra	Europe/Andorra
Europe/Astrakhan - MSK+01 - Astrakhan	Europe/Astrakhan
Europe/Athens	Europe/Athens
Europe/Belgrade	Europe/Belgrade
Europe/Berlin - Germany (most areas)	Europe/Berlin
Europe/Bratislava	Europe/Bratislava
Europe/Brussels	Europe/Brussels

Europe/Bucharest	Europe/Bucharest
Europe/Budapest	Europe/Budapest
Europe/Busingen - Busingen	Europe/Busingen
Europe/Chisinau	Europe/Chisinau
Europe/Copenhagen	Europe/Copenhagen
Europe/Dublin	Europe/Dublin
Europe/Gibraltar	Europe/Gibraltar
Europe/Guernsey	Europe/Guernsey
Europe/Helsinki	Europe/Helsinki
Europe/Isle_of_Man	Europe/Isle_of_Man
Europe/Istanbul	Europe/Istanbul
Europe/Jersey	Europe/Jersey
Europe/Kaliningrad - MSK-01 - Kaliningrad	Europe/Kaliningrad
Europe/Kiev - Ukraine (most areas)	Europe/Kiev
Europe/Kirov - MSK+00 - Kirov	Europe/Kirov
Europe/Lisbon - Portugal (mainland)	Europe/Lisbon
Europe/Ljubljana	Europe/Ljubljana
Europe/London	Europe/London
Europe/Luxembourg	Europe/Luxembourg
Europe/Madrid - Spain (mainland)	Europe/Madrid
Europe/Malta	Europe/Malta
Europe/Mariehamn	Europe/Mariehamn
Europe/Minsk	Europe/Minsk
Europe/Monaco	Europe/Monaco
Europe/Moscow - MSK+00 - Moscow area	Europe/Moscow
Europe/Oslo	Europe/Oslo
Europe/Paris	Europe/Paris
Europe/Podgorica	Europe/Podgorica
Europe/Prague	Europe/Prague
Europe/Riga	Europe/Riga
Europe/Rome	Europe/Rome
Europe/Samara - MSK+01 - Samara, Udmurtia	Europe/Samara
Europe/San_Marino	Europe/San_Marino
Europe/Sarajevo	Europe/Sarajevo
Europe/Saratov - MSK+01 - Saratov	Europe/Saratov
Europe/Simferopol - MSK+00 - Crimea	Europe/Simferopol
Europe/Skopje	Europe/Skopje
Europe/Sofia	Europe/Sofia
Europe/Stockholm	Europe/Stockholm
Europe/Tallinn	Europe/Tallinn
Europe/Tirane	Europe/Tirane

Europe/Ulyanovsk - MSK+01 - Ulyanovsk	Europe/Ulyanovsk
Europe/Uzhgorod - Ruthenia	Europe/Uzhgorod
Europe/Vaduz	Europe/Vaduz
Europe/Vatican	Europe/Vatican
Europe/Vienna	Europe/Vienna
Europe/Vilnius	Europe/Vilnius
Europe/Volgograd - MSK+01 - Volgograd	Europe/Volgograd
Europe/Warsaw	Europe/Warsaw
Europe/Zagreb	Europe/Zagreb
Europe/Zaporozhye - Zaporozh'ye/Zaporizhia; Lugansk/Luhansk (east)	Europe/Zaporozhye
Europe/Zurich	Europe/Zurich
Indian/Antananarivo	Indian/Antananarivo
Indian/Chagos	Indian/Chagos
Indian/Christmas	Indian/Christmas
Indian/Cocos	Indian/Cocos
Indian/Comoro	Indian/Comoro
Indian/Kerguelen	Indian/Kerguelen
Indian/Mahe	Indian/Mahe
Indian/Maldives	Indian/Maldives
Indian/Mauritius	Indian/Mauritius
Indian/Mayotte	Indian/Mayotte
Indian/Reunion	Indian/Reunion
Pacific/Apia	Pacific/Apia
Pacific/Auckland - New Zealand (most areas)	Pacific/Auckland
Pacific/Bougainville - Bougainville	Pacific/Bougainville
Pacific/Chatham - Chatham Islands	Pacific/Chatham
Pacific/Chuuk - Chuuk/Truk, Yap	Pacific/Chuuk
Pacific/Easter - Easter Island	Pacific/Easter
Pacific/Efate	Pacific/Efate
Pacific/Enderbury - Phoenix Islands	Pacific/Enderbury
Pacific/Fakaofu	Pacific/Fakaofu
Pacific/Fiji	Pacific/Fiji
Pacific/Funafuti	Pacific/Funafuti
Pacific/Galapagos - Galapagos Islands	Pacific/Galapagos
Pacific/Gambier - Gambier Islands	Pacific/Gambier
Pacific/Guadalcanal	Pacific/Guadalcanal
Pacific/Guam	Pacific/Guam
Pacific/Honolulu - Hawaii	Pacific/Honolulu
Pacific/Kiritimati - Line Islands	Pacific/Kiritimati
Pacific/Kosrae - Kosrae	Pacific/Kosrae
Pacific/Kwajalein - Kwajalein	Pacific/Kwajalein

Pacific/Majuro - Marshall Islands (most areas)	Pacific/Majuro
Pacific/Marquesas - Marquesas Islands	Pacific/Marquesas
Pacific/Midway - Midway Islands	Pacific/Midway
Pacific/Nauru	Pacific/Nauru
Pacific/Niue	Pacific/Niue
Pacific/Norfolk	Pacific/Norfolk
Pacific/Noumea	Pacific/Noumea
Pacific/Pago_Pago	Pacific/Pago_Pago
Pacific/Palau	Pacific/Palau
Pacific/Pitcairn	Pacific/Pitcairn
Pacific/Pohnpei - Pohnpei/Ponape	Pacific/Pohnpei
Pacific/Port_Moresby - Papua New Guinea (most areas)	Pacific/Port_Moresby
Pacific/Rarotonga	Pacific/Rarotonga
Pacific/Saipan	Pacific/Saipan
Pacific/Tahiti - Society Islands	Pacific/Tahiti
Pacific/Tarawa - Gilbert Islands	Pacific/Tarawa
Pacific/Tongatapu	Pacific/Tongatapu
Pacific/Wake - Wake Island	Pacific/Wake
Pacific/Wallis	Pacific/Wallis

For more information on batch provisioning, see this [page](#).

# Provisioning - Columns

Below we will explain each column of the Provisioning tab:

Name	UUID	Progress	Status	Created	Actions
Batch 1	564D96D0-8157-C344-2387-84870C4AAB53	<div><div></div></div> 50%	<a href="#">Sending deploy</a>	August 19th 2020 - 11:31:55	
Batch 2	564DD38E-BB9D-7B6F-7754-463BB6696040	<div><div></div></div> 50%	<a href="#">Sending deploy</a>	August 19th 2020 - 11:31:55	
Provisioned Device	564D0345-F4E8-7E29-9CD9-030779AD9E0D	<div><div></div></div> 50%	<a href="#">Sending deploy</a>	August 19th 2020 - 11:31:55	

*Provisioning*

- **Name:** Displays the name of the registered provisioned Device;
- **UUID:** Displays the UUID of the registered Device;
- **Progress:** Displays a progress bar for device deployment;
- **Status:** Displays the current state of the device deployment;
- **Created:** Records the date and time when the device was added to this panel;
- **Actions:** The "Actions" menu consists of two buttons:
  - **Edit** : Allows you to edit the settings of the device added in the [Create Device](#) option or through Batch Provisioning;
  - **Delete** : Deletes the device.

# Backups Tab

In this tab is located the tool for managing backups and restores of UTM's, the function of this feature is to create routines through GSM and remotely perform backups in the firewalls API.

The backup routines are based on SMB, NTS, SFTP and USB Storages, in addition, before sending the backup creation instructions, the system checks if there is space available for storage and also checks if another routine is already being executed so as to ensure that there are no conflicts or overwriting. Although the storage directory and backup "order" is done by GSM, it doesn't save these files to local storage but to a remote server, backup routines are sent encrypted through a VPN tunnel. After transferring the files, in order to ensure the reliability of the data transmission, the integrity is verified through Checksum (MD5).

After creating backup routines, the administrator can remotely restore, download, or remove storage files.



For more information on GSM's own automatic backup routines, see this [page](#).

If you want to know more about creating storage devices, see this [page](#).

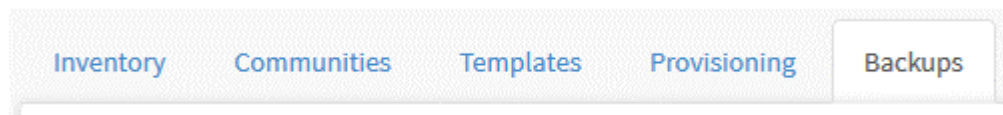


The device backup procedure is only available for version 2.0.1 or higher.



It is possible to consult the logs with more information regarding the backup procedure using the [\[debug-backup\]](#) command.

To access this resource, click on the Backups tab. As shown below:



Backups tab
















The Backups screen will appear. It consists of the "Names", "Last Backup", "Progress", "Status" and "Actions" columns. In addition, the [search bar](#) is located at the top of the screen and in the upper right corner of the screen is the [actions menu](#).

In this window, all items for registering system storage points will be available.



## Devices

[Inventory](#) [Communities](#) [Templates](#) [Provisioning](#) [Backups](#)

5 records							
<input type="checkbox"/>	Name	Last backup	Next backup	Progress	Status	Actions	
<input type="checkbox"/>	NFS BACKUP	26/10/2020 12:36	Unscheduled	<div><div></div></div> 66%	Running	<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	SFTP BACKUP	22/10/2020 11:36	22/11/2020 11:30	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	ONESHOT SFTP BACKUP	Not done	Unscheduled	<div><div></div></div> 0%	Waiting	<input checked="" type="checkbox"/>	  
<input type="checkbox"/>	MONTHLY USB BACKUP	21/10/2020 11:36	22/11/2020 11:30	<div><div></div></div> ✗	Error	<input type="checkbox"/>	  
<input type="checkbox"/>	TEST	Not done	Unscheduled	<div><div></div></div> 0%	Waiting	<input checked="" type="checkbox"/>	  
							< 1 > 10 / page ▾

### Backups

In this session we will analyze:

- [How to create single backups and recurring backup routines;](#)
- [How to edit backup routines;](#)
- [Column components of this screen.](#)

Next, we will detail the [actions menu](#).

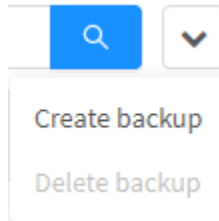
# Backups - Actions Menu

At the top right of the screen we have the actions menu:



Backups - Actions menu button

By clicking on this button the menu below is displayed:




Backups - Actions menu

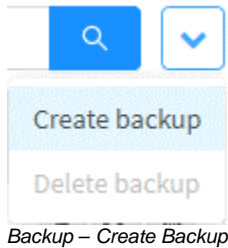
The menu has options:

- [Create Backup](#);
- [Delete Backup](#).

Next, we will detail each menu option.

# Backup - Actions menu - Create Backup

To create a backup, it will be necessary to select the storage point, on which devices the backup routines will be performed and also whether it will be single or recurring. Initially, click on [  ] and select the option **Create Backup**, as shown below:



The following window will be displayed:

Create Backup

General

\*

Name

Name

\*

Devices & Devices Group

Select a device

\*

Devices Group

Select a group

\*

Type

Snapshot

▼

\*

Remote Storage

Select a type

▼

\*

Number of backup retention

Number of backup retention

\*

% Disk usage retention

% Disk usage retention

Schedule

\*

Schedule

Select a type

▼

Cancel

Save

Backup – Create Backup

This window is divided into two panels:

- [General](#);
- [Schedule](#).

Next, we will detail each panel:

## General

The general panel consists of the following fields:

General

\* Name

Name

\* Devices & Devices Group

Select a device

\* Devices Group

Select a group

\* Type

Snapshot

\* Remote Storage

Select a type

\* Number of backup retention

Number of backup retention

\* Percent usage retention

Percent usage retention

Create Backup - General

- **Name:** Defines the name of the backup. Ex.: *System Backup - Daily - UTM Devices 2.1 - SMB*;
- **Device & Devices Group:** Determines which Device or Device group the backup will be applied to. The options that appear in this field are created on the [Inventory](#) tab. Ex.: *UTMDev-2.1*;
- **Type:** Defines whether to create a system backup or just a snapshot of the settings, the available options are:
  - **Snapshot** ("*.snapshot*" extension);
  - **System** ("*.system*" extension).
- **Remote Storage:** Defines the remote storage unit that will be used to save the backup, it is created in the [Storages](#) tab in System. Ex.: *Storage\_SMB*;



**WARNING:** It is recommended that the administrator segment the directories where the backups will be stored in order to prevent the backup files from being accidentally overwritten.

- **Number of Backup Retention:** Determines how many backups will be stored in the directory. At the end of this limit, the oldest backup is deleted. For example, if you choose "3", only the last 3 backups will be kept, so when a new backup is generated the routine will be executed to delete the oldest one, always respecting the value added in this field. Ex.: 1;
- **Percent usage retention:** Defines the percentage of usage that the directory created within the storage will use when saving the backup. If the limit is reached, backup rotation is performed, removing the oldest one in order to always keep the most recent backups. If a directory has 100 GB and 30% retention is chosen, when the records occupy 30 GB the rotation will be activated, otherwise the retention number will be verified. Ex.: 100%;



The system acts first by checking if the usage percentage has been reached and then checking the number of backups retained. Consequently:

1. If you still have free space, the system will check the number of backups retained.
2. If the maximum retention amount has not been reached, the backup storage will continue to function normally without deleting previous records.

Analyzing the opposite scenario, the performance of the system will be as explained below:

1. If the space limit is reached, rotation will be activated to keep only the most recent backups;
2. If disk space still exists, but the number of backups retained exceeds the limit set by the administrator, the oldest records will be removed, respecting the value defined in the field, so that the directory always has the most recent backups.



If the administrator does not want the percentage to be considered, simply add the value "100" so that the space is fully used before activating the rotation. In this way, only the number of backups retained will be considered.

## Schedule

The schedule panel consists of the following fields:

Schedule

\* Schedule

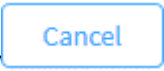

Select a type

Create Backup - Schedule

- **Schedule:** Allows you to determine the frequency at which the backup will be created. The available options are:
  - **Oneshot:** Defines that the backup will be done only once. When selecting this option, the Date and time field will be displayed;
    - **Date and time:** This field has the function of scheduling when the Backup will be executed.
  - **Daily:** Defines that the backup will be made daily. When selecting this option, the Hour field will be displayed;
    - **Hour:** This field has the function of scheduling the time at which the Backup will be performed.
  - **Weekly:** Defines that the backup will be made weekly. When selecting this option, the Weekday and Hour fields will be displayed;
    - **Weekday:** This field has the function of scheduling the day of the week on which the Backup will be executed;
    - **Hour:** This field has the function of scheduling the time at which the Backup will be performed.
  - **Monthly:** Defines that the backup will be made once a month. When selecting this option, the Month day and Hour fields will be displayed;
    - **Month day:** This field has the function of scheduling the day of the month on which the Backup will be executed;
    - **Hour:** This field has the function of scheduling the time at which the Backup will be performed.

Cancel

Save


When finished, click [  ] to cancel or [  ] to save the backup routine.

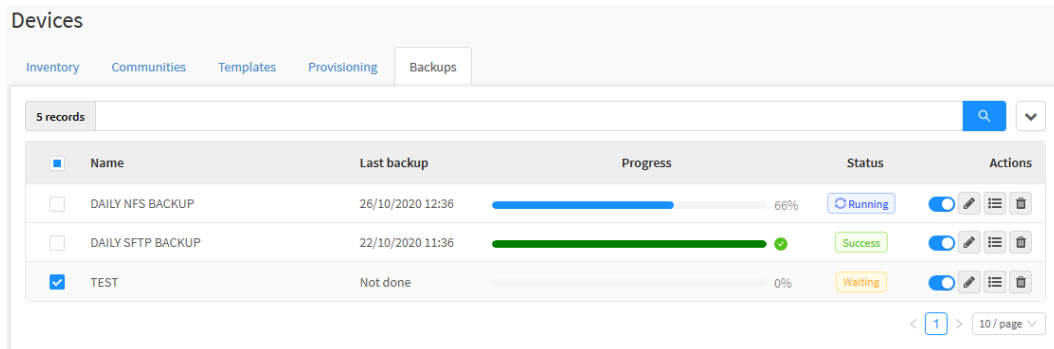
After making these settings, the storage points will have been defined in the system and the backup routines for the devices will be created and listed in the [columns](#).










Below we will detail how to [remove the backups](#).

# Backup - Actions menu - Delete Backup


Through the "Delete" button it is possible to delete several Backup Routines at the same time. To delete via the actions menu, follow these steps:

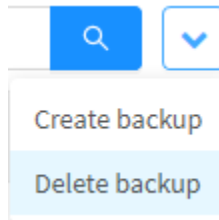
1. Select which Backup you want to remove by clicking [>], as shown below:



<input type="checkbox"/>	Name	Last backup	Progress	Status	Actions
<input type="checkbox"/>	DAILY NFS BACKUP	26/10/2020 12:36	<div><div></div></div> 66%	Running	  
<input type="checkbox"/>	DAILY SFTP BACKUP	22/10/2020 11:36	<div><div></div></div> 100%	Success	  
<input checked="" type="checkbox"/>	TEST	Not done	<div><div></div></div> 0%	Waiting	  

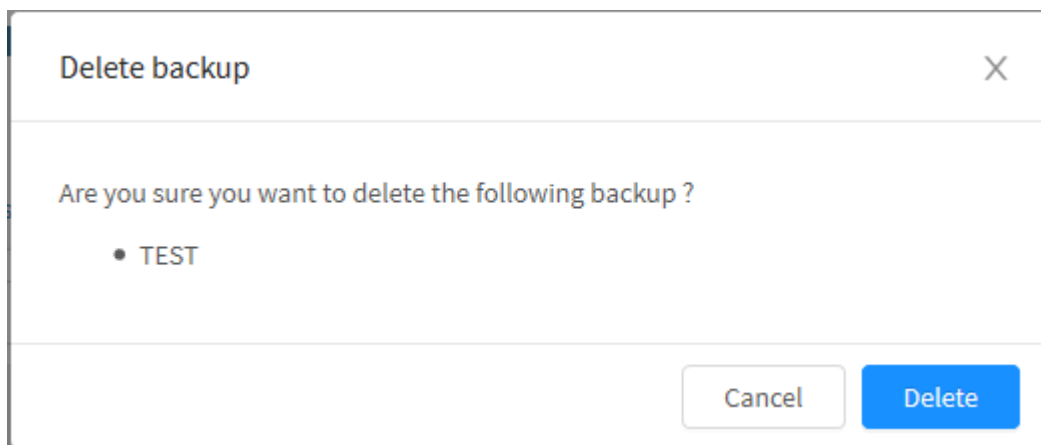
Backups – Selection of Backup Routines to be deleted

2. Enter the **Actions menu** [>] and click on the option "Delete Backup";

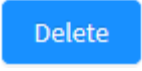
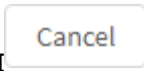


Backups – Delete backup.


3. The message will appear if you really want to delete the selected items;



Backups – Delete Backup



If you wish to cancel, click on the [ ] button. To finish, click on the [ ] button.

 Backup deleted successfully

*Backup deleted successfully*

After performing these procedures, the backups will be successfully deleted.





















# Backups - Columns

Below we will explain each column of the Backups tab:

Devices



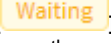
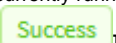





Inventory Communities Templates Provisioning Backups

5 records

<input type="checkbox"/>	Name	Last backup	Next backup	Progress	Status	Actions
<input type="checkbox"/>	NFS BACKUP	26/10/2020 12:36	Unscheduled	<div><div></div></div> 66%	Running	   
<input type="checkbox"/>	SFTP BACKUP	22/10/2020 11:36	22/11/2020 11:30	<div><div></div></div> 100%	Success	   
<input type="checkbox"/>	ONESHOT SFTP BACKUP	Not done	Unscheduled	<div><div></div></div> 0%	Waiting	   
<input type="checkbox"/>	MONTHLY USB BACKUP	21/10/2020 11:36	22/11/2020 11:30	<div><div></div></div> 0%	Error	   
<input type="checkbox"/>	TEST	Not done	Unscheduled	<div><div></div></div> 0%	Waiting	   

< 1 > 10 / page


Backups

- **Name:** Displays the name of the Backup routine;
- **Last backup:** Displays when the last backup was performed;
- **Next backup:** Following what was configured in the schedule, it shows when the next backup will be performed;
- **Progress:** Displays a progress bar and a percentage for running Backup;
- **Status:** Displays the current status of the Backup routine execution, which can be:
  - **Running** : The backup routine is currently running;
  - **Error** : Something went wrong that caused the backup routine to fail;
  - **Waiting** : *Routine is in waiting time.* This can occur when the system detects a process that may interfere with the backup that is currently running (for example, another backup routine);
  - **Success** : The backup was successful;
- **Actions:** The "Actions" menu consists of buttons:
  - **Disable**  / **Enable Backup** : This option disables or enables the backup schedule. *When disabling scheduling, previous backups are not removed;*
  - **Edit** : Allows you to edit the settings of the backup added in the [Create Backup](#) option;
  - **Backup Details** : *Displays more information about backup routines, see this [page](#) for more information;*
  - **Delete** : Deletes the backup routine, is the equivalent of the [Delete Backup](#) option.

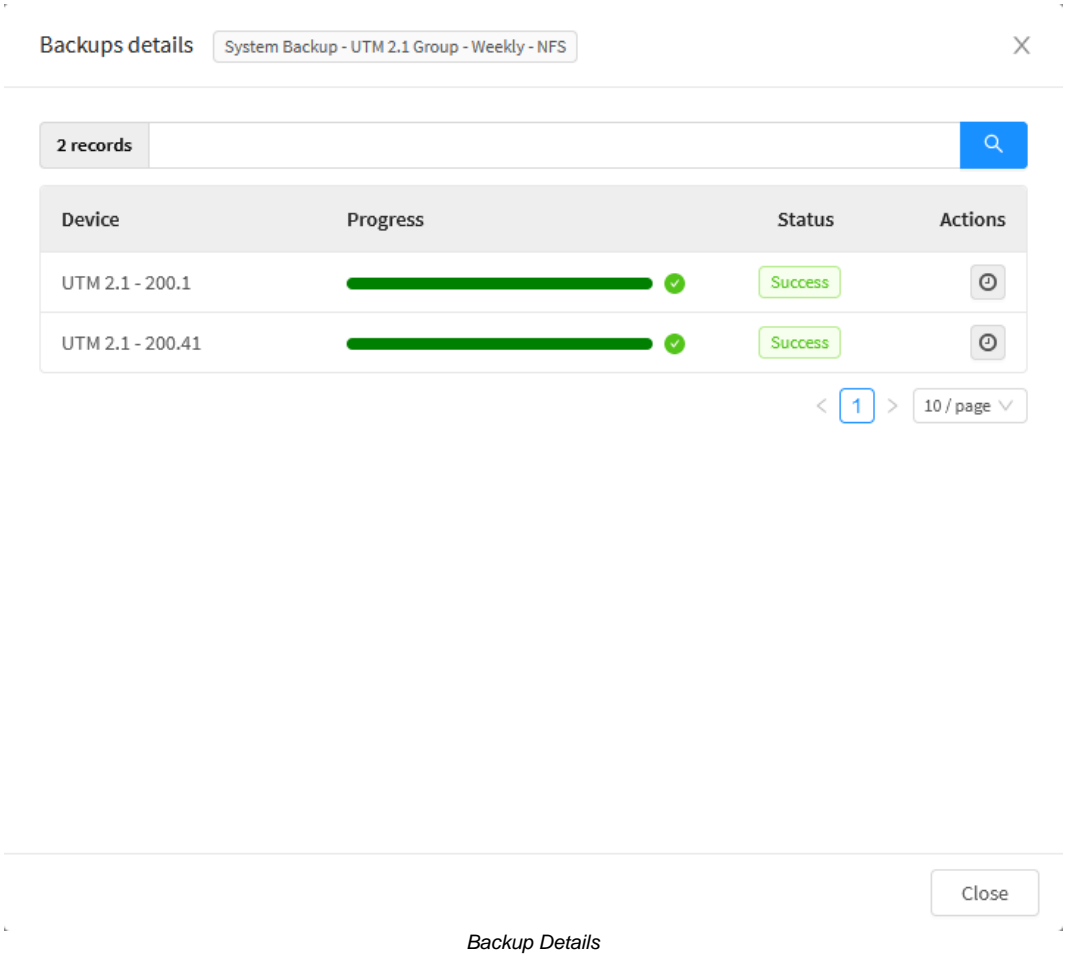
For more details on the backups tab, see this [page](#).








# Backups - Backup Details

The panel displayed when clicking the **Backup Details** [  ] button has the function of detailing the progress of the execution of the backup routines on each device associated with the backup routine.

The Backup details panel consists of the following fields:




- **Device:** Displays the name of the Device routine;
- **Progress:** Displays a progress bar and a percentage for running Backup;
- **Status:** Displays the current status of the Backup routine execution, which can be:
  - [  ]: The backup routine is currently running;
  - [  ]: Something went wrong that caused the backup routine to fail;
  - [  ]: The routine is in waiting time. This can occur when the system detects a process that might interfere with the backup that is currently running (for example, another backup routine);
  - [  ]: The backup was successful;
- **Actions:** The “Actions” menu consists of the button:
  - **Backups History** [  ]: This button has the function of detailing the backup history, for more information, see this [page](#).













Next, we will detail the [Backups History](#) button;

For more information on the columns, visit this [page](#).

# Backups - Backups Details - Backup History

The panel displayed when clicking on the **Backup History**  button has the function of displaying the history of the Backup routines performed on a given device. It consists of the following fields:








Backups history UTM 2.1 - 200.41 X

Name	Size	Last status	Status	Actions
B135-A5AC-A24C-DF29-2.1.0-202103101231.snapshot	18.64 MB	10/03/2021 12:31	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103091231.snapshot	18.64 MB	09/03/2021 12:31	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103091201.snapshot	18.64 MB	09/03/2021 12:01	Success	  
B135-A5AC-A24C-DF29-2.1.0-202103081541.snapshot	18.64 MB	08/03/2021 15:41	Success	  

< 1 > 10 / page

Close

## Backup History

- **Name:** Backup procedure name, in the example above, we have snapshots;
- **Size:** Displays the size of the backup procedure;
- **Last Status:** Defines when the last status change occurred;
- **Status:** Displays the current status of the Backup routine execution, which can be:
  -  **Running**: The backup routine is currently running;
  -  **Error**: Something went wrong that caused the backup routine to fail;
  -  **Waiting**: The routine is in waiting time. This can occur when the system detects a process that might interfere with the backup that is currently running (for example, another backup routine);
  -  **Success**: The backup was successful;
- **Actions:** The "Actions" menu consists of two buttons:
  -  **Restore**: When you click this button, the backup procedure is performed again. If a backup is removed from the directory, it will remain recorded in the history, but this option will be disabled;
  -  **Download**: By clicking on this button, you can download the snapshot;
  -  **Delete**: When you click this button, the backup is removed from the history.

For more information on the columns, visit this [page](#).

# Example - Device Backup

This section will present the step by step for configuring Device Backups.



For more information on Backups, see this [page](#).

This demonstration will consider the following scenarios:

Device Backup - Scenarios considered

Backup routines name	Scenario
System Backup - UTM 2.1 Group - Weekly - NFS-02	Weekly NFS System Backup
System Backup - UTM 2.1 Group - Daily - NFS-01	Daily NFS System Backup
Snapshot Backup - UTM 2.1 Group - Daily - NFS-02	Daily NFS Snapshot Backup
Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01	Weekly SFTP Snapshot Backup
Snapshot Backup - UTM 200.41 - Single Time - SFTP-01	Single SFTP Snapshot Backup

The following devices will be used in this example:

Device Backup - Devices used

Device Name	Device Group
UTM 2.1 - 200.1	UTM 2.1 Group
UTM 2.1 - 200.41	

The following Storages will be used in this example:

Device Backup - Storages used

Nome	IP
Storage_NFS_01	172.16.102.200
Storage_NFS_02	172.31.160.30
Storage_SFTP_01	172.31.160.31

The steps we will take in this demonstration will be:

- [Inclusion of Devices](#);
- [Creation of Storages](#);
- [Backup Routines Creation](#);
- [Validation of settings](#).

We will start the demo by adding the [devices to the inventory](#).

# Device Backup - Inclusion of Devices

This section will present the step-by-step for configuring Backups.



For more information on adding Devices, see the [page](#) on the Inventory tab.

The steps we will take in this demonstration will be:

- [Addition of Device UTM 2.1 - 200.1](#);
- [Addition of Device UTM 2.1 - 200.41](#).

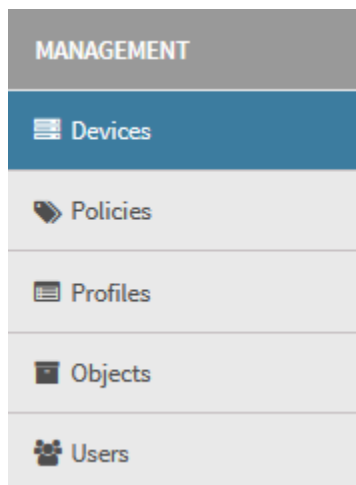
The following Devices will be used in this example:

Device Backup - Devices used

Name	Group
UTM 2.1 - 200.1	UTM 2.1 Group
UTM 2.1 - 200.41	

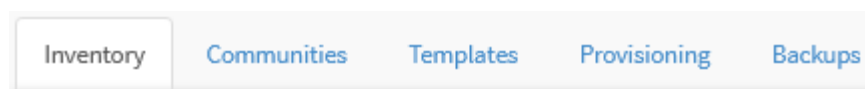
This session will not detail the process of installing and registering devices on GSM, for more in-depth information about these procedures, see the instructions on this [page](#).

Access the Management menu and click on the Devices option:



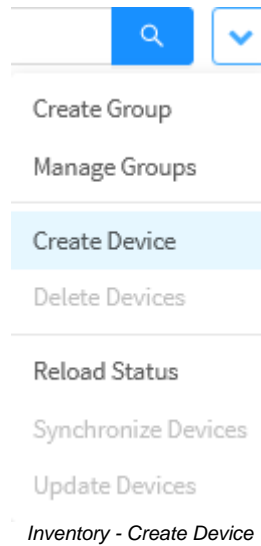
Management - Devices

Click the Inventory tab:



Inventory Tab

Click on the **Actions Menu** [  ] icon and select the "Create Device" option;



Initially we will add the Device "UTM 2.1 - 200.1":

## Addition of Device UTM 2.1 - 200.1

Complete the form as shown below:

Add Device

X

\* Name

UTM 2.1 - 200.1

\* Company

Blockbit QA

\* Deploy Key

53616c7465645f5fae71eb02a17a5d94c92c040ff40cf8dc43412c6e06e4b4d4a055f258e4  
0354841d548f92c6ab29d68dd21f863a59b4f72e16d999e11d90cf6cf6ef66b67d17064fd  
deba6705ac64f6e1b04b34237535a2959be5f0dc5709f0799a93c7bccode13d8130eacac

\* API Key

870eb285442b834592efbc5d55f4eeb0

\* User Admin

admin

Password

.....

Device Group

UTM 2.1 Group

Logger

Remote Logger - 200.30


Description

Cancel

Save

#### Inventory - Add Device

- **Name:** We will name the device "UTM 2.1 - 200.1";
- **Company:** In this field we will use "Blockbit QA";
- **Deploy Key:** We will use the deployment key obtained from the Central Management of the UTM in question;
- **API Key:** We will also use the API Key obtained from the UTM Central Management;
- **User Admin:** Add the UTM user with administrative permissions to access via GSM;
- **Password:** Add the UTM user password with administrative permissions to access via GSM;
- **Device Group:** In this example we will add the device to the "UTM 2.1 Group" group;
- **Logger:** In this example we will not be dealing with Logger, so this field is optional;
- **Description:** We will not add a description.

Click  to save the settings.

Next, we will configure the device "UTM 2.1 - 200.41":

## Addition of Device UTM 2.1 - 200.41

We will use the following settings:

Add Device
X

\* Name

UTM 2.1 - 200.41

\* Company

Blockbit QA

\* Deploy Key

53616c7465645f5d521f743a467c4a6751fc30f77f581100f7be38547c4459f1039bcab4fc  
1354fc3f3fd1588d99a2a5a736f2552e653a2f4cd9b3839d2191f32f540e64b0ea5b7f3293  
50635b3b947da09b876e0c94e4647f252e56ec7a91eaecaa503e8299f374052862acb4cc

\* API Key

9ed9ebc2047978f87471837059c9312f

\* User Admin

admin

Password

.....

Device Group

Grupo UTM 2.1

Logger

Logger Remoto - 200.30

Description

Cancel

Save

Inventory - Add Device

- **Name:** We will name the device "UTM 2.1 - 200.41";
- **Company:** In this field we will use "Blockbit QA";
- **Deploy Key:** We will use the deployment key obtained from the Central Management of the UTM in question;
- **API Key:** We will also use the API Key obtained from the UTM Central Management;
- **User Admin:** Add the UTM user with administrative permissions to access via GSM;
- **Password:** Add the UTM user password with administrative permissions to access via GSM;
- **Device Group:** In this example we will add the device to the "UTM 2.1 Group" group;
- **Logger:** In this example we will not be dealing with Logger, so this field is optional;
- **Description:** We will not add a description.

Save

We will not configure the other fields, click [ Save ] to save the settings.

When finishing all the configurations, the screen will be as shown below:

Devices

Inventory

Communities

Templates

Provisioning

Backups

5 records

☐

Name

Group

Model

License Status

Version

Template

Policy IPv4

Policy IPv6

Actions

<input type="checkbox"/>	UTM 2.1 - 200.1	Grupo UTM 2.1	BBv-10	E0C4-385A-A41B-4DAA	BLOCKBIT UTM 2.1.0 build 21030815				
<input type="checkbox"/>	UTM 2.1 - 200.41	Grupo UTM 2.1	BBv-10	B135-A5AC-A24C-DF29	BLOCKBIT UTM 2.1.0 build 21030815				

<

1

>

10 / page

## Loggers - Loggers

This finalizes the configuration of the devices, next we will [create the storages](#).



# Device Backup - Storage Creation

After [adding the devices](#), in this step we will perform the following steps:

- **Object Creation;**
  - [Creating the Storage\\_NFS\\_01 IP Object;](#)
  - [Creating the Storage\\_NFS\\_02 IP Object;](#)
  - [Creation of the IP Object Storage\\_SFTP\\_02.](#)
- **Storages Configuration;**
  - [Storage\\_NFS\\_01 creation;](#)
  - [Storage\\_NFS\\_02 creation;](#)
  - [Storage\\_SFTP\\_01 creation.](#)

In this step we will detail the installation of the Storages used by Backup, the following Storages will be used in this example:



This example will assume that the storage that will be used by the administrator is installed and configured correctly. For more information about Blockbit GSM compatibility with remote storage see this [page](#).

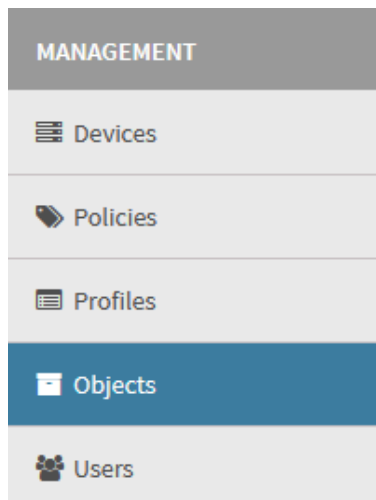
Device Backup - Storages used

Name	IP
Storage_NFS_01	172.16.102.200
Storage_NFS_02	172.31.160.30
Storage_SFTP_01	172.31.160.31

Initially we will generate the IPs that will be used by the Storages.

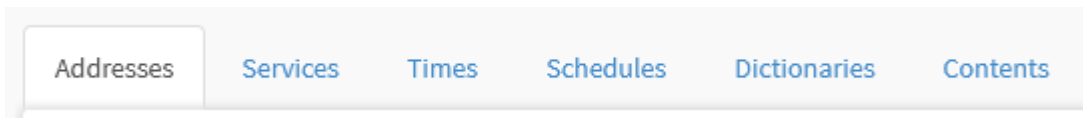
## Object Creation

First, we will create the Single IP Objects that will be used to connect to the Remote Storages, so access the Management menu and click on the Objects option:



Management - Objects

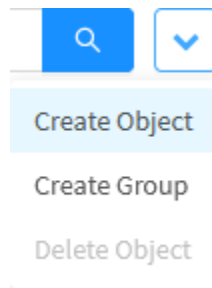
Click on the Addresses tab:



Addresses tab

### ***Creating the Storage\_NFS\_01 IP Object***

Click on the **Actions Menu** [  ] icon and select the “Create Object” option;



*Inventory - Create Device*

Initially we will add the Storage\_NFS\_01 IP, complete the form as shown below:

Create Addresses Object

X

---

\* Name

Storage\_NFS\_01

\* Type

IPv4 Address

☒ Unique

\* Address

172.16.102.200

Mask

255.255.255.255

+

^

v

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** We will use the name "Storage\_NFS\_01";
- **Type:** Select the "IPv4 Address" option;
- **Unique** ☒: This will be an object of a unique type, so be sure to check this checkbox;
- **Address:** The Storage address is "172.16.102.200";
- **Mask:** The mask can remain the default;
- **Description:** In this example, we will not add a description.

Click  to save the settings.

### Creating the Storage\_NFS\_02 IP Object

In addition, we will add the Storage\_NFS\_02 IP, complete the form as shown below:

Create Addresses Object

X

---

\* Name

Storage\_NFS\_02

\* Type

IPv4 Address

☒ Unique

\* Address

172.31.160.30

Mask

255.255.255.255

+

^

v

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** We will use the name "Storage\_NFS\_02";
- **Type:** Select the "IPv4 Address" option;
- **Unique** ☒: This will be an object of a unique type, so be sure to check this checkbox;
- **Address:** The Storage address is "172.31.160.30";
- **Mask:** The mask can remain the default;
- **Description:** In this example, we will not add a description.

Click  to save the settings.

### Creation of the IP Object Storage\_SFTP\_02

In addition, we will add the Storage\_SFTP\_02 IP, complete the form as shown below:

Create Addresses Object

X

\* Name

Storage\_SFTP\_02

\* Type

IPv4 Address

☒ Unique

\* Address

172.31.160.31

Mask

255.255.255.255

+

^

v

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

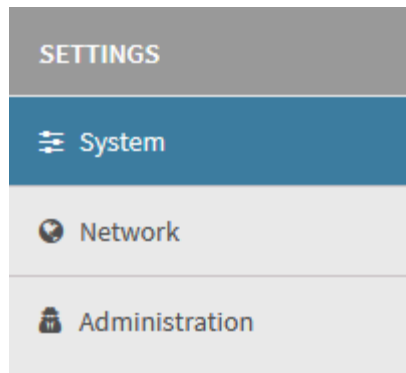
- **Name:** We will use the name "Storage\_SFTP\_02";
- **Type:** Select the "IPv4 Address" option;
- **Unique** ☒: This will be an object of a unique type, so be sure to check this checkbox;
- **Address:** The Storage address is "172.31.160.31";
- **Mask:** The mask can remain the default;
- **Description:** In this example, we will not add a description.

Click  to save the settings.

After creating the address objects, we will create the Storages.

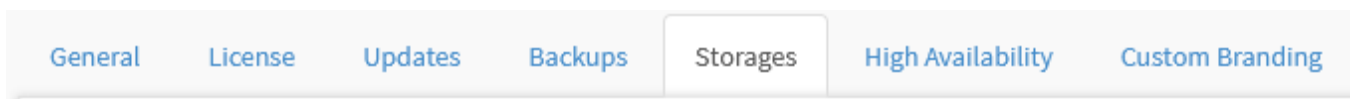
## Configuring the Storages

Access the Settings menu and click on the option System:



Settings - System


Access the Storages tab:

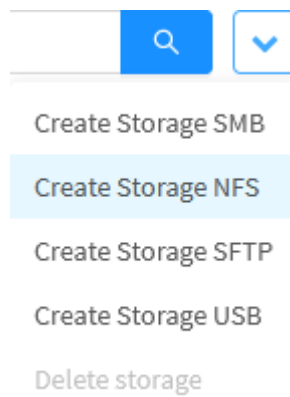


Storages tab

We will create two NFS Storages and one SFTP.

### ***Storage\_NFS\_01 creation***

We will start creating the NFS Storages, click on the Actions Menu icon [  ] and select the option "Create Storage NFS";



Storages - Create Storages NFS

Initially we will add Storage\_NFS\_01, complete the form as shown below:

Create Storage NFS

×

\* Description

Storage\_NFS\_01

\* IP

Storage\_NFS\_01

\* Directory

/home/bkp-nfs/User/nfs-200.30

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

☐ Protocol TCP

☐ Disable locking

☐ Enable posix

Operation Mode

☒ Hard ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel


Save

Storages - Create Storage NFS

In this window we will just configure the following fields:

- **Description:** In this example, we will name the storage "Storage\_NFS\_01";
- **IP:** Select the IP address of the NFS server configured in the previous step, in this case we will use the object "Storage\_NFS\_01";
- **Directory:** We will use the /home/bkp-nfs/User/nfs-200.30 directory.

The other fields can be kept with the default configuration.

Click  to save the settings.

## Storage\_NFS\_02 creation

Again, we will create an NFS Storages, click on the **Actions Menu**  icon and select the option "Create Storage NFS";

Create Storage SMB

Create Storage NFS

Create Storage SFTP

Create Storage USB

Delete storage

Storages - Create Storages NFS

Initially we will add Storage\_NFS\_02, complete the form as shown below:

Create Storage NFS

✕

\* Description

Storage\_NFS\_02

\* IP

Storage\_NFS\_02

▼

\* Directory

/bkp-blockbit-nfs/user/nfs-200.30

Reading Bytes

Writing Bytes

Port

Block sizes Bytes

4096

4096

2049

☐ Protocol TCP
 ☐ Disable locking
 ☐ Enable posix

Operation Mode

☒ Hard
 ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storages - Create Storage NFS

In this window we will just configure the following fields:

- **Description:** In this example we will name the storage "Storage\_NFS\_02";
- **IP:** Select the IP address of the NFS server configured in the previous step, in this case we will use the object "Storage\_NFS\_02";
- **Directory:** We will use the "/bkp-blockbit-nfs/user/nfs-200.30" directory.

The other fields can be kept with the default configuration.

Click 


Save



 to save the settings.



### Creation of Storage\_SFTP\_01

Finally, we will create an SFTP Storages, click on the **Actions Menu** [  ] icon and select the option “Create Storage SFTP”;

ns Menu [  ] icon and select t

Create Storage SMB

Create Storage NFS

Create Storage SFTP

Create Storage USB

Delete storage

Storages - Create Storages SFTP

Initially we will add Storage\_SFTP\_01, complete the form as shown below:

Create Storage SFTP

X

\* Description

Storage\_SFTP\_01

\* User

root

\* IP

Storage\_SFTP\_02

▼

\* Port

SSH

▼

\* Directory

/bkp-blockbit-ssh/user/ssh-200.31

\* Simultaneous transfers

5

☐ Compression

☐ Only Logger

Cancel

Save

## Storages - Create Storage SFTP

- **Description:** In this example, we will name the storage "Storage\_SFTP\_01";
- **User:** Add the administrative user "root";
- **IP:** Select the IP address of the NFS server configured in the previous step, in this case we will use the object "Storage\_SFTP\_01";
- **Port:** The access category will be "SSH";
- **Directory:** We will use the "/bkp-blockbit-ssh/user/ssh-200.3.3" directory.
- **Simultaneous transfers:** We can leave it as "5";
- **Compression** [ ☐ ]: We will not use this option;
- **Only Logger** [ ☐ ]: We will not use this option.

Save

Click on [ ] to save the settings.

To finish all the configurations, a fabric similar to that shown below:

System

GeneralLicenseUpdatesBackupsStoragesHigh AvailabilityCustom Branding

4 records

Description

Type

Size

Actions

Storage\_NFS\_01

NFS

52%

Storage\_NFS\_02

NFS

45%

Storage\_SFTP\_02

SFTP

45%

<

1

>

10 / page

System - Storages

Not next step, we will create [Backup routines](#).

# Device Backup - Creation of Backup Routines

After creating the [storages](#), we will go deeper into the backup routines:

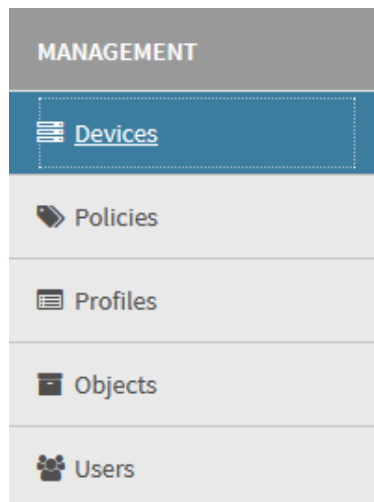
- [Weekly NFS System Backup Creation](#);
- [Daily NFS System Backup Creation](#);
- [Daily NFS Snapshot Backup Creation](#)
- [Weekly SFTP Snapshot Backup Creation](#);
- [Single SFTP Snapshot Backup Creation](#);

The following backup routines will be created in this example:

Device Backup - Backups

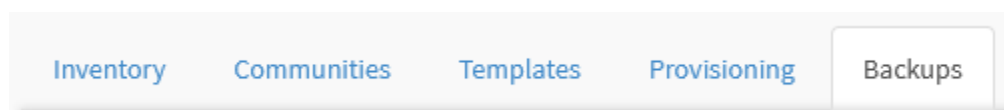
Name
System Backup - UTM 2.1 Group - Weekly - NFS-02
System Backup - UTM 2.1 Group - Daily - NFS-01
Snapshot Backup - UTM 2.1 Group - Daily - NFS-02
Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01
Snapshot Backup - UTM 200.41 - Single Time - SFTP-01

Initially, access the Management menu and click on the Devices option:



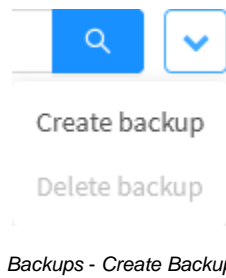
Management - Devices

Click on the "Backups" tab:



Devices - Backups Tab

Click on the **Actions Menu** [  ] icon and select the “Create Backup” option;



## Weekly NFS System Backup Creation

We will start by creating a Weekly Backup:

Create Backup

General

\*

Name

System Backup - UTM 2.1 Group - Weekly - NFS-02

Devices

Select a device

\* Devices Group

UTM 2.1 Group X

\* Type

System

\* Remote Storage

Storage\_NFS\_02

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

\* Schedule

Weekly

\* Weekday

Sunday

\* Hour

16:00

Cancel

Save

Backups - Create Backup

272

- **Name:** In this example we will name the backup "System Backup - UTM 2.1 Group - Weekly - NFS-02";
- **Device & Devices Group:** We will use the device group "UTM 2.1 Group";
- **Type:** In this example we will use the type: "System";
- **Remote Storage:** We will select "Storage\_NFS\_02";
- **Number of Backup Retention:** In this case we will configure it so that only 1 backup will be retained;
- **Percent usage retention:** We will use 100% of the directory space, so that there is no limitation;
- **Schedule:** The schedule will be weekly, so we will select the option "Weekly";
- **Weekday:** Choose the day when the backup will be made, in this case "Sunday";
- **Hour:** Finally, select the time at which it will be done, in this example, it will be at 16:00.

Save

Click [ ] to save the settings.

## Daily NFS System Backup Creation

Next, we will create a Daily Backup:

Create Backup
X

General

\* Name

System Backup - UTM 2.1 Group - Daily - NFS-01

Devices

UTM Dev - 2.1.0 X

Devices Group

UTM 2.1 Group X

\* Type

System

\* Remote Storage

Storage\_NFS\_01

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

\* Schedule

Daily

\* Hour

18:00

Cancel
Save

Backups - Create Backup

- **Name:** In this example we will name the backup as "System Backup - UTM 2.1 Group - Daily - NFS-01";

- **Device & Devices Group:** We will use the device group "UTM 2.1 Group";
- **Type:** In this example we will use the type: "System";
- **Remote Storage:** We will select "Storage\_NFS\_01";
- **Number of Backup Retention:** In this case we will configure it so that only 1 backup will be retained;
- **Percent usage retention:** We will use 100% of the directory space, so that there is no limitation;
- **Schedule:** The schedule will be daily, so we will select the option "Daily";
- **Hour:** Finally, select the time at which it will be done, in this example, it will be at "18:00".

Save

Click [ ] to save the settings.

## Daily NFS Snapshot Backup Creation

Next, we will create a Daily Snapshot Backup:

Create Backup

General

\* Name

Snapshot Backup - UTM 2.1 Group - Daily - NFS-02

Devices

Select a device

\* Devices Group

UTM 2.1 Group X

\* Type

Snapshot

\* Remote Storage

Storage\_NFS\_02

Number of Backup Retention

2

Percent Usage Retention

100

Schedule

\* Schedule

Daily

\* Hour

12:30

Cancel

Save

Backups - Create Backup

- **Name:** In this example we will name the backup as "Snapshot Backup - UTM 2.1 Group - Daily - NFS-02";
- **Device & Devices Group:** We will use the device group "UTM 2.1 Group";
- **Type:** In this example we will use the type: "Snapshot";
- **Remote Storage:** We will select "Storage\_NFS\_02";

- **Number of Backup Retention:** In this case we will configure so that there is retention of 2 backups;
- **Percent usage retention:** We will use 100% of the directory space, so that there is no limitation;
- **Schedule:** The schedule will be daily, so we will select the option "Daily":
- **Hour:** Finally, select the time when it will be done, in this example, it will be at "12:30".

Save

Click [ ] to save the settings.

## Weekly SFTP Snapshot Backup Creation

Next, we will create a Weekly Snapshot Backup:

Edit Backup
X

General

Name

Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01

Devices

UTM 2.1 - 200.41 X

3 X

Devices Group

Select a group

Type

Snapshot

Remote Storage

Storage\_SFTP\_01

Number of Backup Retention

2

Percent Usage Retention

20

Schedule

Schedule

Weekly

Weekday

Monday

Hour

15:55

Cancel
Save

Backups - Create Backup

- **Name:** In this example we will name the backup as "Snapshot Backup - UTM 2.1 Group - Weekly - SFTP-01";
- **Device & Devices Group:** We will use the device "UTM 2.1 - 200.41";
- **Type:** In this example we will use the type: "Snapshot";
- **Remote Storage:** We will select "Storage\_SFTP\_01";
- **Number of Backup Retention:** In this case we will configure so that there is retention of 2 backups;
- **Percent usage retention:** In this case we will use 20% of the directory space;

- **Schedule:** The schedule will be daily, so we will select the option "Weekly";
- **Weekday:** Choose the day when the backup will be made, in this case "Monday";
- **Hour:** Finally, select the time when it will be done, in this example, it will be at 15:55.

Save

Click [ ] to save the settings.

## Single SFTP Snapshot Backup Creation

Finally, we will create a single Snapshot Backup:

Edit Backup
X

General

\* Name

Snapshot Backup - UTM 200.41 - Single Time - SFTP-01

\* Devices

UTM 2.1 - 200.41 X

Devices Group

Select a group

\* Type

Snapshot

\* Remote Storage

Storage\_SFTP\_01

Number of Backup Retention

1

Percent Usage Retention

100

Schedule

\* Schedule

Oneshot

\* Date and time

08/03/2021 17:08

Cancel
Save

Backups - Create Backup

- **Name:** In this example we will name the backup as "Snapshot Backup - UTM 200.41 - Single Time - SFTP-01";
- **Device & Devices Group:** We will use the device "UTM 2.1 - 200.41";
- **Type:** In this example we will use the type: "Snapshot";
- **Remote Storage:** We will select "Storage\_SFTP\_01";
- **Number of Backup Retention:** In this case we will configure so that there is retention of 1 backups;
- **Percent usage retention:** In this case we will use 100% of the directory space;
- **Schedule:** This will be a single snapshot, so we'll select the "Oneshot" option;



- **Date and Time:** Choose the day and time when the backup will be made, in this case "08/03/2021 17:08".

Save

Click [ ] to save the settings.

When finishing all the configurations, the screen will be as shown below:

Devices

Inventory Communities Templates Provisioning Backups

5 records

<input type="checkbox"/>	Name	Last backup	Next backup	Progress	Status	Actions
<input type="checkbox"/>	Snapshot Backup - UTM 2.1 Grou...	10/03/2021 12:31	11/03/2021 12:30	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Snapshot Backup - UTM 2.1 Grou...	08/03/2021 15:56	16/03/2021 16:01	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Snapshot Backup - UTM 200.41 - ...	08/03/2021 17:09	Unscheduled	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Backup - UTM 2.1 Group ...	10/03/2021 17:15	11/03/2021 16:02	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>
<input type="checkbox"/>	System Backup - UTM 2.1 Group ...	08/03/2021 16:51	08/04/2021 16:00	<div><div></div></div> ✓	Success	<input checked="" type="checkbox"/>

< 1 > 10 / page

Devices - Backups

Finally, we'll discuss [validating](#) the settings we've made.

# Device Backup - Configuration validation

To validate the correct functioning of the backup settings, just check the status and progress of the backups on the interface where they were created, an example follows:

Devices

Inventory Communities Templates Provisioning Backups

5 records

<input type="checkbox"/>	Name	Last backup	Next backup	Progress	Status	Actions
<input type="checkbox"/>	Snapshot Backup - UTM 2.1 Grou...	11/03/2021 12:31	12/03/2021 12:30	<div><div></div></div> ✓	Success	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	Snapshot Backup - UTM 2.1 Grou...	08/03/2021 15:56	16/03/2021 16:01	<div><div></div></div> ✓	Success	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	Snapshot Backup - UTM 200.41 - ...	08/03/2021 17:09	Unscheduled	<div><div></div></div> ✓	Success	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	System Backup - UTM 2.1 Group ...	11/03/2021 17:18	12/03/2021 16:02	<div><div></div></div> ✓	Success	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	System Backup - UTM 2.1 Group ...	08/03/2021 16:51	08/04/2021 16:00	<div><div></div></div> ✓	Success	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

< 1 > 10 / page

Devices - Backups



For more information on the components of this screen, see this [page](#).

In addition, the operations performed by the backups generate audit logs, as shown in the image below:

Administration

Administrators Users Profiles Auth Servers Identity Provider Audit Log

142 records

Date	User	Interface	Activity	IP	Actions
2021-03-10 20:58:57	Administrator	backups	Delete	192.168.200.2	<input type="checkbox"/>
2021-03-10 20:58:03	Administrator	backups	Edit	192.168.200.2	<input type="checkbox"/>
2021-03-10 20:16:21	Administrator	device-backups	Edit	192.168.200.2	<input type="checkbox"/>
2021-03-10 19:12:49	Administrator	device-backups	Save	172.31.200.253	<input type="checkbox"/>
2021-03-10 18:53:51	Administrator	device-backups	Delete	172.31.200.253	<input type="checkbox"/>
2021-03-10 18:00:23	Administrator	backups	Edit	172.31.200.253	<input type="checkbox"/>
2021-03-10 16:10:58	Administrator	device-backups	Edit	192.168.111.85	<input type="checkbox"/>
2021-03-10 16:01:42	Administrator	device-backups	Save	192.168.112.21	<input type="checkbox"/>
2021-03-10 16:01:13	Administrator	device-backups	Save	192.168.112.21	<input type="checkbox"/>
2021-03-10 16:01:01	Administrator	device-backups	Save	192.168.112.21	<input type="checkbox"/>

< 1 2 3 4 5 ... 15 > 10 / page

Administration - Audit Log



For more information on audit reports, see this [page](#).

Finally, during the backup process, it is also possible to check more details in the CLI using the [\[debug-backup\]](#) command.

```

admin >debug-backup
date="2021-03-10 16:02:03" device_id="4" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM 2.1 - 200.41" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running"
status_message="" service="backup_manager"
date="2021-03-10 16:02:03" device_id="5" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM Dev - 2.1.0" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running" s
tatus_message="" service="backup_manager"
date="2021-03-10 16:02:04" device_id="6" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM 2.1 - 200.1" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="running" s
tatus_message="" service="backup_manager"
date="2021-03-10 16:08:10" device_id="5" backup_id="20" backup_name="System Backup - UTM 2.1 Group - Daily - NFS-01" device_type="firewal
l" action="backup" device_name="UTM Dev - 2.1.0" storage_name="Storage_NFS_01" storage_type="nfs" backup_type="system" status="downloadin
g" status_message="" service="backup_manager"

```


*CLI - debug-backup*



For more information on device backups, see this [page](#).


# Profiles

In this session it is possible to create profiles for the UTM Web Filter, Application Control, Threat Protection, Intrusion Prevention, SSL Inspection and SD-WAN services.

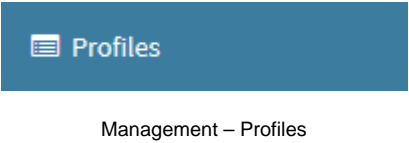
The main function of these profiles is to make it possible to administer the services previously mentioned on all connected devices through a single central point.

 For more information on each configuration, refer to the Blockbit UTM manual.

To apply the profiles created in this session, access the Device template of a UTM 2.0 and after clicking on the [  ] button, enable the desired modules, done that, access the module, click on the **actions menu** [  ] button, create a service and in the "profile" field select the profile that was created in this session. For more information, visit [Device template](#).

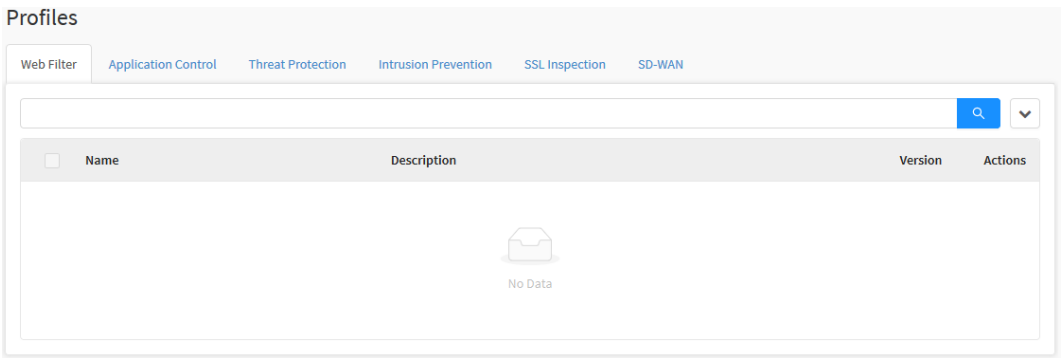
 The profiles created in this tab cannot be applied to UTM version 1.5 or earlier.  
In these cases, during the process of creating a device template 1.5 it will be necessary to create the profile functions, directly in the template itself.  
For more information access [Templates - Menu de ações - Create Template](#).

To access the screen, just select the "Profiles" button.



Management – Profiles

The screen below will appear:



Profiles – Web Filter

The Profiles screen has the following tabs:


- [Web Filter](#);
- [Application Control](#);

- [Threat Protection](#);
- [Intrusion Prevention](#);
- [SSL Inspection](#);
- [SD-WAN](#).

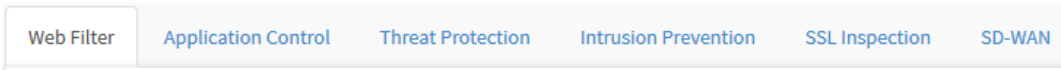
Next, the components of the [Web Filter](#) will be analyzed.

# Web Filter tab

Web Filter acts as a second layer to filter users' navigation. It is responsible for the content filter and can only be used when HTTP / HTTPS web access requests are forwarded by a proxy server, before requesting data from the remote server, it redirects some information from the request (url, user and user IP address) to the Web Filter service.

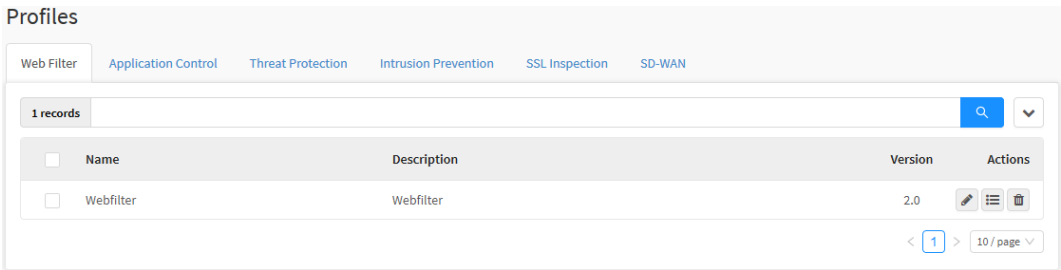
 For more information about Web Filter, consult the [Blockbit UTM manual](#).

Click on the "Web Filter" tab.



Web Filter Tab

The "Web Filter" screen will appear. It consists of the "Name", "Description", "Version" and "Actions" columns. In addition, the search bar and the actions menu are located at the top right of the screen.



Profiles – Web Filter

Next, the menu of actions will be analyzed, and later we will delve into the content of the columns of the Web Filter panel.

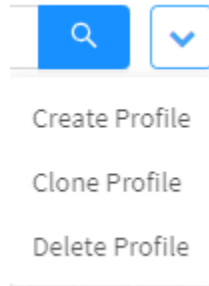
# Web Filter - Actions Menu

At the top right of the screen we have the actions menu:



Web Filter - Actions Menu Button

By clicking on this button the menu below is displayed:



Web Filter - Actions Menu

The menu consists of the following options:

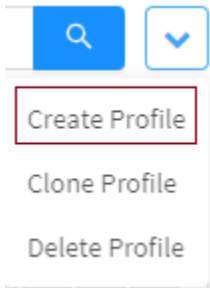
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

Next, each action menu option will be detailed.

# Web Filter - Actions Menu - Create Profile

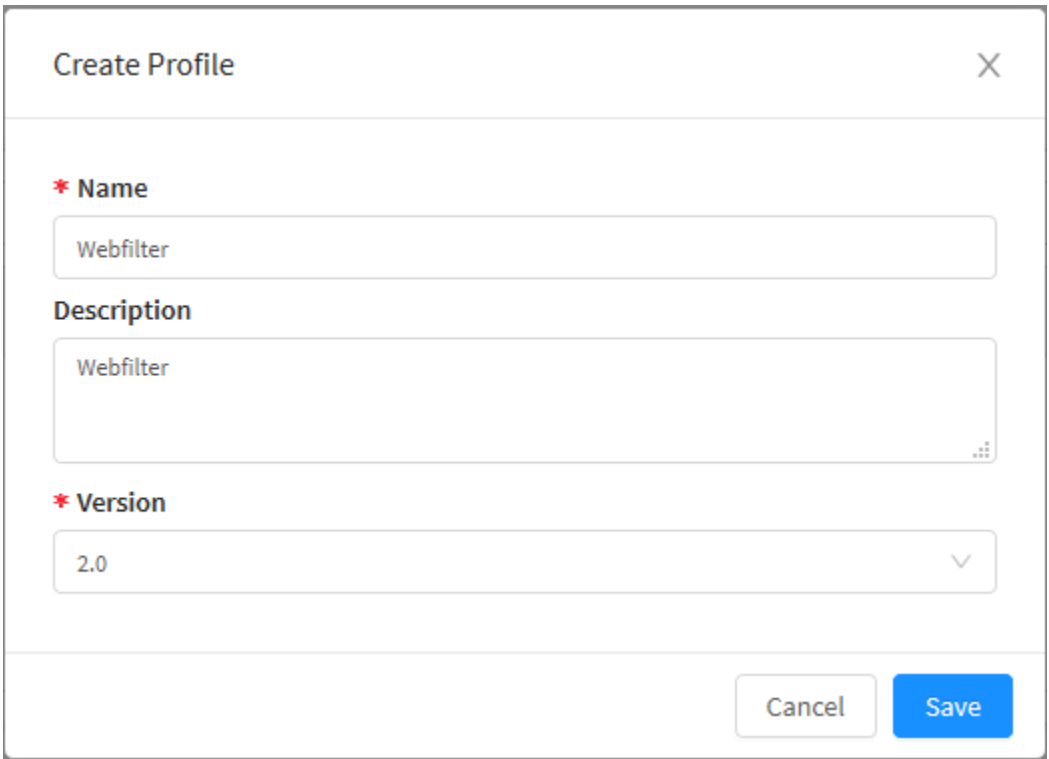
Through the option "Create Profile" it is possible to create a new Web Filter profile. To access, click on the actions menu [  ].

1. Click on the "Create Profile" option;




Web Filter - Create Profile

2. The "Create Profile" screen will be displayed. Fill it with the following data:

A screenshot of a 'Create Profile' form. The form has a title bar with 'Create Profile' and a close button (X). It contains three main sections: 'Name' with a text input field containing 'Webfilter'; 'Description' with a text area containing 'Webfilter'; and 'Version' with a dropdown menu showing '2.0'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Web Filter – Create Profile

- **Name:** Profile name. Ex.: *Webfilter*;
- **Description:** Profile description. Ex.: *Webfilter*;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM;

 **ATTENTION:** If the profile version is different from the UTM version, they will not be compatible.



Always create profiles with the same version of the UTMs to which they will be applied.

Cancel

Save

If you want to cancel click on the [ ] button. To complete the creation of the policy package click on the [ ] button.


 Profile saved successfully

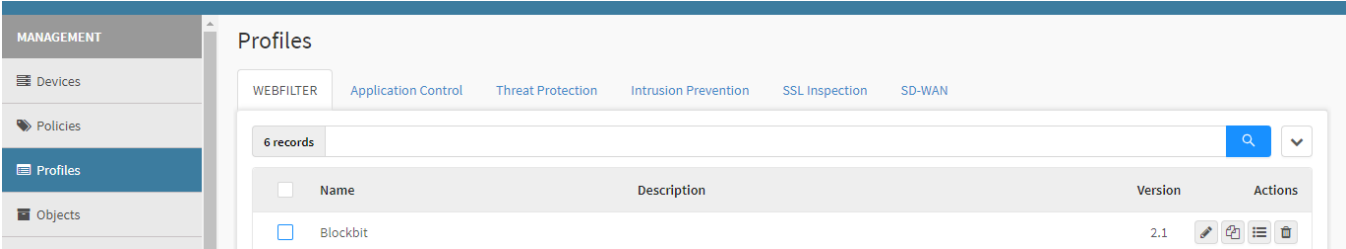
Profile saved successfully

Profile was created successfully.

Next we will look at how to [clone a Web Filter profile](#).

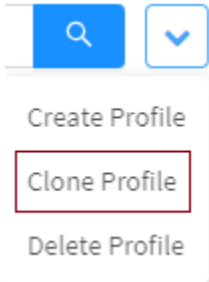
# Web Filter - Actions Menu - Clone Profile

Through the "Clone Profile" option it's possible to clone a Web Filter profile. To access, click on the actions menu [  ].



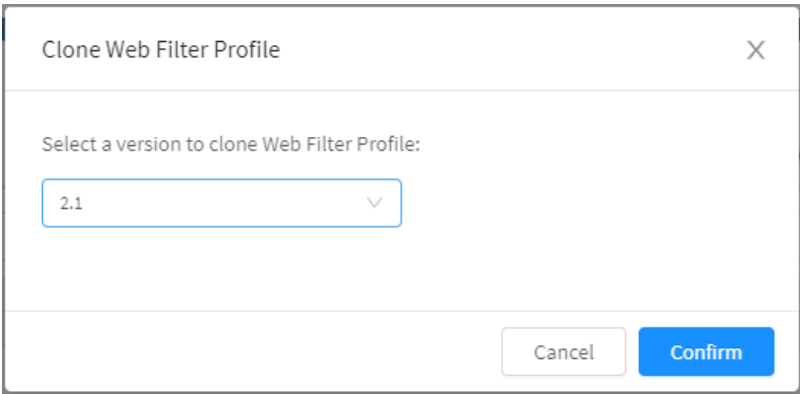
Web Filter - Main Screen.

1. Click on the "Clone Profile" option;



Web Filter - Clone Profile

2. To confirm just click,"Confirm":



Web Filter – Clone Profile

MANAGEMENT

Devices

Policies

Profiles

Objects

Users

Profiles

WEBFILTERApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN

7 records

Name

Description

Version

Actions


Blockbit-clone

2.1

Blockbit

2.1


Profile successfully cloned.

It's also possible to clone a profile by clicking the "Clone" button [  ].

Next we will look at how to [remove a Web Filter profile](#).

# Web Filter - Actions Menu - Delete Profile

Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the Actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles the checkbox will change from gray to blue [  ]. Ex.: Test;

Profiles

Web Filter

Application Control

Threat Protection

Intrusion Prevention

SSL Inspection

SD-WAN

2 records

Name

Description

Version

Actions

Webfilter

Webfilter

2.0

Test

Test

2.0

<

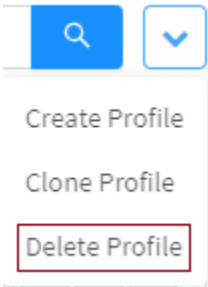
1

>

10 / page

Web Filter - Profiles

2. Enter the actions menu [  ] and click on the "Delete Profile" option.



Web Filter - Delete Profiles

3. The notification message will appear asking if you really want to delete the selected Profiles:

Delete Profile

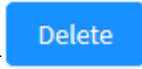
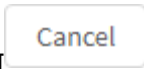
X

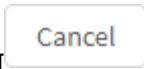
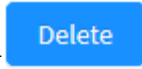
Are you sure you want to delete: Test ?

Cancel

Delete

Web Filter - Profile deletion message



If you want to cancel click on the [  ]. To finish, click the [  ] button.



**Profile deleted successfully!**

Profile has been successfully deleted

After performing these procedures, the profiles will have been successfully deleted.

Next, we will analyze the content of the [columns](#) menu.

# Web Filter - Columns




Below we will explain each column of the Application Control tab:

Profiles

Web Filter   Application Control   Threat Protection   Intrusion Prevention   SSL Inspection   SD-WAN

1 records





☐

Name	Description	Version	Actions
<input type="checkbox"/> Webfilter	Webfilter	2.0	  

< 1 > 10 / page


Profiles – Web Filter

We will explain each column below:


- **Selection box** [  ]: Select the profile;
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Actions**: The “Actions” column consists of several buttons:
  - **Edit** [  ]: Allows you to edit the profile settings added in the option [Create Profile](#) from the actions menu;
  - **List Profiles** [  ]: Allows you to view, edit and add more specific profile options, for more information, check [Web Filter - List Profile](#);
  - **Delete** [  ]: Delete the profile.

Following are the button functions [List Profiles](#) will be explained and exemplified.

# Web Filter - List Profile

By clicking on the detail button [  ] it is possible to configure the profile;

In this panel it is possible to make the general configurations, configure filters and quotas that will be used in this profile.

 For more information about Web Filter, consult the Blockbit UTM manual.

Edit Profile

X

General

\* Name

Webfilter

Description

Webfilter

Search

☐ Restrict login domains for Google Apps

☐ Enforce Safe Search for Google, Bing, Yahoo

Filters

☐ Web categories

☐ File Filter

Surfing Quotas

☐ Maximum Time

☐ Maximum Download Size

Hours per day

▼

MB

▼

☐ Maximum Traffic

☐ Maximum Upload Size

MB per day

▼

MB

▼

Cancel

Save

Web Filter - Edit Profile

## General

In "General" we have the following text boxes:



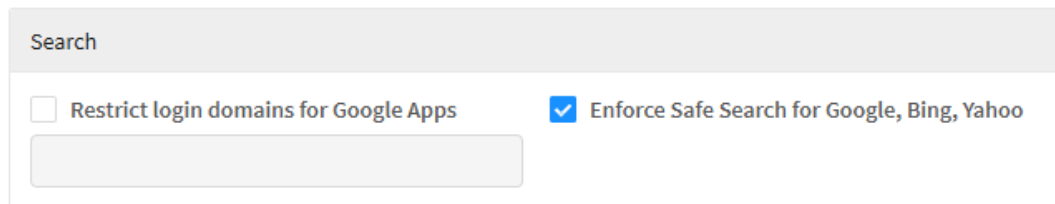
The screenshot shows the 'General' tab of a configuration window. It contains two text input fields. The first field is labeled with a red asterisk and the word 'Name', and it contains the text 'Webfilter'. The second field is labeled 'Description' and also contains the text 'Webfilter'.

Web Filter – General

- **Name:** Define a name for the profile. Ex.: Webfilter;
- **Description:** Set a description for the profile. Ex.: Webfilter.

## Search

In "Search" it is possible to manage access to search services:



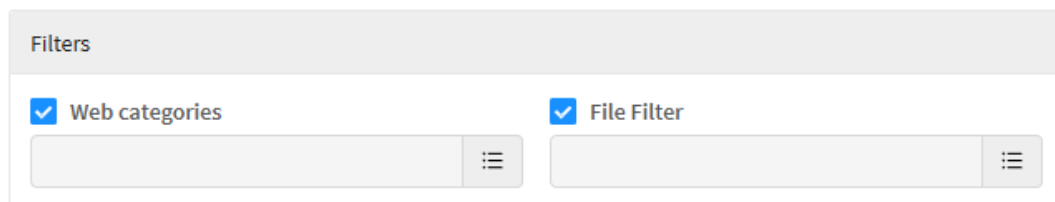
The screenshot shows the 'Search' tab of a configuration window. It features two checkboxes. The first checkbox, labeled 'Restrict login domains for Google Apps', is unchecked. Below it is an empty text input field. The second checkbox, labeled 'Enforce Safe Search for Google, Bing, Yahoo', is checked.

Web Filter - Search

- **Restrict login domains for Google Apps** ☒: This option allows you to control which domains will access Google Apps;
- **Enforce Safe Search for Google, Bing, Yahoo** ☒: This check box forces Safe Search to be activated on search engines.

## Filters




In "Filters" the following options are available:



The screenshot shows the 'Filters' tab of a configuration window. It contains two checked checkboxes. The first is 'Web categories', followed by an empty text input field with a menu icon. The second is 'File Filter', followed by another empty text input field with a menu icon.

Web Filter - Filters



- **Web categories** [  ]: Allows you to select the web categories to apply “Block” or “Exception” filters to the set of applied policies. To select the categories, click the [  ] button, choose the desired categories and then select **Allow**, **Deny** or **Disable**. In the actions menu [  ], it is also possible to apply any of these options in all categories in **Allow All**, **Deny All** and **Disable All** to disable them. Below is a brief description of the function of each action:
  - **Allow**: Below is a brief description of the function of each action;
  - **Deny**: Access to URLs classified under this category is denied;
  - **Disable**: This category is disabled, this means that the Web Filter will ignore it and will only consider URLs in allowed or blocked categories.

Add Category

All

Pro-Choice

Activism Groups

Adult Material

Adult Content

Nudity

Sex

Sex Education

Lingerie and Swimsuit

Business and Economy

Financial Data and Services

Drugs

Abused Drugs

Prescribed Medications

Supplements and Unregulated Compounds

Marijuana

Education

Allow

Allow All

Deny All

Disable All

Allow

Allow

Allow

Allow

Allow

Allow

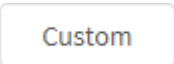
Allow

Allow

Allow

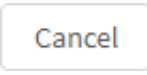
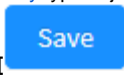
Allow


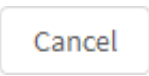
Web Filter - Add Category



It is also possible to add custom categories by clicking on the [  ] button;

*Web Filter - Add Category - Custom*

Click in the field and select the desired category, in this field [dictionary](#) type objects will be available, the selected objects will be added as tags. Finally,

click the [  ] button to exit this window or click the [  ] button to save.

To finish adding the categories, click the [  ] button to save or click the [  ] button to exit this window.

- **File Filter** [  ]: Allows you to select the file types added in [Objects - Contents](#) to apply filters to the set of applied policies. To select the objects, click on the [  ] button, and enable the desired checkboxes. In the action menu, you can also click **Select All** to check all or **Deselect All** to deselect all categories.

Add FileFilter

All

☒

Item

☐

ActiveX

☐

Compressed

☒

Executables

☐

Image group

☐

Images

☐

Javascript

☐

Multimedia

☐

Office

<

1

>

Cancel

Save

Web Filter - Add File Filter

Click the  button to cancel. Click the  button to save.

## Surfing Quotas

In "Surfing Quotas" the following panel is displayed:

Surfing Quotas

☐ Maximum Time
 

Hours per day

☐ Maximum Download Size
 

MB

☐ Maximum Traffic
 

MB per day

☐ Maximum Upload Size
 

MB

Web Filter - Surfing Quotas

- ☒ **Maximum Time:** Allows you to set a time share in minutes or hours per day.

☒ Maximum Time
 

Hours per day

☐ Maximum Traffic
 

Minutes per day

☐ Maximum Upload Size
 

Hours per day

Web Filter – Maximum Time

- ☒ **Maximum Traffic:** Allows you to configure a share of traffic in MB per day.

☒ Maximum Traffic
 

MB per day

☐ Maximum Upload Size
 

MB per day

Web Filter – Maximum Traffic

- ☒ **Max Download Size:** Allows you to configure the maximum download size, in MB or GB.

☒ Maximum Download Size
 

MB

☐ Maximum Upload Size
 

MB

☐ Maximum Traffic
 

GB

Web Filter - Maximum Download Size

- ☒ **Max Upload Size:** Allows you to configure the maximum upload size, in MB or GB.

☒ **Maximum Upload Size**

MB ^

MB

GB

*Web Filter - Maximum Upload Size*



The settings made can be added to a [policy](#) in the Inspection menu in the Web Filter option.

Cancel

Save


After completing all settings, click the [ Cancel ] button to return to the Profiles panel or click the [ Save ] button to save.

For more information about the Web Filter tab, see this [page](#).

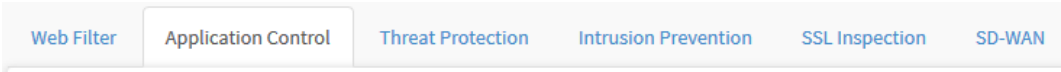
Next, we will detail the contents of the [Application Control](#) tab.

# Application Control tab

Through the Application Control feature, it is possible to control whether users will be allowed access to certain applications or if they will not be authorized to use any application. The applications are divided into categories allowing the administrator to specifically determine the access of each item.

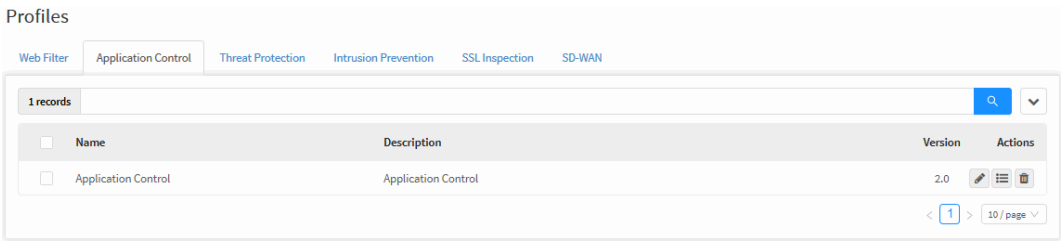
 For more information on Application Control, refer to the Blockbit UTM manual.

Click on the "Application Control" tab.



Application Control tab

The "Application Control" screen will appear. It consists of the columns "Name", "Description", "Type", "Version" and "Actions". In addition, at the top right of the screen is located the [search bar](#) e o [actions menu](#).



Profiles – Application Control

Next, the [actions menu](#) will be analyzed and later we will delve into the content of the [columns](#) of the Application Control panel.

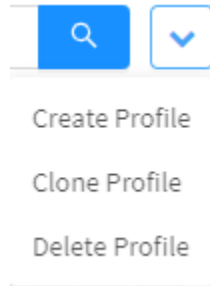
# Application Control - Actions menu

At the top right of the screen we have the actions menu:



Application Control – Actions menu button

By clicking this button, the menu below will be displayed:



Application Control – Actions menu

The menu consists of the following options:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

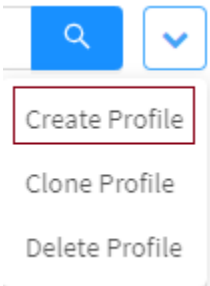
Next, each action menu option will be detailed.

# Application Control - Actions menu - Create Profile



Through the option "Create Profile" it is possible to create a new Application Control profile. To access, click on the **actions menu** [ ].

1. Click on the "Create Profile" option;



Application Control - Create Profile

2. The "Create Application Control" screen will be displayed. Fill it with the following data:

- **Name:** Profile name. Ex.: Stores;
- **Description:** Profile description. Ex.: Application Control - Stores;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM;



**ATTENTION:** If the version of the profile is different from that of the UTM, they will not be compatible.


Always create profiles with the same version of the UTMs to which they will be applied.

Application Control – Create Application Control



A rectangular button with a thin border and the word "Cancel" in a dark font.A solid blue rectangular button with the word "Save" in white font.

If you want to cancel click on the [ ] button. To complete the creation of the policy package click on the [ ] button.


 **Profile saved successfully**

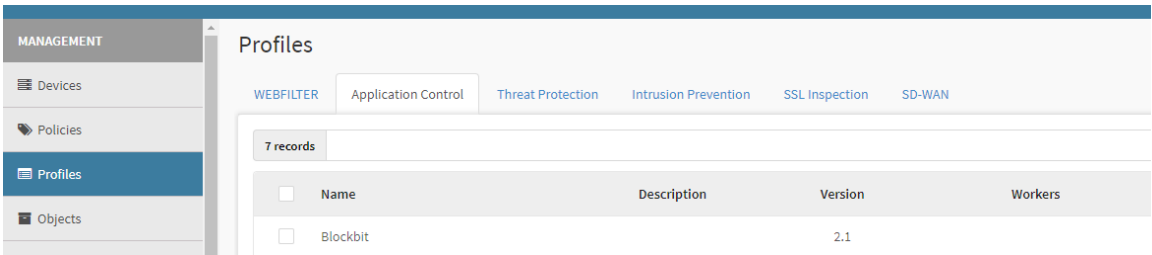
*Profile saved successfully*

Profile was created successfully.

Next, we will look at how to [clone a Profile](#).

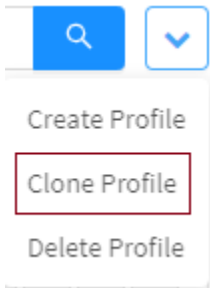
# Application Control - Actions menu - Clone Profile

Through the "Clone Profile" option it is possible to clone an Application Control profile. To access, click on the **actions menu** [  ].



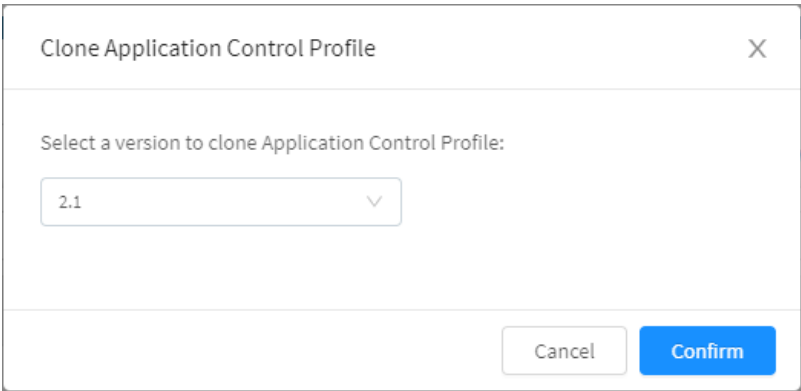
Application Control - Main screen.

1. Click on the "Clone Profile" option;

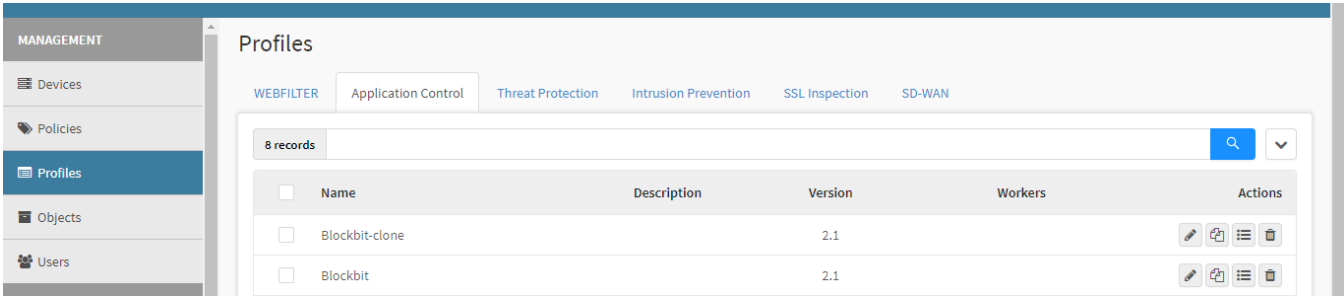


Application Control - Clone Profile

2. To confirm just click the "Confirm" button:



Application Control - Clone Profile.




Profile was created successfully.

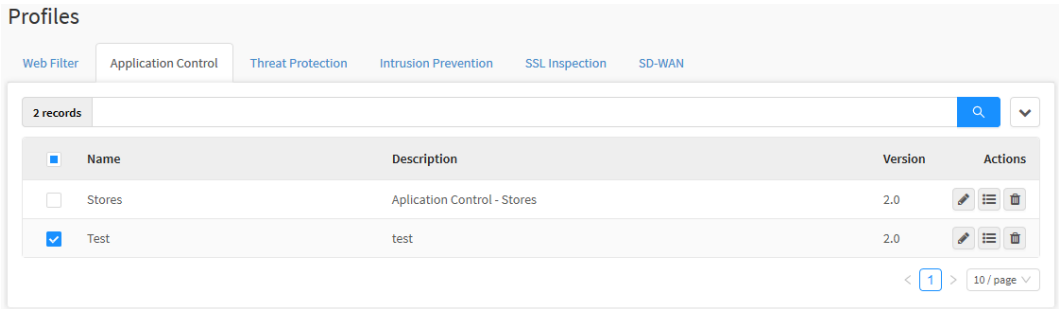
It's also possible to clone a profile by clicking the "Clone" button [  ].

Next, we will see how to [delete a Profile](#).

# Application Control - Actions menu - Delete Profile

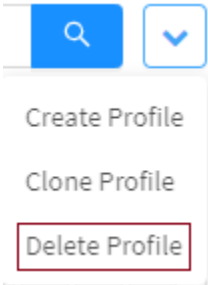
Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the Actions Menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles the checkbox will change from gray to blue . Ex.: Test;



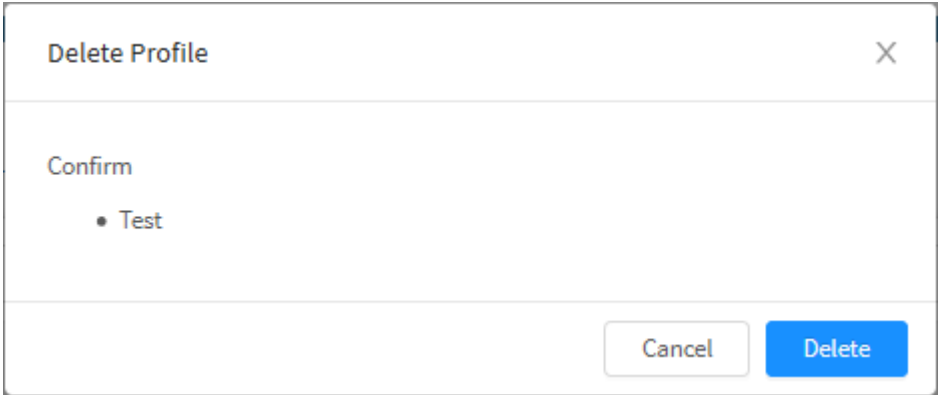
Application Control - Profiles

2. Enter the actions menu [  ] and click on the "Delete Profile" option.

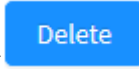
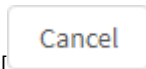


Application Control – Delete Profile

3. The notification message will appear asking if you really want to delete the selected Profiles:



Application Control - Profile deletion confirmation.



If you want to cancel click on the [ ] button. To finish, click the [ ] button.



**Profile removed successfully**

The profile has been successfully removed.

After performing these procedures, the Profiles will have been successfully deleted.

# Application Control - Columns

Below we will explain each column of the Application Control tab:

Profiles

Web Filter

Application Control

Threat Protection

Intrusion Prevention

SSL Inspection

SD-WAN

2 records

Name

Description

Version

Actions

Application Control

Application Control

2.0

Stores

Application Control - Stores

2.0

<





1

>

10 / page

Profiles – Application Control

We will explain each column below:

- **Checkbox** [  ]: Select the profile;
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Actions**: The “Actions” column consists of several buttons:
  - **Edit** [  ]: Allows you to edit the profile settings added in the option [Create Profile](#) from the actions menu;
  - **List Profiles** [  ]: Allows you to view, edit and add more specific profile options, for more information, check [Application Control - Actions Menu - Create Profile](#);
  - **Delete** [  ]: Delete the profile.

Following, the button functions of [List Profiles](#) will be explained and exemplified.

# Application Control - List Profile

By clicking on the **detail button** it is possible to configure the profile;

In this panel it is possible to make the general configurations and define the permissions of the applications used in that profile.

Create Profile

General

\* Name

Stores

Description

Application Control - Stores

Application Control

☐ Applications

Cancel

Save

Application Control - Create Profile

## General

In "General" we have the following text boxes:

General

\* Name

Stores

Description

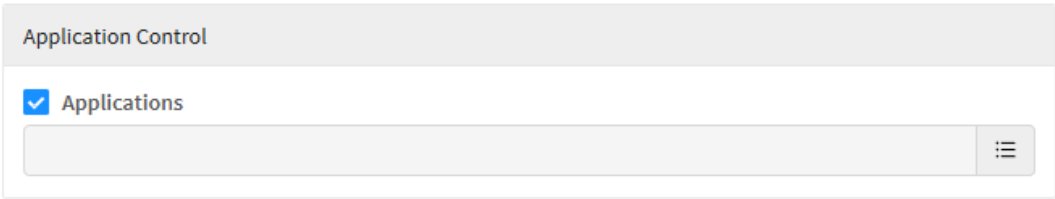
Application Control - Stores

Application Control – General



- **Name:** Define a name for the profile. Ex.: Load Balance;
- **Description:** Define a description for the profile. Ex.: SD-WAN - Load Balance.

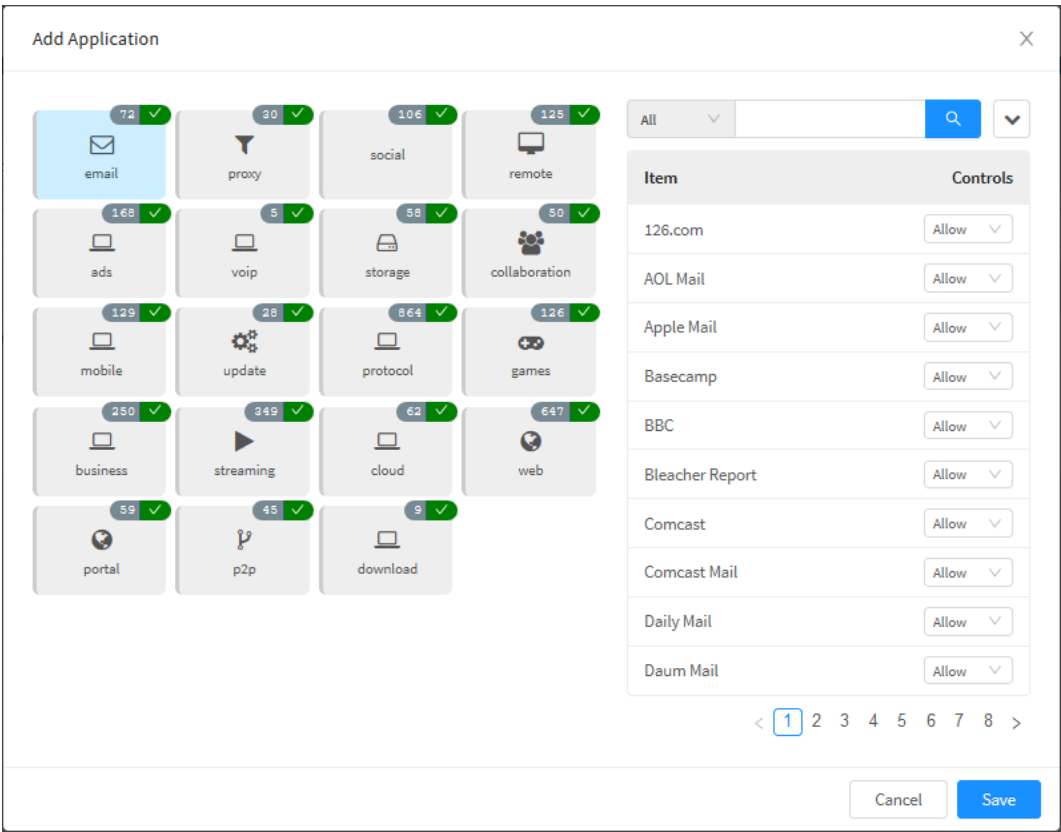
# Application Control

"Application Control" determines the applications that will be allowed or denied access:



Application Control - Applications

To edit the applications, make sure that the **checkbox**  is enabled, then click the **list applications**  button to manage permissions.



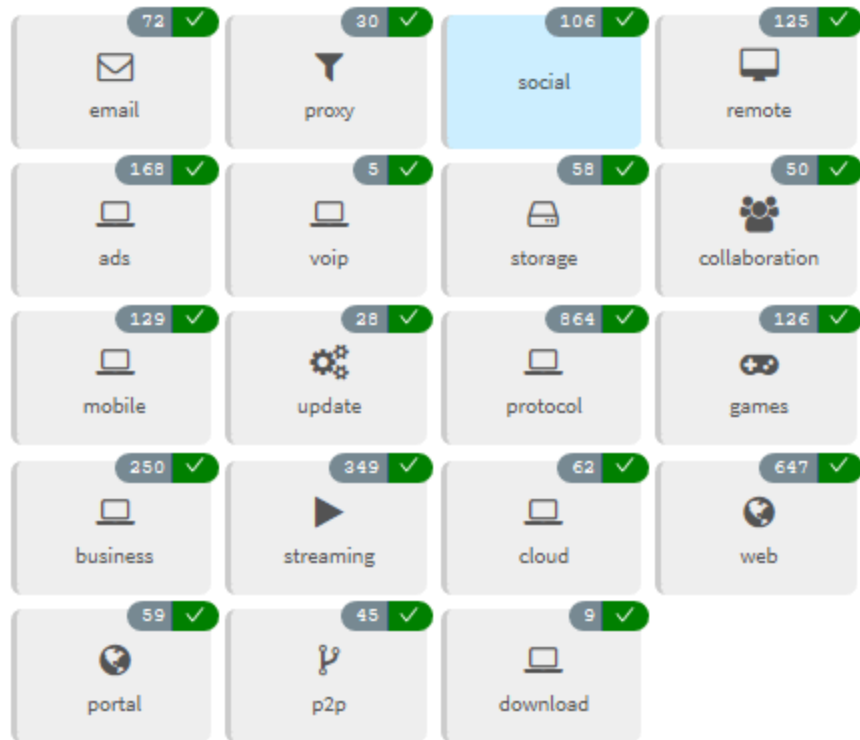
Application Control - Add Application

When selecting one of the icons on the left, the applications will be displayed in the panel on the right.


In the example below, we will disable access for some chat applications.

To do so, select the desired category, in this example, we will select the "social" option:






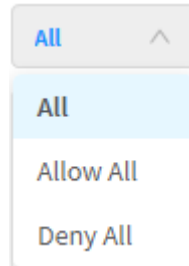
Application Control - Add Application - "Social" option selected

Determine the desired application and in the selection box, choose the option **Deny** [  ], as exemplified in the image below:

Item	Controls
Eventbrite	Allow ▾
Facebook Apps	Allow ▲
Facebook Like	Allow
Family Tree	Deny
Fazed	Disable
Facebook Comment	Allow ▾
Facebook event	Allow ▾
Facebook Message	Allow ▾
Facebook Status Update	Allow ▾
Facebook search	Allow ▾

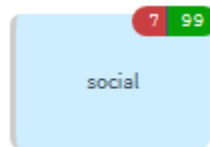
Application Control - Add Application - Denied items

If it is necessary to make a configuration for all items in a category, simply select the desired option in the **actions menu** [  ] or in the checkbox shown below:

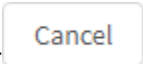
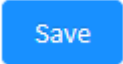


Application Control - Add Application - All, Allow All and Deny All

When having an application with permission denied, the amount of applications denied and allowed will be displayed under the icon of its respective category on the left, as shown below:



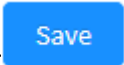
Application Control - Add Application - 7 items denied and 99 allowed

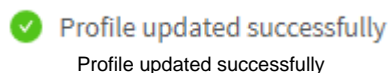
Finally, if you want to cancel click on the [  ] button. To finish editing the applications click on the [  ] button.

After having performed the previous processes, a summary of all allowed and denied applications will be displayed in the Applications field, as shown below:



Application Control - Applications - Applications allowed and denied

To complete this process, just click the button [  ] button again.

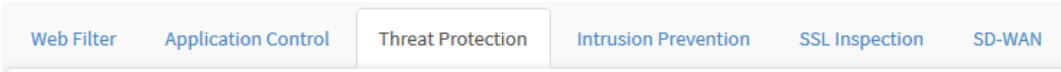


The profile was created successfully.

# Threat Protection Tab

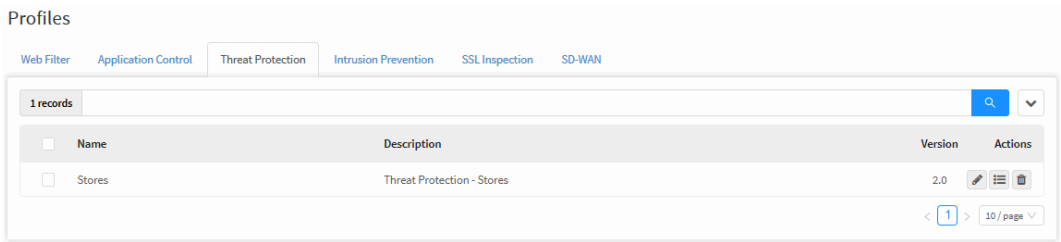
With Threat Protection profiles, you can analyze files for malware inspection and threat blocking. This section will demonstrate how to create profiles that will later be installed in the policies.

Click on the "Threat Protection" tab.



Threat Protection Tab

The "Threat Protection" screen will appear. It consists of the "Name", "Description", "Version" and "Actions" columns. In addition, the [search bar](#) is located at the top right of the screen and the [actions menu](#).



Profiles – Threat Protection

Next, the [actions menu](#) will be analyzed and later we will delve into the content of the Threat Protection panel columns.

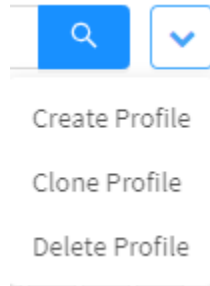
# Threat Protection - Actions menu

At the top right of the screen we have the actions menu:



Threat Protection - Actions menu button

By clicking on this button the menu below is displayed:



Threat Protection - Actions menu

The menu consists of the following options:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

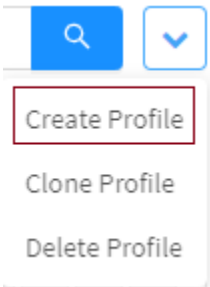
Next, each action menu option will be detailed.

# Threat Protection - Actions menu - Create Profile



Through the "Create Profile" option it is possible to create a new Threat Protection profile. To access, click on the **actions menu** [

1. Click on the "Create Profile" option;



Threat Protection - Create Profile

2. The "Create Threat Protection" screen will be displayed. Fill it with the following data:

- **Name:** Profile name. Ex.: Stores;
- **Description:** Profile description. Ex.: Application Control - Stores;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM's;



**ATTENTION:** If the version of the profile is different from that of the UTM, they will not be compatible.

Always create profiles with the same version of the UTMs to which they will be applied.

Create Threat Protection

\*

Name

Stores

Description

Threat Protection - Stores

\*

Version

2.0


Cancel

Save

Threat Protection - Create Threat Protection

A rectangular button with a thin border and the word "Cancel" in a dark blue font.A solid blue rectangular button with the word "Save" in white font.

If you want to cancel click on the [ ] button. To complete the creation of the policy package click on the [ ] button.

 **Profile saved successfully**

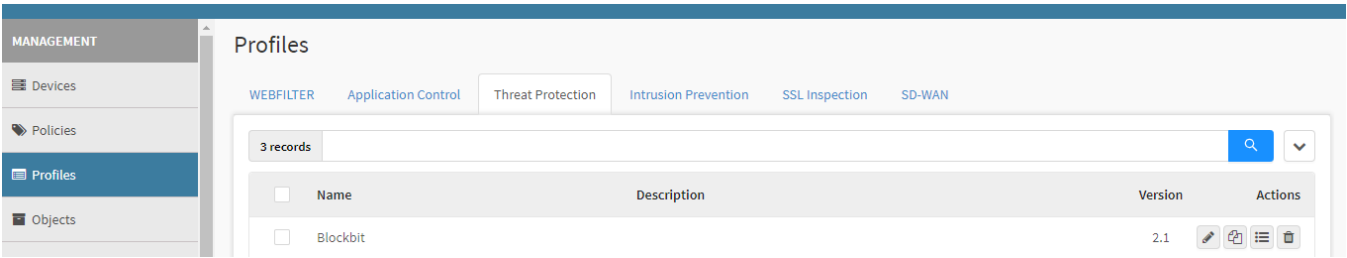
The profile has been successfully saved.

Profile was created successfully.

Next we will look at how to [Clone a Profile](#).

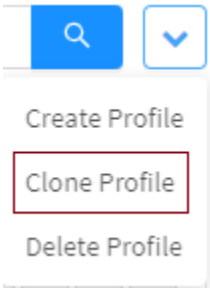
# Threat Protection - Actions menu - Clone Profile

Through the "Clone Profile" option it's possible to clone a Threat Protection profile. To access, click on the **actions menu** [  ].



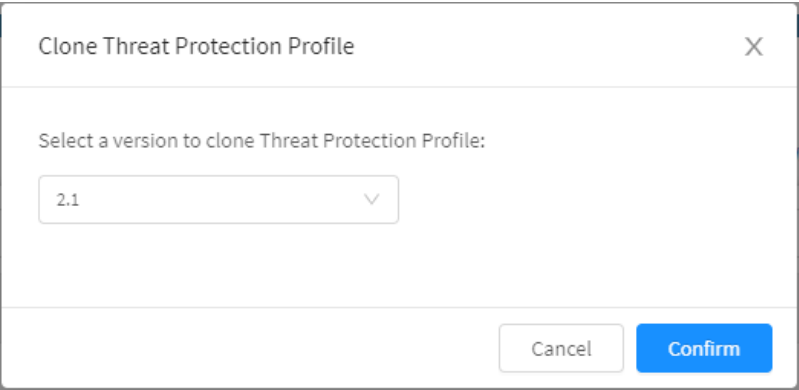
Threat Protection - Main menu.

1. Click on the "Clone Profile" option;



Threat Protection - Clone Profile

2. To confirm just click the "Confirm" button:



Threat Protection - Clone profile.

MANAGEMENT

Devices

Policies

Profiles

Objects

Users

Profiles

WEBFILTERApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN

4 records

Name

Description

Version

Actions


Blockbit-clone

2.1

Blockbit

2.1

The profile has been successfully cloned .


It's also possible to clone a profile by clicking the "Clone" button [  ].

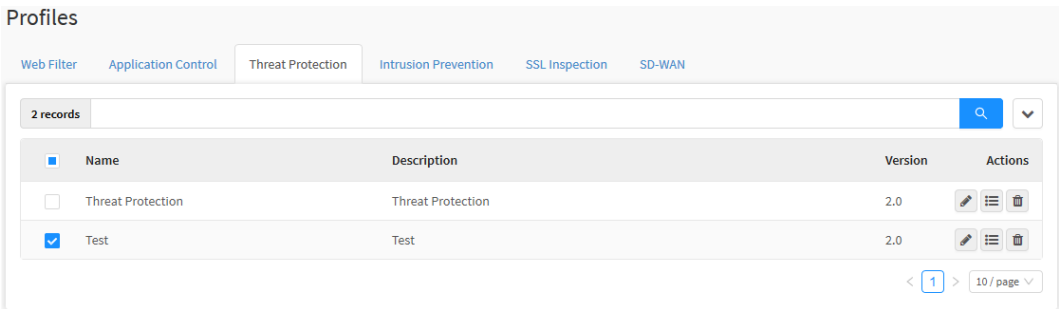
Next we will look at how to [Delete a Profile](#).



# Threat Protection - Actions Menu - Delete Profile

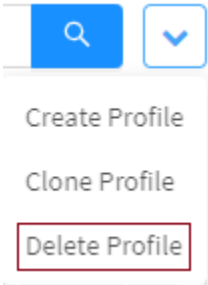
Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

- 1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles the checkbox will change from gray to blue [  ]. Ex.: Test;



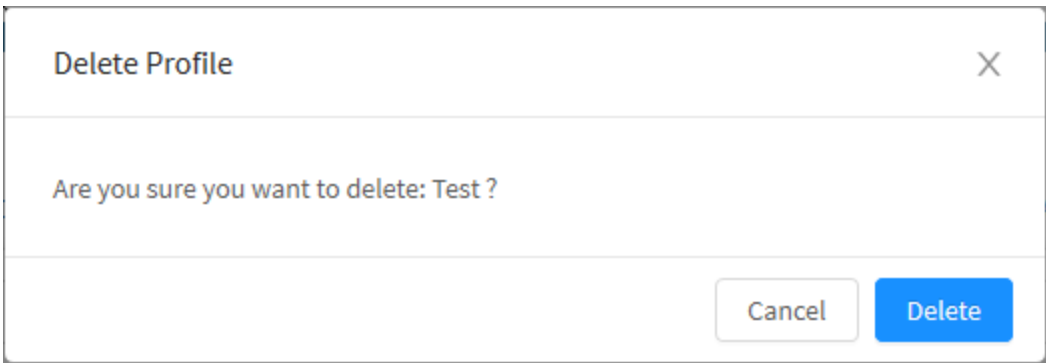
Threat Protection – Selection of Profiles to delete

- 2. Access the **actions menu** [  ] and click on the "Delete Profiles" option.

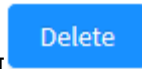
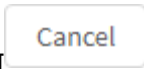


Threat Protection – Delete Profiles.

- 3. The notification message will appear asking if you really want to delete the selected Profiles:



Threat Protection – Profile deletion confirmation



If you want to cancel click on the [ ] button. To finish, click the [ ] button.



**Profile removed successfully**

The profile has been successfully deleted.

After performing these procedures, the profiles will have been successfully deleted.

Now we will look at the [Columns menu](#).

# Threat Protection - Columns

Below we will explain each column of the Threat Protection tab:

Profiles

Web Filter   Application Control   Threat Protection   Intrusion Prevention   SSL Inspection   SD-WAN

1 records

Name

Description

Version

Actions

Threat Protection





Threat Protection

2.0

< 1 > 10 / page

Profiles – Threat Protection

In the following we will explain each column:

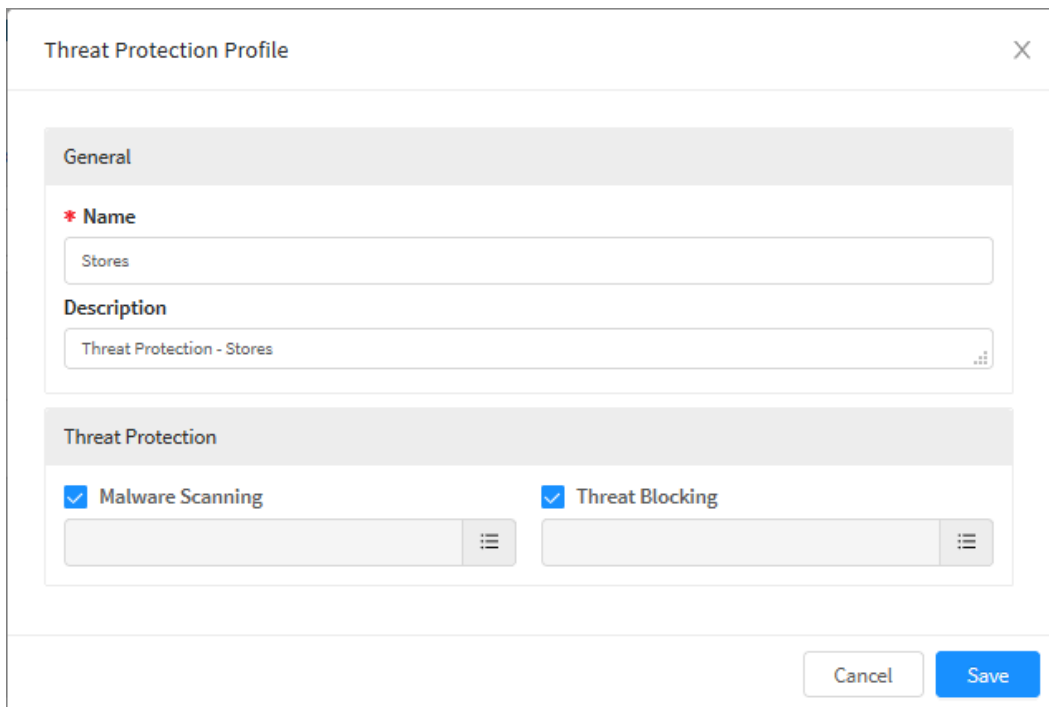
- **Checkbox** [  ]: Select the profile;
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Actions**: The “Actions” column is made up of several buttons:
  - **Edit** [  ]: Allows you to edit the settings of the profile added in the [Create Profile](#) option of the actions menu;
  - **List Profiles** [  ]: Allows you to view, edit and add more specific profile options, for more information, check [Threat Protection - Actions Menu - Create Profile](#);
  - **Delete** [  ]: Delete the profile.

Next, the functions of the [List Profiles](#) button will be explained and exemplified.

# Threat Protection - List Profile

By clicking on the **detail button**  it is possible to configure the profile;

In this panel it is possible to make general profile settings, trigger malware scan and block threats.



*Threat Protection - Profile*

## General

In "General" we have the following text boxes:

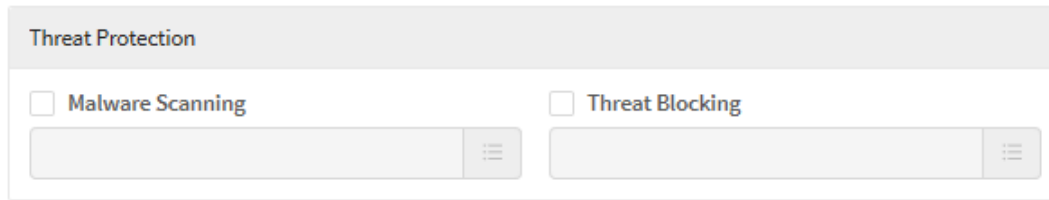


*Threat Protection – General*

- **Name:** Define a name for the profile. Ex.: Threat Protection;
- **Description:** Set a description for the profile. Ex.: Threat Protection.

## Threat Protection

"Threat Protection" determines the scanning of malware and the blocking of threats.



Threat Protection



☒ Malware Scanning

☐ Threat Blocking

Threat Protection - Threat Protection

In the following, we will analyze in detail these two fields.

### Malware Scanning

To add Malware Scanning, make sure that the **checkbox**  is enabled, then click on the **list applications**  button the following panel will be displayed:

Add Malware Scanning

All

☐

Item

☐

ActiveX

☐

Compressed

☐

Executables

☐

Images

☐

Javascript

☐

Multimedia

☐

Office

<

1

>

Cancel

Save

Threat Protection - Add Malware Scanning

Check the checkboxes to add malware scanning, as shown below:


Add Malware Scanning
✕

All

<input checked="" type="checkbox"/>	Item
<input checked="" type="checkbox"/>	ActiveX
<input type="checkbox"/>	Compressed
<input type="checkbox"/>	Executables
<input type="checkbox"/>	Images
<input checked="" type="checkbox"/>	Javascript
<input type="checkbox"/>	Multimedia
<input type="checkbox"/>	Office

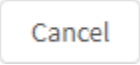

<
1
>

Threat Protection - Check boxes checked



If it is necessary to make a configuration on all items, just select the desired option in the **action menu** [  ]:

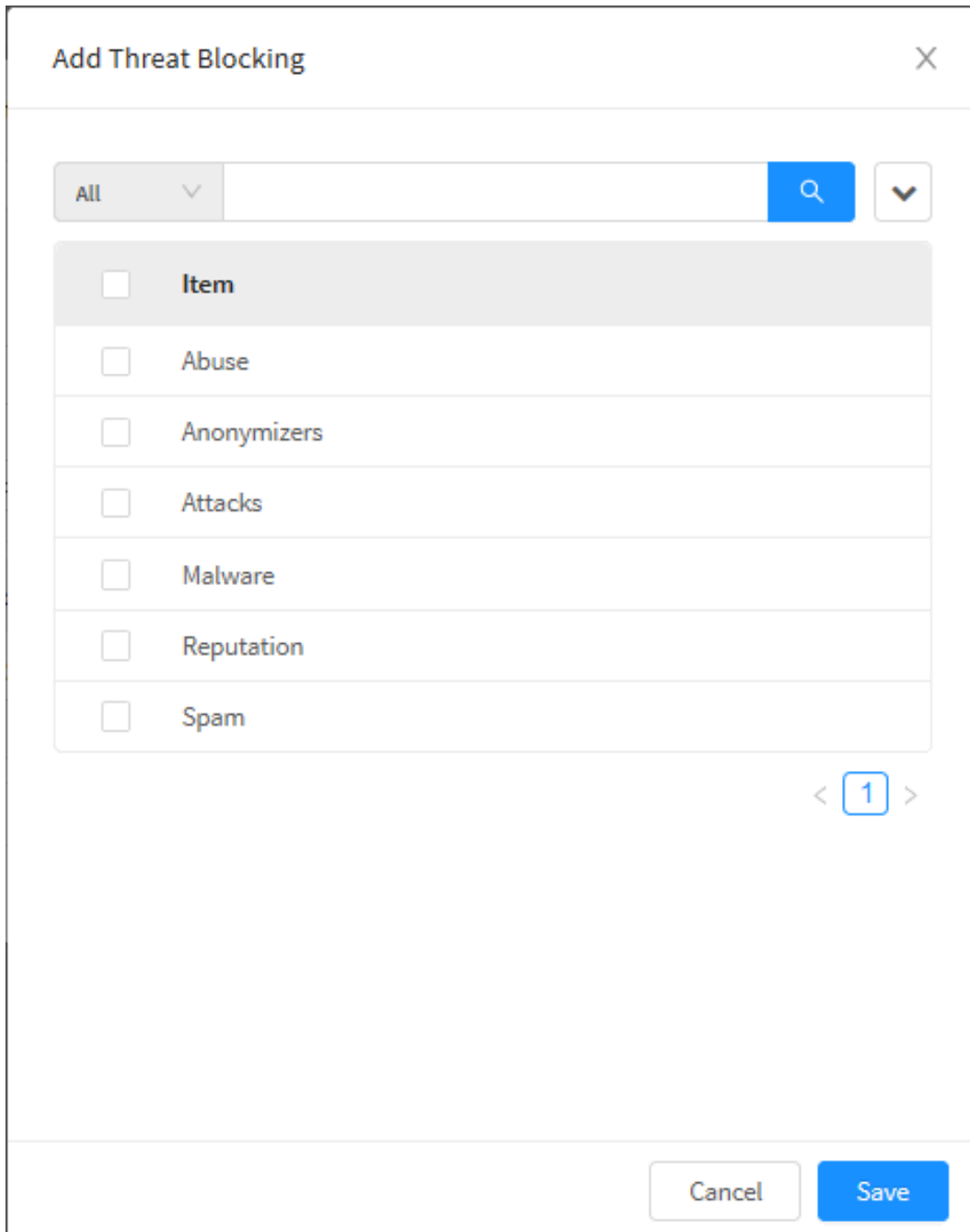
Select All  
Deselect All

Threat Protection - Select all and Deselect All

Finally, if you want to cancel click on the  button. To finish adding Malware Scanning to applications, click on the  button.

## Threat Blocking

To add Threat Blocking, make sure that the **checkbox**  is enabled, then click on the **list applications**  button the following panel will be displayed:



The dialog box titled "Add Threat Blocking" features a close button (X) in the top right corner. Below the title bar is a search bar with a dropdown menu currently set to "All", a search icon, and a filter icon. The main content area contains a list of threat categories, each with a checkbox and a label: "Item", "Abuse", "Anonymizers", "Attacks", "Malware", "Reputation", and "Spam". At the bottom right of the list is a pagination control showing "< 1 >". The bottom of the dialog box has "Cancel" and "Save" buttons.

<input type="checkbox"/>	Item
<input type="checkbox"/>	Abuse
<input type="checkbox"/>	Anonymizers
<input type="checkbox"/>	Attacks
<input type="checkbox"/>	Malware
<input type="checkbox"/>	Reputation
<input type="checkbox"/>	Spam

Threat Protection - Add Threat Blocking



Check the checkboxes to add the threat block, as shown below:

Add Threat Blocking

All

Item

Abuse

Anonymizers

Attacks

Malware

Reputation

Spam

<

1

>

Cancel

Save

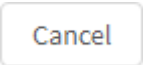

Threat Protection - Add Threat Blocking

If it is necessary to make a configuration on all items, just select the desired option in the **action menu** [  ]:

Select All

Deselect All

Threat Protection - Select all and Deselect All

Finally, if you want to cancel click the [  ] button. To finish adding Malware Scanning to applications, click the [  ] button.

After having performed the previous processes, a summary of all selected threat protection items will be displayed in both fields, as shown below:

Threat Protection

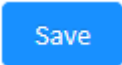
☒ Malware Scanning

2 Selected

☒ Threat Blocking


3 Selected

Threat Protection - Selected items

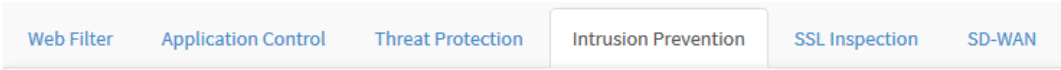
To finish, just click the [  ] button again.

# Intrusion Prevention tab

The Intrusion Prevention System (IPS) is an attack and intrusion prevention module, it works by analyzing the traffic flow in order to detect and stop vulnerabilities in the network.

 For more information on Intrusion Prevention, consult the Blockbit UTM manual.

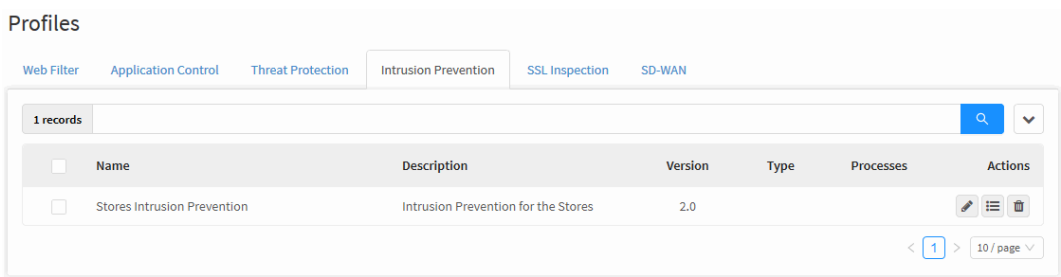
Click on the “Intrusion Prevention” tab.



Intrusion Prevention tab

The “Intrusion Prevention” Screen will appear. It consists of the columns “Name”, “Description”, “Version”, “Type”, “Processes” and “Actions”. In addition, at the top right of the screen is located the

[search bar](#) and the [actions menu](#).



Profiles – Intrusion Prevention

Next, the action menu will be analyzed and later we will delve into the content of the Intrusion Prevention panel columns.

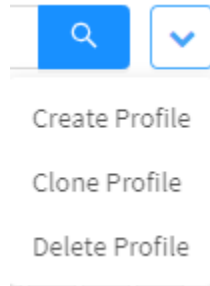
# Intrusion Prevention - Actions Menu

At the top right of the screen we have the actions menu:



Intrusion Prevention - Actions Menu Button

By clicking on this button the menu below is displayed:



Intrusion Prevention - Actions Menu

The menu consists of the following options:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

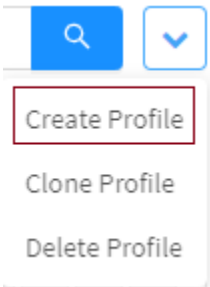
Next, each action menu option will be detailed.

# Intrusion Prevention - Actions Menu - Create Profile



Through the option "Create Profile" it is possible to create a new Intrusion Prevention profile. To access, click on the **actions menu** [

1. Click on the "Create Profile" option;



*Intrusion Prevention - Create Profile*

2. The "Add Profile" screen will be displayed. Fill it with the following data:

Add Profile

\*

Name

Stores Intrusion Prevention

Description

Intrusion Prevention for the Stores

Version

2.0

Cancel

Save

*Intrusion Prevention – Add Profile*

- **Name:** Profile name. Ex.: Intrusion Prevention - Stores;
- **Description:** Profile description. Ex.: Intrusion Prevention - Stores;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM's;

**ATTENTION:** If the version of the profile is different from that of the UTM, they will not be compatible.

Always create profiles with the same version of the UTM to which they will be applied.

Cancel

Save

If you want to cancel click on the [ ] button. To complete the creation of the policy package click on the [ ] button.

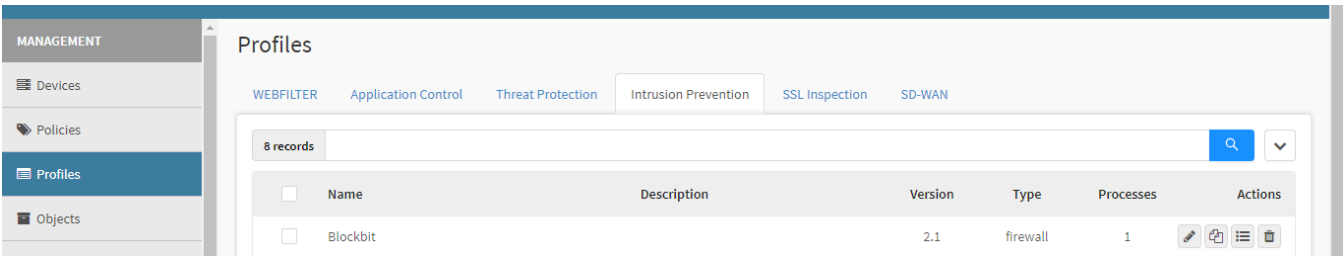
✓ Profile saved successfully

*The profile has been successfully saved.*

Now, we will look at the [Clone Profile menu](#).

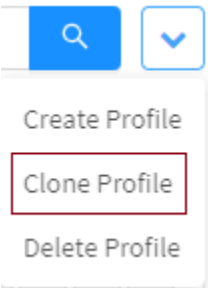
# Intrusion Prevention - Actions Menu - Clone Profile

Through the "Clone Profile" option it's possible to clone a Intrusion Prevention profile. To access, click on the **actions menu** [  ].



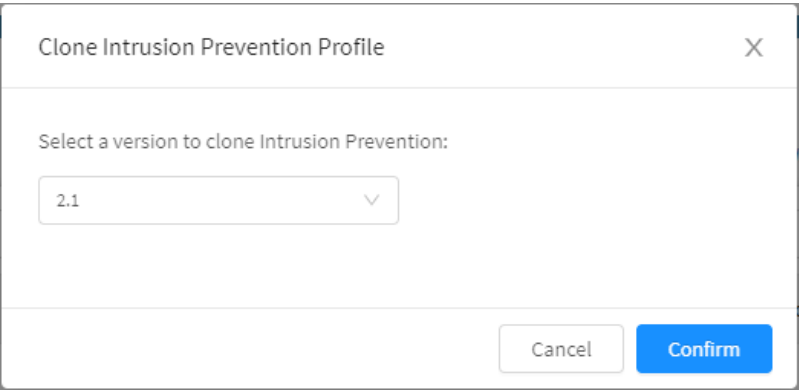
*Intrusion Prevention - Main screen.*

1. Click on the "Clone Profile" option;



*Intrusion Prevention - Clone Profile*

2. To confirm just click the "Confirm" button:



*Intrusion Prevention - Clone Profile.*

MANAGEMENT

Devices

Policies

Profiles









Objects

Users


Profiles

WEBFILTERApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN

9 records

	Name	Description	Version	Type	Processes	Actions
<input type="checkbox"/>	Blockbit-clone		2.1	firewall	1	   
<input type="checkbox"/>	Blockbit		2.1	firewall	1	   

The profile has been successfully cloned.


It's also possible to clone a profile by clicking the "Clone button []."

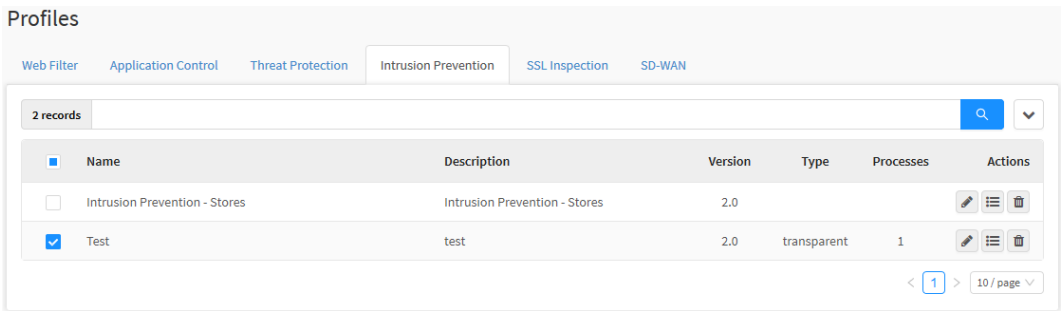
Next we will look at how to [Delete a Profile](#).




# Intrusion Prevention - Actions Menu - Delete Profile

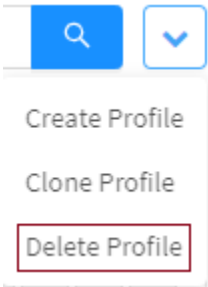
Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

- 1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox that is located next to the Name. In the selected profiles the checkbox will change from gray to blue [  ]. Ex.: Test;



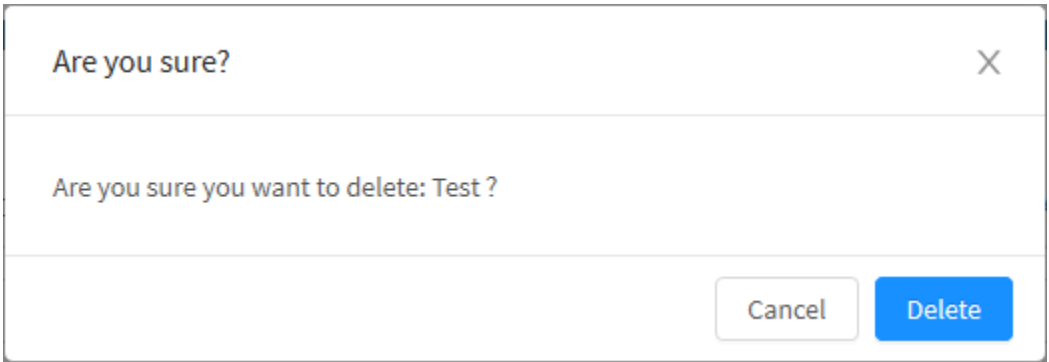
Intrusion Prevention - Profile selection

- 2. Enter the **actions menu** [  ] and click on the option "Delete Profile".

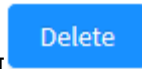
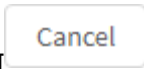


Intrusion Prevention – Delete Profile

- 3. The notification message will appear asking if you really want to delete the selected Profiles:



Intrusion Prevention - Profile deletion confirmation message.



If you want to cancel click on the [ ] button. To finish, click the [ ] button.



**Profile removed successfully**

*The profile has been successfully deleted.*

After performing these procedures, the profiles will have been successfully deleted.

Next, we will look at the [Columns menu](#).




# Intrusion Prevention - Columns

Next we will explain each column of the Intrusion Prevention tab:

Profiles

Web FilterApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN




1 records

<input type="checkbox"/>	Name	Description	Version	Type	Processes	Actions
<input type="checkbox"/>	Stores Intrusion Prevention	Intrusion Prevention for the Stores	2.0	firewall	1	  

< 1 > 10 / page

Profiles – Intrusion Prevention

In the following we will explain each column:

- **Checkbox**[ ☐ ]: Select the profile;
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Type**: Determines what type of prevention will be applied. The available options are Firewall, Transparent and Passive;
- **Processes**: Determines the number of simultaneous processes for loading the profile. Each process refers to a thread. We recommend that this value be “ less or Equal” to the number of processing cores in your Appliance;
- **Actions**: The “Actions” column is made up of several buttons:
  - **Edit** [  ]: Allows you to edit the settings of the profile added in the [Create Profile](#) option of the actions menu;
  - **List Profiles** [  ]: Allows you to view, edit and add more specific profile options, for more information, check [Intrusion Prevention - Create Profile](#);
  - **Delete** [  ]: Delete the profile.

Next, the functions of the [List Profiles](#) button will be explained and exemplified.

# Intrusion Prevention - Create Profile

By clicking on the **detail button**  it is possible to configure the profile;

Create Profile

Settings

Client

Server

General

\*

Name

Intrusion Prevention - Stores

Description

Intrusion Prevention - Stores

Version

2.0

Mode

\*

Processes

1

Device

Device

Type

Firewall

Transparent

Passive

Device

Definitions

Enable client recommended rules

Enable server recommended rules

Inspect all ports

Restore

Cancel

Save

Intrusion Prevention - Create Profile

## Settings Tab

In this tab it is possible to make the general configurations, definitions and the way in which Intrusion Prevention works.

### General

In "General" we have the following text boxes:



**General**

**\* Name**  
Stores Intrusion Prevention

**Description**  
Intrusion Prevention for the Stores

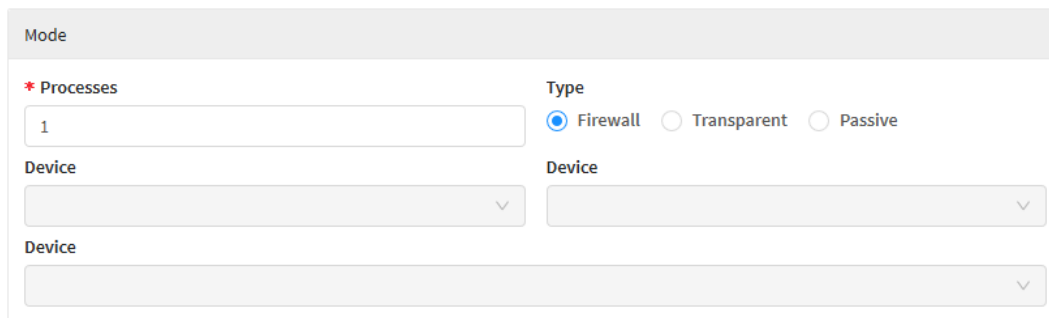
**Version**  
2.0

Intrusion Prevention – General

- **Name:** Define a name for the profile. Ex.: Intrusion Prevention - Stores;
- **Description:** Define a description for the profile. Ex.: Intrusion Prevention - Stores;
- **Version:** Determine the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible.

## Mode

In "Mode" are determined the applications whose access will be allowed or denied:



**Mode**

**\* Processes**  
1

**Type**  
☒ Firewall 
 ☐ Transparent 
 ☐ Passive

**Device**

Intrusion Prevention - Mode

- **Processes:** Define a name for the profile. Ex.: Intrusion Prevention - Stores;
- **Type:** Select the IPS operating mode. The available types are: Firewall, Transparent and Passive;
- **Flow:** This item is only required for configuration in "Transparent". Select the packet targeting flow. The flow is determined by the input device of the packet. Ex.: Eth1 : Eth2;
- **Interface:** This item is only required for configuration in "Passive" mode. Select the incoming packet flow network interface. Ex.: Eth1.



In the Flow and Interface fields, the network interfaces must be "enabled" and without an IP address.

## Definitions

In "Definitions" are determined the applications whose access will be allowed or denied:

Definitions

☒ Enable client recommended rules
 ☒ Enable server recommended rules
 ☐ Inspect all ports

#### Intrusion Prevention - Definitions

- **Enable client recommended rules** ☒: Enabling this option enables the display of Blockbit's standard ATP rules. These rules will be displayed on the client;
- **Enable server recommended rules** ☒: Enabling this option enables the display of Blockbit's standard IPS rules. These rules will be displayed on the server tab;
- **Inspect all ports** ☒: Enables independent inspection of the port the application is running on.



Enabling the Inspect all Ports option limits the process of your network traffic.

## Client tab

When enabling the **Enable client recommended rules** option in the Settings tab, the Client tab will display the ATP signatures as shown below:



For more information about ATP, refer to the Blockbit UTM manual.

Status

All

Quarantine

Disabled

Risk

All

Category

All

Name / SID

Status	Block	Quarantine	Risk	Category	Name	SID
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Low</div>	browser-other	BROWSER-OTHER Adobe Acrobat Pro ...	<div>45043</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Low</div>	browser-other	BROWSER-OTHER Adobe Acrobat Pro ...	<div>45042</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Medium</div>	browser-other	BROWSER-OTHER Android browser file ...	<div>40458</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Medium</div>	browser-other	BROWSER-OTHER Android Browser pot...	<div>40361</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>High</div>	browser-other	BROWSER-OTHER Android WebView sa...	<div>32029</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Medium</div>	browser-other	BROWSER-OTHER Apple iOS CoreGrap...	<div>38135</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Low</div>	browser-other	BROWSER-OTHER Apple Safari docume...	<div>44051</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Low</div>	browser-other	BROWSER-OTHER Apple Safari docume...	<div>44050</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Medium</div>	browser-other	BROWSER-OTHER Apple Safari javascr...	<div>45355</div>
<div><div></div></div>	<div><div></div></div>	<div><div>Disabled</div><div></div></div>	<div>Medium</div>	browser-other	BROWSER-OTHER Apple Safari javascr...	<div>45354</div>

Total items: 3799

<

1

2

3

4

5

...

380

>

10 / page

#### Intrusion Prevention - Client

The signatures are divided as follows:

- **Status:** Defines whether the subscription is “Enable / Disable”;
- **Block:** Defines if the subscription is “Enable / Disable” for blocking;
- **Quarantine:** It is possible to “Enable / Disable” the quarantine option informing if it will be validated by source or destination IP. By enabling the quarantine option automatically, the system will enable the signature with the **block** status. With that, all traffic that matches the signature will dynamically insert the address into the quarantine in this way, keeping it blocked according to the time that was configured for quarantine;
- **Risk:** Which determines the risk of the signature based on the criticality and complexity of the attack that can be of the **Low**, **Medium** and **high** type;
- **Category:** These are groups of signatures that serve the same purpose;
- **Name:** Determines the name of the subscription in the system;
- **SID:** It is the unique identifier of the signature.



Enable or clear the checkbox **Enable rules recommended by the client** or **Enable rules recommended by the server** in Settings tab, some SIDs will be highlighted, the SID in blue is the default recommended by Blockbit (for example, when editing some of them, it will becomes gray).

See the example below, where the third and fourth SID are highlighted:

Status	Block	Quarantine	Risk	Category	Name	SID
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46978
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Cr...	46977
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49360
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	49361
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21446
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome Fil...	21447
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome flo...	19710
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Medium	browser-chrome	BROWSER-CHROME Google Chrome FT...	16795
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16667
<input type="checkbox"/>	<input type="checkbox"/>	Disabled ▾	Low	browser-chrome	BROWSER-CHROME Google Chrome GU...	16668

*Highlighted SID example*

## Server tab

When enabling the **Enable server recommended rules** option on the Settings tab, the Server tab will display the IPS signatures as shown below:



For more information on IPS, refer to the Blockbit UTM manual.

Status	Quarantine	Risk	Category	Name / SID
All	Disabled	All	All	<input type="text"/>

Status	Block	Quarantine	Risk	Category	Name	SID
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Low	attack_response	ATTACK_RESPONSE 401TRG Perl DDoS ...	2024977
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Medium	attack_response	ATTACK_RESPONSE ALBANIA id.php de...	2007656
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Low	attack_response	ATTACK_RESPONSE Backdoor reDuh ht...	2011667
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Medium	attack_response	ATTACK_RESPONSE C99 Modified phps...	2007654
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Medium	attack_response	ATTACK_RESPONSE c99shell phpshell ...	2007652
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Medium	attack_response	ATTACK_RESPONSE Cisco TcIShell TFT...	2009245
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Medium	attack_response	ATTACK_RESPONSE Cisco TcIShell TFT...	2009244
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	Low	attack_response	ATTACK_RESPONSE FTP CWD to windo...	2008556
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	High	attack_response	ATTACK_RESPONSE FTP inaccessible di...	2000507
<input type="checkbox"/>	<input type="checkbox"/>	Disabled	High	attack_response	ATTACK_RESPONSE FTP inaccessible di...	2000499

Total items: 24029 < 1 2 3 4 5 ... 2403 > 10 / page

Intrusion Prevention - Server

The signatures are divided as follows:

- **Status:** Defines whether the subscription is "Enable / Disable";
- **Block:** Defines if the subscription is "Enable / Disable" for blocking;
- **Quarantine:** It is possible to "Enable / Disable" the quarantine option informing if it will be validated by source or destination IP. By enabling the quarantine option automatically, the system will enable the signature with the **block** status. With that, all traffic that matches the signature will dynamically insert the address into the quarantine in this way, keeping it blocked according to the time that was configured for quarantine;
- **Risk:** Which determines the risk of the signature based on the criticality and complexity of the attack that can be of the **Low**, **Medium** and **high** type;
- **Category:** These are groups of signatures that serve the same purpose;
- **Name:** Determines the name of the subscription in the system;
- **SID:** It is the unique identifier of the signature.

## Restore button

If at any time you want to restore the profile and default settings of Blockbit, click the Restore button, the following window will be displayed.

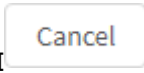
Are you sure?

Do you really want to restore the profile to default?


Cancel Restore

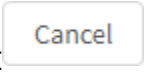
Intrusion Prevention - Do you really want to restore the profile to default?






Click the [ ] button to exit this window or the [ ] button to restore the profile pattern.

 **Profile restored.**  
Profile restored




Finally, if you want to cancel click on the [ ] button. To finish editing the applications click on the button [ ] button.

 **Saved successfully**  
Saved successfully

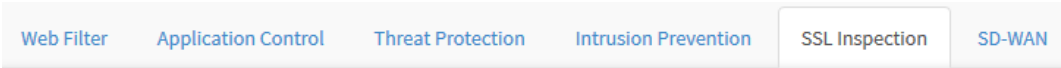
The settings have been successfully made.

# SSL Inspection tab

SSL Inspection works by intercepting SSL traffic and inspecting encrypted content, using this feature it is possible to select the content to be inspected through compliance policies.

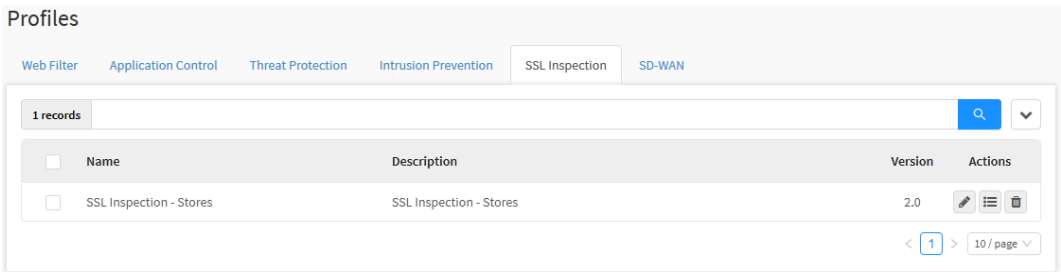
 For more information on SSL Inspection, see this [page](#) of the Blockbit UTM manual.

Click on the “SSL Inspection” tab.



SSL Inspection tab

The “SSL Inspection” Screen will appear. It is composed of the “Name”, “Description”, “Mode”, “Version” and “Actions” columns. In addition, the search bar and the [actions menu](#) are located at the top right of the screen.



Profiles – SSL Inspection

Next, the [actions menu](#) will be analyzed and later we will delve into the content of the [columns](#) of the SSL Inspection panel.

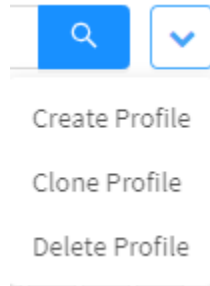
# SSL Inspection - Actions menu

At the top right of the screen we have the actions menu:



SSL Inspection – Actions Menu Button

By clicking on this button the menu below is displayed:



SSL Inspection – Actions Menu

The menu consists of the following options:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

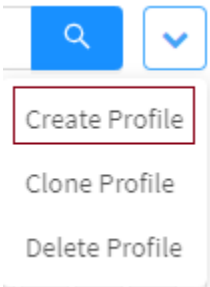
Next, each action menu option will be detailed.

# SSL Inspection - Action Menu - Create Profile



Through the option "Create Profile" it is possible to create a new SSL Inspection profile. To access, click on the actions menu [  ].

1. Click on the "Create Profile" option;



SSL Inspection - Create Profile

2. The "Create SSL Profile" screen will be displayed. Fill it with the following data:

SSL Inspection – Create SSL Profile

- **Name:** Profile name. Ex.: Stores;
- **Description:** Profile description. Ex.: Application Control - Stores;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM's;



**ATTENTION:** If the version of the profile is different from that of the UTM, they will not be compatible.

Always create profiles with the same version of the UTMs to which they will be applied.

---

A rectangular button with a thin border and the word "Cancel" in a sans-serif font.A solid blue rectangular button with the word "Save" in white sans-serif font.

If you want to cancel click on the [ ] button. To complete the creation of the policy package click on the [ ] button.

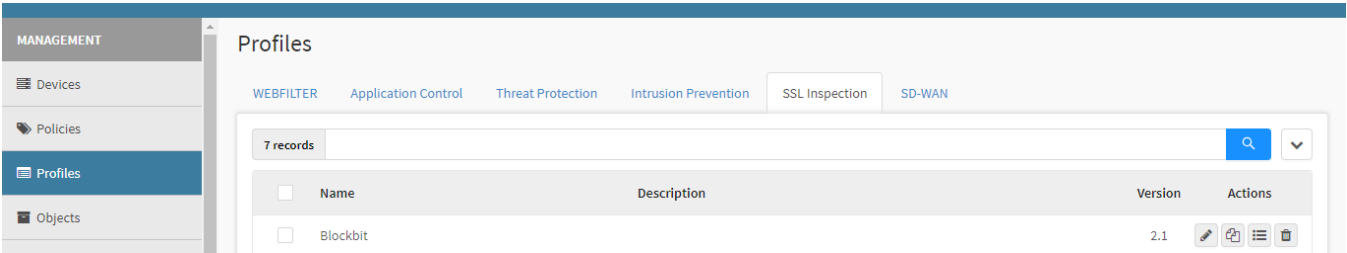
 **Profile saved successfully**

*The profile has been successfully saved.*

Next, we will look at how to [Clone a Profile](#).

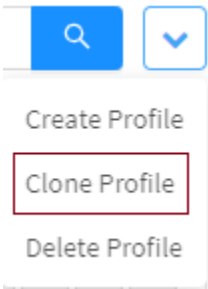
# SSL Inspection - Action Menu - Clone Profile

Through the "Clone Profile" option it's possible to clone an SSL Inspection profile. To access, click on the actions menu [  ].



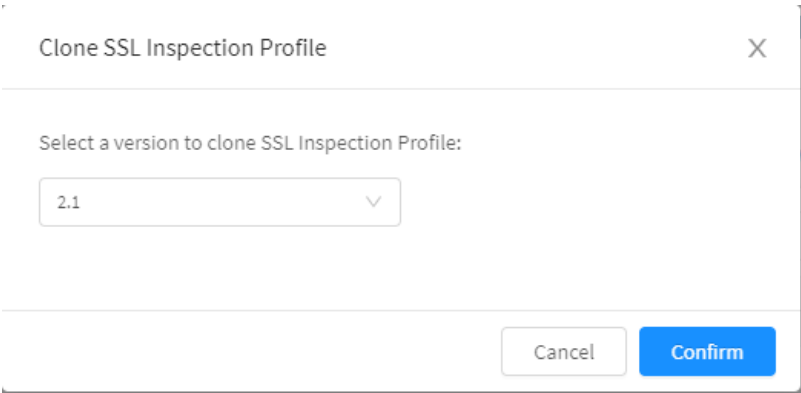
SSL Inspection - Main menu.

1. Click on the "Clone Profile" option;



SSL Inspection - Clone Profile.

2. To confirm, just click in the "Confirm button":



SSL Inspection - Clone Profile.

MANAGEMENT

Devices

Policies

Profiles

Objects

Users

Profiles

WEBFILTERApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN

8 records

Name

Description

Version

Actions


Blockbit-clone

2.1

Blockbit

2.1


The profile has been successfully cloned.

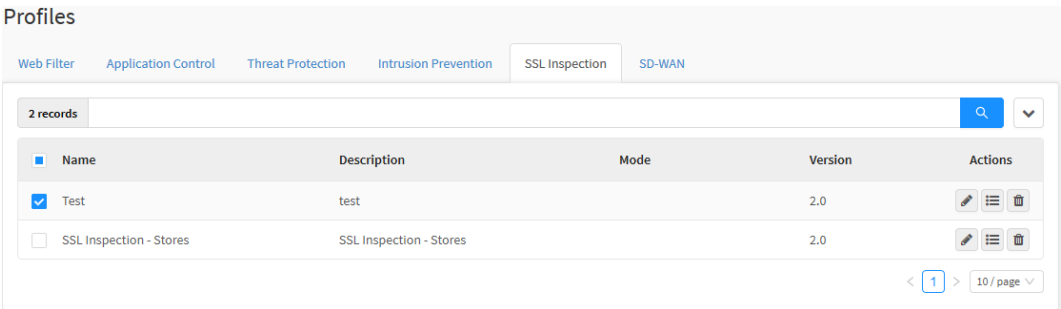
It's also possible to clone a profile by clicking the "Clone" button [

Next we will look at how to [Delete a Profile](#).

# SSL Inspection - Actions Menu - Delete Profile

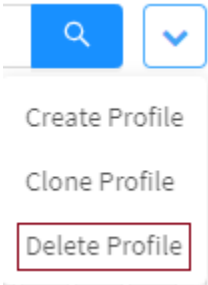
Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles the checkbox will change from gray to blue . Ex.: Test;



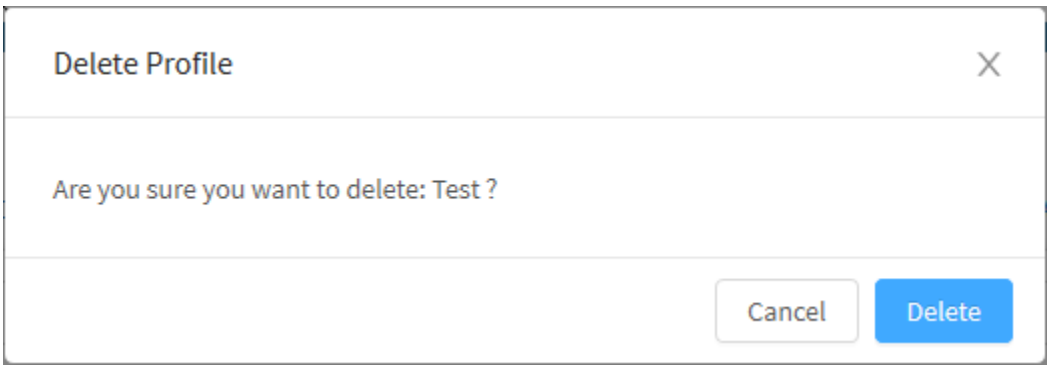
SSL Inspection – Profile selection

2. Enter the **actions menu**  and click on the "Delete Profile" option.



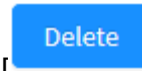
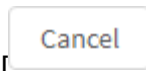
SSL Inspection – Delete Profile.

3. The notification message will appear asking if you really want to delete the selected Profiles:



SSL Inspection – Message if you want to delete the profiles





If you want to cancel click on the button [ ] button. To finish, click the button [ ] button.



**Profile deleted successfully!**

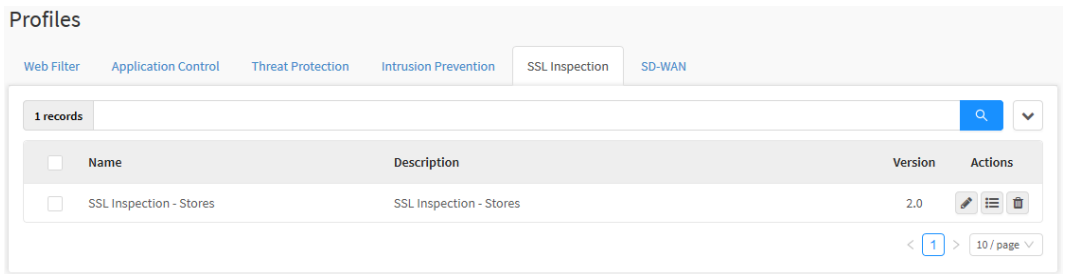
*The profile has been successfully deleted.*

After performing these procedures, the profiles will have been successfully deleted.

Now we will look at the [Columns Menu](#).

# SSL Inspection - Columns

In the following we will explain each column of the SSL Inspection tab:




Profiles – SSL Inspection

In the following we will explain each column:

- **Checkbox** [ ☐ ]: Select the profile.
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Actions**: The “Actions” column is made up of several buttons:
  - **Edit** [ ]: Allows you to edit the settings of the profile added in the [Create Profile](#) option of the actions menu;
  - **List Profiles** [ ]: Allows you to view, edit and add more specific profile options, for more information, check [SSL Inspection - SSL Profile](#);
  - **Delete** [ ]: Delete the profile.

Next, the functions of the [List Profiles](#) button will be explained and exemplified.

# SSL Inspection - SSL Profile

By clicking on the detail [  ] button it is possible to configure the profile;

In this panel it is possible to make general configurations, inspection exceptions and which protocols are used in this profile.

SSL Profile

General

\*

Name

SSL Inspection - Stores

Description

SSL Inspection - Stores

\*

Protocols

☒ HTTPS

☐ SMTPS

☐ POP3S

Inspection Exception

☒ Web Categories



1 Selected

Cancel

Save

SSL Inspection - SSL Profile

- **Name:** Define a name for the profile. Ex.: *SSL Inspection - Stores*;
- **Description:** Define a description for the profile. Ex.: *SSL Inspection - Stores*;
- **Protocols:** Determines which protocols will be used by SSL Inspection. The available options are: *HTTPS*, *SMTPS* e *POP3S*;
- **Inspection Exception:** Determines exceptions to SSL inspection. The values entered in this field will be added as tags;
- **Web Categories:** It allows selecting the web categories to apply "Block" or "Exception" filters to the set of applied policies. To select the

categories, click the [  ] button, choose the desired categories by checking the checkbox [  ], as shown below:


351

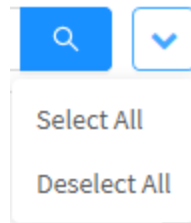
Add Category
X

All

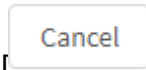
- ☐ Uncategorized Sites
- ▼ ☐ Abortion
  - ☐ Pro-life
  - ☐ Pro-Choice
- ☐ Activism Groups
- ▼ ☒ Adult Material
  - ☒ Adult Content
  - ☒ Nudity
  - ☒ Sex
  - ☒ Sex Education
  - ☐ Lingerie and Swimsuit
- ▼ ☐ Business and Economy
  - ☐ Financial Data and Services
- ▼ ☒ Drugs
  - ☒ Abused Drugs
  - ☐ Prescribed Medications

SSL Inspection - Add Category

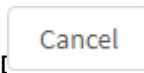
If it is necessary to make a configuration on all items, just select the desired option in the **actions menu** [  ]:



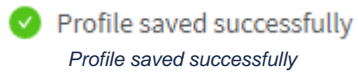
SSL Inspection - Add Category - Actions Menu



To exit this panel, click the [ ] button or click the [ ] button to complete adding the categories.




Finally, if you want to cancel the configuration click on the [ ] button. To finish editing the profile click on [ ] button.



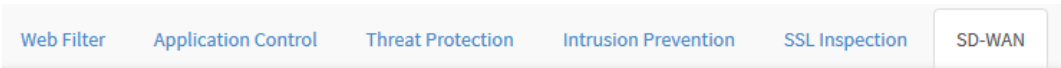
The profile has been successfully edited.

# SD-WAN tab

The monitoring function of the SD-WAN is to allow the supervision of specific data from the WAN, enabling the best network path according to the factors determined by the administrator, this allows directing the most appropriate resources according to predetermined rules and policies or based on in the specific profile of users.

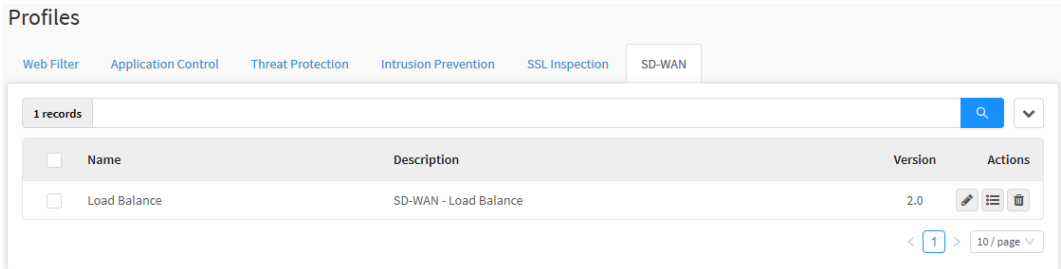
 For more information on SD-WAN, refer to the Blockbit UTM manual.

Click on the “SD-WAN” tab.



SD-WAN tab

The “SD-WAN” screen will appear. It consists of the “Name”, “Description”, “Version” and “Actions” columns. In addition, at the top right of the screen is located the [search bar](#) and the actions menu.



Profiles – SD-WAN

Next, the [actions menu](#) will be analyzed and later we will delve into the content of the [columns](#) of the SSL Inspection panel.

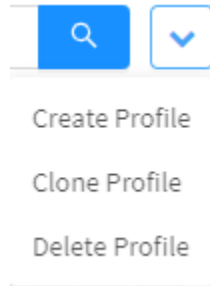
# SD-WAN - Actions menu

At the top right of the screen we have the actions menu:



SD-WAN – Actions Menu button

By clicking on this button the menu below is displayed:



SD-WAN – Actions menu

The menu consists of the following options:

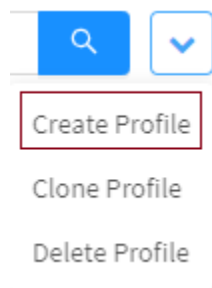
- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

Next, each action menu option will be detailed.

## SD-WAN - Actions menu - Create Profile

Through the option “Create Profile” it is possible to create a new SD-WAN profile. To access, click on the **Actions menu** [  ].

1. Click on the “Create Profile” option;



## SD-WAN - Create Profile

2. The “Create Profile SDWAN” screen will be displayed. Fill it with the following data:

- **Name:** Profile name. Ex.: *Load Balance*;
- **Description:** Profile description. Ex.: *SD-WAN - Load Balance*;
- **Version:** Defines the version that will be used in the profile. It is important that the version is the same as the UTM's;



**ATTENTION:** If the version of the profile is different from that of the UTM, they will not be compatible.

Always create profiles with the same version of the UTMs to which they will be applied.

Create Profile SDWAN

X

\* Name

Load Balance

Description

SD-WAN - Load Balance

\* Version

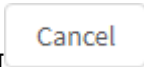
2.0

Cancel

Save

## SD-WAN – Create an SD-WAN Profile






If you want to cancel click on the [




] button. To complete the creation of the policy package click on the [

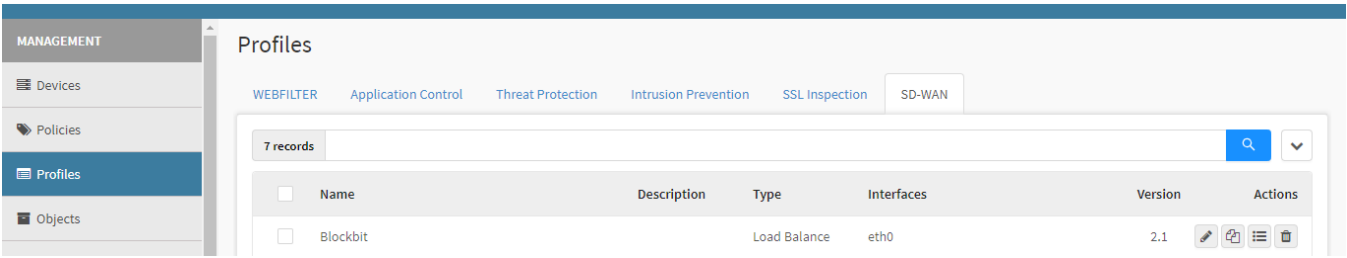
 Profile saved successfully

*The profile has been successfully saved.*

Now, we will look at how to [Clone a Profile](#).

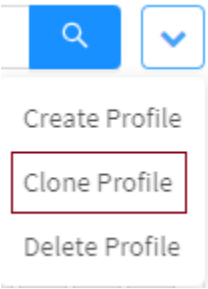
# SD-WAN - Actions menu - Clone Profile

Through the "Clone Profile" option it's possible to clone a new SD-WAN profile. To access, click on the **Actions menu** [  ].



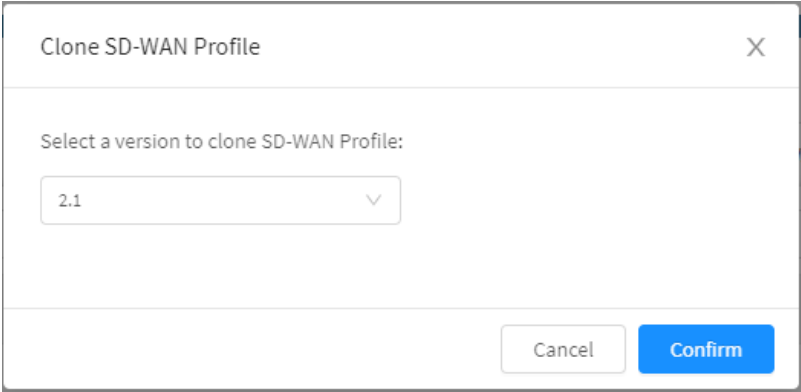
SD-WAN - Main Screen.

1. Click on the "Clone Profile" option:



SD-WAN - Clone Profile

2. To confirm just click the "Confirm" Button:



SD-WAN - Clone Profile

MANAGEMENT

Devices

Policies

Profiles









Objects

Users


Profiles

WEBFILTERApplication ControlThreat ProtectionIntrusion PreventionSSL InspectionSD-WAN

8 records

<input type="checkbox"/>	Name	Description	Type	Interfaces	Version	Actions
<input type="checkbox"/>	Blockbit-clone		Load Balance	eth0	2.1	   
<input type="checkbox"/>	Blockbit		Load Balance	eth0	2.1	   


The profile has been successfully cloned.

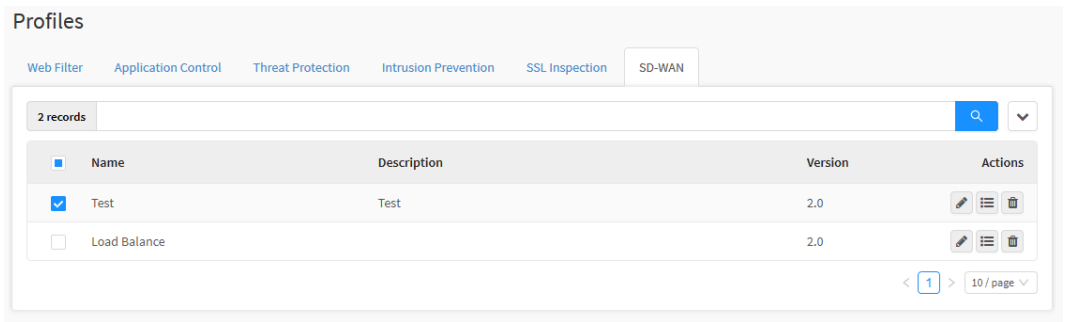
It's also possible to clone a profile by clicking the "Clone" button [].

Next we will look at how to [Delete a Profile](#).

# SD-WAN - Actions menu - Delete Profile

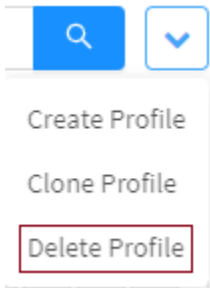
Through the button "Delete Profile" it is possible to delete the selected Profiles. To delete from the actions menu, follow these steps:

- 1. Select which Profile (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Name. In the selected profiles the checkbox will change from gray to blue . Ex.: Test;



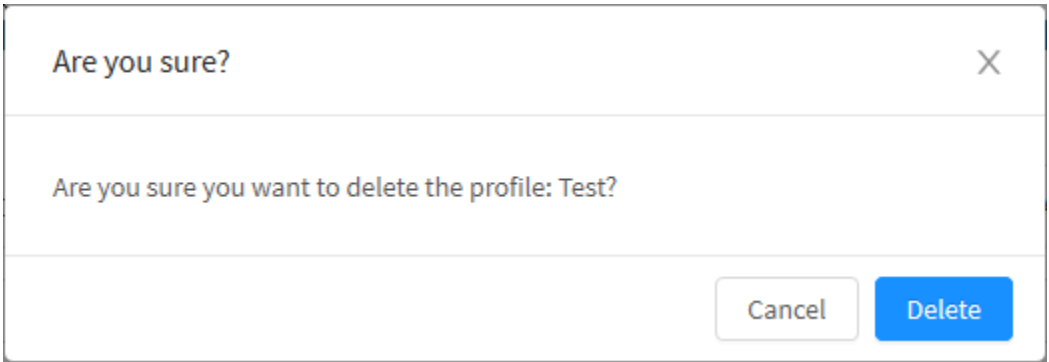
SD-WAN – Profile selection

- 2. Enter the Actions Menu and click on the "Delete Templates" option.

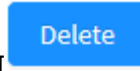
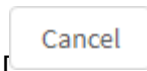


SD-WAN – Delete Profiles.

- 3. The notification message will appear asking if you really want to delete the selected Profiles:



SD-WAN – Profile deletion confirmation message



If you want to cancel click on [ ] button. To finish, click on [ ] button.



**Profile deleted successfully!**

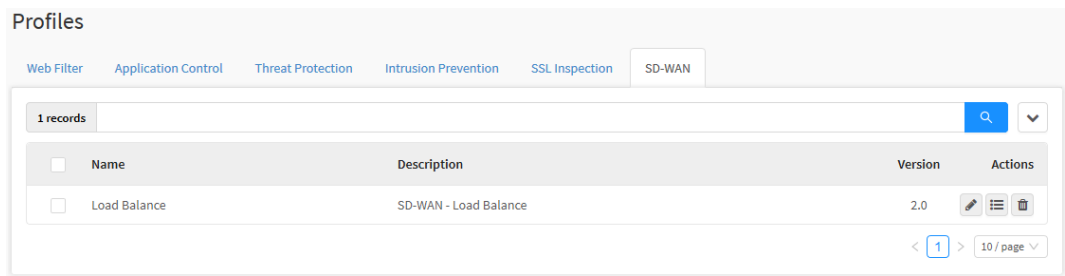
*The profile has been successfully deleted.*

After performing these procedures, the profiles will have been successfully deleted.

Next, we will look at the [Columns Menu](#).





# SD-WAN - Columns

In the following we will explain each column of the SD-WAN tab:




Profiles – SD-WAN.


In the following we will explain each column:

- **Checkbox** [  ]: Select the profile.
- **Name**: Displays the name of the registered profile;
- **Description**: Displays the description of the registered profile;
- **Version**: Displays the version in which the profile was created. It is extremely important to create profiles of the same version as UTM, otherwise the profile will not be compatible;
- **Actions**: The "Actions" column is made up of several buttons:
  - **Edit** [  ]: Allows you to edit the settings of the profile added in the [Create Profile](#) option of the actions menu;
  - **List Profiles** [  ]: Allows you to view, edit and add more specific profile options, for more information, check [SD-WAN - SDWAN Profile](#);
  - **Delete** [  ]: Delete the profile.

Next, the functions of the [List Profiles](#) button will be explained and exemplified.

# SD-WAN - SDWAN Profile

By clicking on the **detail** [  ] button it is possible to configure the profile;

 For more information on each configuration, see this [page](#) of the Blockbit UTM manual.

In this panel it is possible to make all the configurations referring to the performance of the SD-WAN. Next we will demonstrate configuring the Load Balance.

## Interfaces tab

In this tab it is possible to configure how the SD-WAN will interact with the eth interfaces.

SDWAN Profile

X

Interfaces

Monitor

General

\* Name

Load Balance

Description

SD-WAN - Load Balance

\* Type

Load Balance

\* Fail ratio (1 - 100%)

10

\* Monitoring Interval (sec)

5

☒ Persistence timeout 1-1440 min

30

Interfaces

ETH0

0%

☐

ETH1

0%

☐

ETH2

0%

☐

ETH3

0%

☐

Cancel

Save

363

## General

In "General" we have the following text boxes:

The screenshot shows the 'General' configuration tab for an SD-WAN profile. The fields are as follows:

- Name:** Load Balance
- Description:** SD-WAN - Load Balance
- Type:** Load Balance (dropdown menu)
- Fail ratio (1 - 100%):** 10
- Monitoring Interval (sec):** 5
- Persistence timeout 1-1440 min:** 30 (checkbox is checked)

SD-WAN – General

- **Name:** Define a name for the profile. Ex.: Load Balance;
- **Description:** Set a description for the profile. Ex.: SD-WAN - Load Balance;
- **Type:** In this field it is defined how the SD-WAN will act. Selecting these options defines which text fields will be displayed in the General panel. It is possible to select any type, but in this demonstration we will use "Load Balance". For more information about the types of SD-WAN check the chapter [Types of Profile](#). The available options are:
  - Load Balance;
  - Failover;
  - Spillover;
  - Dynamic Selection.
- **Interfaces:** It is essential for the correct functioning of the SD-WAN to define the internet link interfaces that will be used in the composition of the profile. In this example we will select the interfaces: "tun0 – Network 10" and "tun1 – Network 11";
- **Monitoring Interval (sec.):** Define the monitoring interval between each test. It is recommended to leave as 1 second. Ex.: 1 second;
- **Fail Ratio 1-100%:** Set the failure rate value between 1 to 100%. It is recommended to leave the default of 70%. Ex.: 70%.

## Interfaces

In "Interfaces" we have the following options:




Interfaces

⋮	ETH0	50%	<input checked="" type="checkbox"/>
⋮	ETH1	50%	<input checked="" type="checkbox"/>
⋮	ETH2	0%	<input type="checkbox"/>
⋮	ETH3	0%	<input type="checkbox"/>

SD-WAN – Interfaces



It is only possible to interact with the interfaces that have been **enabled** [ ☒ ] if an interface is **disabled** [ ☐ ], it will be grayed out, it will not be possible to edit it and will be disregarded.

- **Mover** [  ]: Click and drag to the desired position, so the link that is in the first position from top to bottom will be used for outgoing traffic, if the link is disabled, traffic will be automatically redirected to the subsequent link in the list, thus ensuring high availability of internet access, when the link is enabled again, the system will automatically return the output to the first link in the list;
- **Interfaces**: It is essential for the correct functioning of the SD-WAN to define the internet link interfaces that will be used in the composition of the profile. In this example we will select the interfaces: "eth0" and "eth1";

## Monitor Tab

In this tab are configured the performance indicators and monitoring targets, used by the SD-WAN.

SD-WAN Profile

×

Interfaces

Monitor

\* Performance Indicators

☒ Latency (ms)
 ☐ Jitter (ms)

☐ Packet Loss (%)
 ☐ Bandwidth (%)

10

10

10

85

Monitoring Targets

\* Address

\* Protocol

\* Attempts

\* Timeout

www.blockbit.com

ICMP

3

3 sec.

+

Cancel

Save

SD-WAN - SDWAN Profile - Monitor Tab

## Performance Indicators

In "Performance Indicators" we have the following text boxes:

\* Performance Indicators

☒ Latency (ms)
 ☐ Jitter (ms)

☐ Packet Loss (%)
 ☐ Bandwidth (%)

10

10

10

85

SD-WAN – SDWAN Profile - Performance Indicators

- **Latency:** Determines how long it takes for a data packet to leave the origin, arrive at the destination, and return. Ex.: 10 ms;
- **Jitter:** Determines the average of how long it takes for a data packet to leave the origin, arrive at the destination and return. Ex.: 30 ms;
- **Packet Loss:** Determines the acceptable percentage of packet loss. Ex.: 75%;
- **Bandwidth:** Determines the acceptable percentage of bandwidth consumption. Uses as a base the download values in "Traffic Shaping". Ex.: 70%.



For more information on each configuration, refer to this [page](#) of the Blockbit UTM manual.

## Monitoring Targets

In "Monitoring Targets" we have the following text boxes:

* Address	* Protocol	* Attempts	* Timeout
<input type="text" value="www.blockbit.com"/>	<input type="text" value="ICMP"/>	<input type="text" value="3"/>	<input type="text" value="3 sec."/>

*SD-WAN – SDWAN Profile - Monitoring Interfaces*

Defines the addresses where the tests will be performed. It is recommended that in the "Monitoring Targets" the virtual IPs are placed on the other side of the tunnel so that if the communication is successful, this indicates that the Tunnel is correctly configured.

Cancel

Save

Finally, if you want to cancel click the [Cancel] button. To finish editing the applications click on the [Save] button.

# Objects

This section will demonstrate how to create, edit, and delete objects.

The system was developed object-oriented to facilitate the process of adjusting, maintaining and reading rules and configurations.

Objects can be shared between system services and devices.

All changes applied to an object are automatically replicated and applied to all services in use by the respective object.

To access the screen, simply select the "Objects" button;



The screen below will appear:

Objects

Addresses

Services

Times

Schedules

Dictionaries

Contents

9 records

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Class A network	Reserved network Class A 10.0.0.0/8	IPv4	<div>i</div>	<div></div> <div></div>
<input type="checkbox"/>	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Localhost	Loopback 127.0.0.1	IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Private class network	Special-use address reserved to private network (A...	IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Skype Servers		IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Teste endereço		IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Webex Servers		IPv4	-	<div></div> <div></div>
<input type="checkbox"/>	Whatsapp Servers		IPv4	-	<div></div> <div></div>

< 1 >

10 / page

Objects - Addresses

The Objects screen has the following tabs:

- [Addresses](#);
- [Services](#);
- [Times](#);
- [Schedules](#);
- [Dictionaries](#);
- [Contents](#).

Next, the components of the [Addresses](#) tab will be analyzed.

# Objects - Addresses

Address type objects are used to identify hosts (machines) or networks (networks).

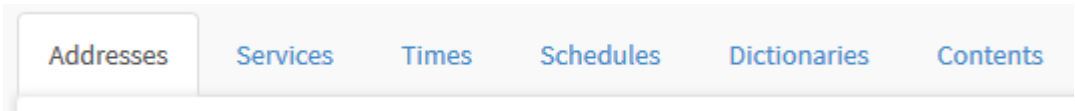
By default, the system brings some pre-registered objects, for example, objects referring to invalid network classes: "Class A reserved", "Class B reserved", "Class C reserved".

All of these objects are available to be used in the processes of configuring and enabling services.

Blockbit GSM allows the definition of three ways of identifying Address:

- **IP address / Network address:** They are objects that identify machines and networks through their IP addresses. Ex .: 172.16.102.235 or 172.16.102.0/24;
- **MAC address:** They are objects that identify the machines through the physical addresses of their network cards. Ex .: 38:59:F9:1F:4E:16;
- **FQDN address:** They are objects that identify the machines through their DNS address. Ex .: [blockbit.com](#) or [www.blockbit.com](#);

To access, click on the "Addresses" tab:



Addresses tab

The "Adresses" screen will appear. It consists of the columns "Select", "Name", "Description", "Type", "Used" and "Actions". In addition, at the top of the screen is the [search bar](#) and the [action menu](#) on the right.

Objects

Addresses Services Times Schedules Dictionaries Contents

9 records

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Class A network	Reserved network Class A 10.0.0.0/8	IPv4	1	
<input type="checkbox"/>	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	
<input type="checkbox"/>	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	
<input type="checkbox"/>	Localhost	Loopback 127.0.0.1	IPv4	-	
<input type="checkbox"/>	Private class network	Special-use address reserved to private network (A...	IPv4	-	
<input type="checkbox"/>	Skype Servers		IPv4	-	
<input type="checkbox"/>	Teste endereço		IPv4	-	
<input type="checkbox"/>	Webex Servers		IPv4	-	
<input type="checkbox"/>	Whatsapp Servers		IPv4	-	

< 1 > 10 / page

Objects – Addresses

We will explain in detail the [action menu](#) and later the columns of the "Addresses" tab.

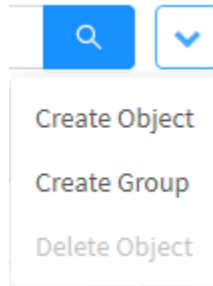
# Objects - Addresses - Actions Menu

At the top right of the screen we have the actions menu:



Objects - Actions menu button

By clicking on this button the menu below is displayed:



*Objects - Actions menu*

The menu consists of the following options:

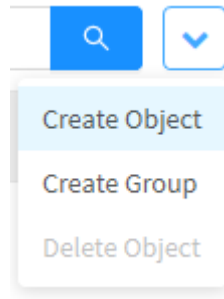
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

Next, each action menu option will be detailed.

# Objects - Addresses - Actions Menu - Create Object

Through the option "Create Object" it is possible to create a new Object Address. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;



*Objects – Addresses – Create Object*

2. The Create Addresses Object screen will appear. Fill in the fields:

Create Addresses Object

×

\* Name

\* Type

IPv4 Address

▼

☐ Unique

\* Address

Mask

255.255.255.255

▼

+

^

▼

–

Description

Cancel

Import Address

Save

Objects – Create Addresses Object

It is possible to create IPv4, IPv6, Mac and FQDN addresses. Here are some examples:

- [Example 1 - Creating IPv4 Address Object;](#)
- [Example 2 - Creating IPv6 Address Object;](#)
- [Example 3 - Creating Physical Address Object.](#)



# Objects - Example 1 - Creating an IPv4 Address Object

Here is a demonstration of how to create an IPv4 address object:

Create Addresses Object

\* Name

Servers IP

\* Type

IPv4 Address

☐ Unique

\* Address

Mask

255.255.255.255

+

10.0.0.1  
189.175.102.208  
172.16.0.0

-

Description

Servers IP

Cancel

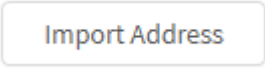


Import Address

Save

Objects – Create Addresses Object - IPv4

**Attention:** Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- **Name:** Name of the object. Ex .: IP Servers;
- **Type:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- **Unique**☐: Determines whether the address will be unique or not, disabling the Mask field;
- **Address:** The address of the type of connection object selected later. After entering an address, click [] to add it to the list or select it and click [] to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- **Mask:** This field will be available to add the IP address mask, if the type IPv4 Address or IPv6 Address is selected in the field "type";
- **Description:** This field is intended for the object description. Ex.: Servers IP.

By clicking on the **Import Address**  button and select the file to be imported, click  to add the contents of the file inside the object, if you want to remove any registered address, select the IP address and click the button  and the content will be removed.



The supported format of the list is one IP or network address per line.



*Ex.: 10.0.0.1*

*189.175.102.208*

*172.16.0.0/16*

Cancel

Save

Click on the  button to Cancel or  button to save.



**Object successfully changed!**

*Object successfully changed*

The object address was created successfully.

Here is a demonstration of how to create an IPv4 address object:

Create Addresses Object

X

\* Name

Servers IP

\* Type

IPv4 Address

Unique

\* Address

Mask

255.255.255.255

+

10.0.0.1

189.175.102.208

172.16.0.0

-

Description

Servers IP

Cancel



Import Address

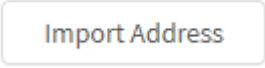


Save

Objects – Create Addresses Object - IPv4



**Attention:** Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- **Name:** Name of the object. Ex.: IP Servers;
- **Type:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- **Unique** ☐: Determines whether the address will be unique or not, disabling the Mask field;
- **Address:** The address of the type of connection object selected later. After entering an address, click  to add it to the list or select it and click  to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- **Mask:** This field will be available to add the IP address mask, if the type IPv4 Address or IPv6 Address is selected in the field "type";
- **Description:** This field is intended for the object description. Ex.: Servers IP.

By clicking on the **Import Address** [  ] button and select the file to be imported, click [  ] to add the contents of the file inside the object, if you want to remove any registered address, select the IP address and click the button [  ] and the content will be removed.



The supported format of the list is one IP or network address per line.

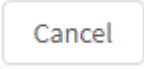
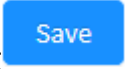
*Ex.: 10.0.0.1*

*189.175.102.208*

*172.16.0.0/16*

Cancel

Save

Click on the [  ] button to Cancel or [  ] button to save.



**Object successfully changed!**

*Object successfully changed*

The object address was created successfully.

# Objects - Example 2 - Creating IPv6 Address Object

Here is a demonstration of how to create an IPv6 address object:

Create Addresses Object

\* Name

Server IPs - IPv6

\* Type

IPv6 Address

☐ Unique

\* Address

Prefix

128

+

2001:db8::1

2001:db8::2

2001:db8::3

2001:db8::4

−

Description

Server IPs - IPv6

Cancel

Import Address

Save

Objects – Create Addresses Object - IPv6

**Attention:** Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- **Name:** Name of the object. Ex .: Server IPs - IPv6;
- **Type:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- **Unique**☐: Determines whether the address will be unique or not, disabling the Prefix field;
- **Address:** The address of the type of connection object selected later. After entering an address, click [] to add it to the list or select it and click [] to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- **Prefix:** Defines the prefix of the IP address that will be added to the object. Ex.: 128;
- **Description:** This field is intended for the object description. Ex.: Server IPs - IPv6.

Import Address



By clicking on the button [ ] and select the file to be imported, click [ ] to add the contents of the file inside the object, if



you want to remove any registered address, select the IP address and click the button [ ] and the content will be removed.



The supported format of the list is one IP or network address per line.

Ex.: 2001::FF:01/68

::FF:0A/128

2001:abcd:172.16.102.0/120

Cancel

Save

Click the [ ] button to Cancel or the [ ] button to save.



**Object successfully changed!**

Object successfully changed

The object address was created successfully.

Here is a demonstration of how to create an IPv6 address object:

Create Addresses Object

X

\* Name

Server IPs - IPv6

\* Type

IPv6 Address

Unique

\* Address

Prefix

128

+

2001:db8::1

2001:db8::2

2001:db8::3

2001:db8::4

-

Description

Server IPs - IPv6

Cancel



Import Address

Save

Objects – Create Addresses Object - IPv6



**Attention:** Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- **Name:** Name of the object. Ex.: Server IPs - IPv6;
- **Type:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- **Unique** ☐: Determines whether the address will be unique or not, disabling the Prefix field;
- **Address:** The address of the type of connection object selected later. After entering an address, click [  ] to add it to the list or select it and click [  ] to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- **Prefix:** Defines the prefix of the IP address that will be added to the object. Ex: 128;
- **Description:** This field is intended for the object description. Ex.: Server IPs - IPv6.

Import Address



By clicking on the button [ ] and select the file to be imported, click [ ] to add the contents of the file inside the object, if



you want to remove any registered address, select the IP address and click the button [ ] and the content will be removed.



The supported format of the list is one IP or network address per line.

Ex.: 2001::FF:01/68

::FF:0A/128

2001:abcd:172.16.102.0/120

Cancel

Save

Click the [ ] button to Cancel or the [ ] button to save.



**Object successfully changed!**

Object successfully changed

The object address was created successfully.



# Objects - Example 3 - Creating Physical Address Object

Here is a demonstration of how to create a MAC Address object:

Create Addresses Object

\* Name

Mac Dev

\* Type

MACAddress

☐ Unique

\* Address

00:0B:AB:F1:9B:D4

00:0B:AB:F1:9B:D5

+

-

Description

Mac Dev

Cancel

Import Address

Save

Objects – Create Addresses Object - Mac Address

**Attention:** Once the Type field has been defined and after saving the object, it is not possible to change it during editing.

- **Name:** Object name. Ex.: Mac Dev;
- **Type:** Type of connection object, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address. After saving the object, it will no longer be possible to edit this field;
- **Unique**☐: Determines whether the address will be unique or not;
- **Address:** The address of the type of connection object selected later. After entering an address, click to add it to the list or select it and click to remove. After adding an address of the selected type, the Type field will be disabled, if you want to change the type, remove all addresses from the list;
- **Description:** This field is intended for the description of the object. Ex .: Mac Dev.

Import Address



By clicking on the [ ] button and select the file to be imported, click [ ] to add the contents of the file inside the object,



if you want to remove any registered address, select the IP address and click the button [ ] and the content will be removed.



The definition of the MAC address is made up of 48 bits and its format is completely specific, it has 12 hexadecimal digits, grouped two by two separated by colons.

Object syntax:

*00:01:02:AA:CC:FF*

Cancel

Save

Click on the [ ] button to Cancel or the [ ] button to save.



**Object successfully changed!**

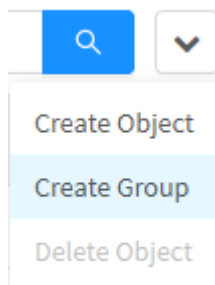
*Object successfully changed*

The object address was created successfully.

# Objects - Addresses - Actions Menu - Create Group

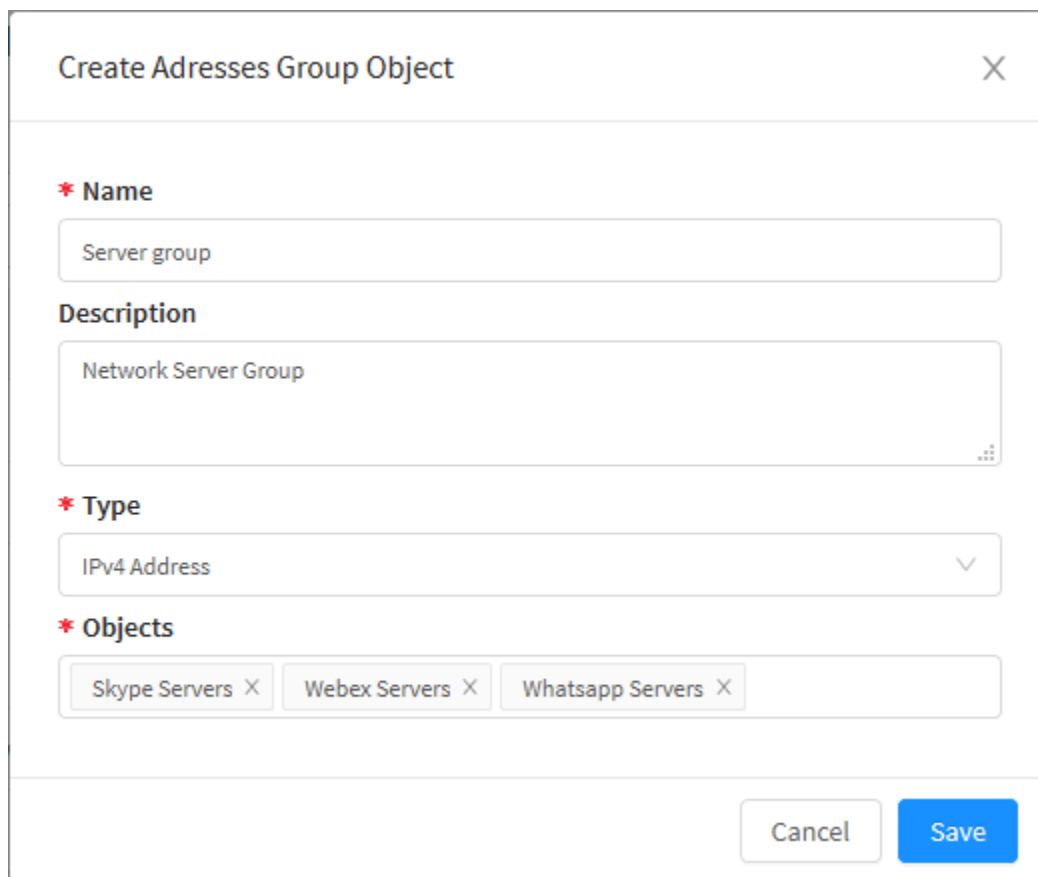
Through the button "Create Group" it is possible to create a new object group. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Group" option;



*Objects – Addresses – Create Group*

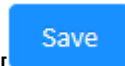
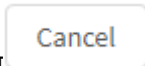
2. Fill in the information on the Create Addresses Group Object screen:

A screenshot of a web form titled 'Create Addresses Group Object'. The form has a close button (X) in the top right corner. It contains four main sections: 1. 'Name' with a red asterisk, followed by a text input field containing 'Server group'. 2. 'Description' with a text area containing 'Network Server Group'. 3. 'Type' with a red asterisk, followed by a dropdown menu showing 'IPv4 Address'. 4. 'Objects' with a red asterisk, followed by a container with three tags: 'Skype Servers', 'Webex Servers', and 'Whatsapp Servers', each with a close button (X). At the bottom right, there are 'Cancel' and 'Save' buttons.


*Objects – Create Addresses Group Object*

- **Name:** Object group name. Ex.: *Server group*;
- **Description:** This field is intended for the description of the group. Ex.: *Network Server Group*;
- **Type:** Connection object type, being able to choose between: IPv4 Address, IPv6 Address, MAC Address and FQDN Address;

- **Objects:** Allows you to select the objects that were previously added in [Objects - Addresses - Actions Menu - Create Object](#). The objects added in this field will be inserted as tags.



Click on the [ ] button to Cancel or click the [ ] button to save.

 **Settings successfully changed!**  
*Settings successfully changed*

The group was created successfully.

# Objects - Addresses - Actions Menu - Delete Object

Through the button "Delete Object" it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the **checkbox** [  ].Ex.: *Test*;

Objects

Addresses Services Times Schedules Dictionaries Contents

10 records

Name

Description

Type

Used

Actions

Class A network

Reserved network Class A 10.0.0.0/8

IPv4

-

Class B network

Reserved network Class B 172.16.0.0/12

IPv4

-

Class C network

Reserved network Class C 192.168.0.0/16

IPv4

-

Localhost

Loopback 127.0.0.1

IPv4

-

Private class network

Special-use address reserved to private network (...)

IPv4

-

Server group

Network Server Group

GROUP IP

-

Skype Servers

IPv4

-

Test

Test

IPv4

-

Webex Servers

IPv4

-

Whatsapp Servers


IPv4

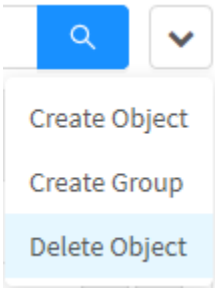
-

< 1 >

10 / page

Objects - Objects selected for deletion

2. Enter the **actions menu** [  ] and click on the "Delete Object" button.



Objects - Actions Menu - Delete Object

3. The message will appear if you really want to delete the selected groups or objects:

Confirm delete

Are you sure you want to delete the following objects address?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following objects address


If you want to cancel click on 

Cancel

 button. To finish, click on 

Delete

 button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.

Through the button "Delete Object" it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the **checkbox** ☐ .Ex.: *Test*,

Objects

Addresses

Services

Times

Schedules

Dictionaries

Contents

10 records

Name

Description

Type

Used

Actions

☐

Class A network

Reserved network Class A 10.0.0.0/8

IPv4

-

☐

Class B network

Reserved network Class B 172.16.0.0/12

IPv4

-

☐

Class C network

Reserved network Class C 192.168.0.0/16

IPv4

-

☐

Localhost

Loopback 127.0.0.1

IPv4

-

☐

Private class network

Special-use address reserved to private network (...)

IPv4

-

☐

Server group

Network Server Group

GROUP IP

-

☐

Skype Servers

IPv4

-

☒

Test

Test

IPv4

-

☐

Webex Servers

IPv4

-

☐

Whatsapp Servers

IPv4

-

<

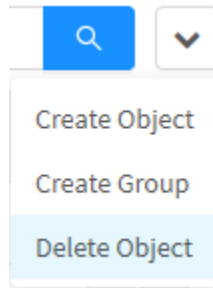
1

>

10 / page

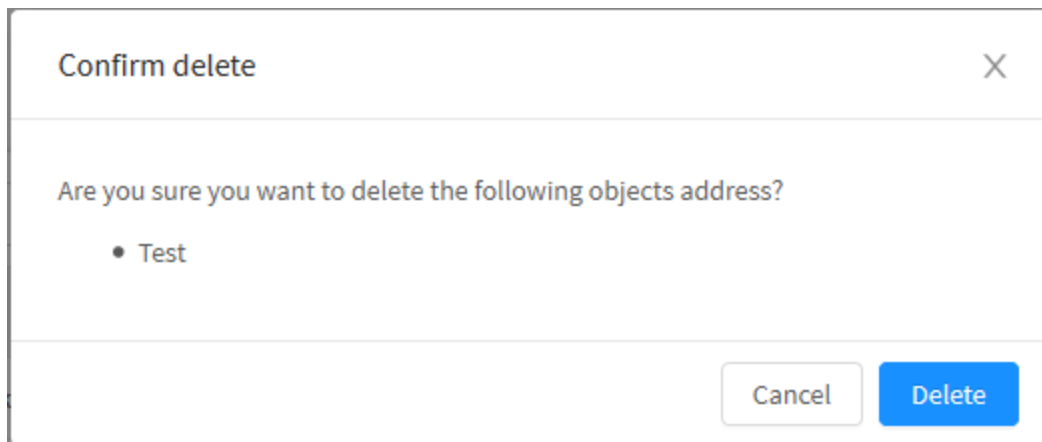
Objects - Objects selected for deletion

2. Enter the **actions menu** [  ] and click on the “Delete Object” button.



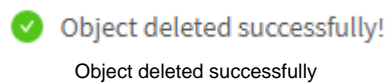
*Objects - Actions Menu - Delete Object*

3. The message will appear if you really want to delete the selected groups or objects:



*Objects - Are you sure you want to delete the following objects address*

If you want to cancel click on [  ] button. To finish, click on [  ] button.



After performing these procedures, the packages will have been successfully deleted.

# Objects - Addresses - Columns

In the “Addresses” tab, it is possible to view the actions menu and six columns:

Objects

Addresses

Services

Times

Schedules

Dictionaries

Contents

9 records





<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Class A network	Reserved network Class A 10.0.0.0/8	IPv4	1	<div><div></div><div></div></div>
<input type="checkbox"/>	Class B network	Reserved network Class B 172.16.0.0/12	IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Class C network	Reserved network Class C 192.168.0.0/16	IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Localhost	Loopback 127.0.0.1	IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Private class network	Special-use address reserved to private network (A...	IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Skype Servers		IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Teste endereço		IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Webex Servers		IPv4	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Whatsapp Servers		IPv4	-	<div><div></div><div></div></div>

< 1 >

10 / page

Objects – Addresses tab

Below we will explain each column of the Addresses tab:

- **Checkbox**: Select the desired objects;
- **Name**: Object Name;
- **Description**: Displays the object description;
- **Type**: Object Type;
- **Used**: Enumerates the number of times this object is being used. By clicking on this number the window [Object Mapping](#) is displayed.
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit**: Allows you to edit the settings of the Object added in the option [Create Object](#) from the actions menu;
  - **Deletar**: Allows you to remove the object.

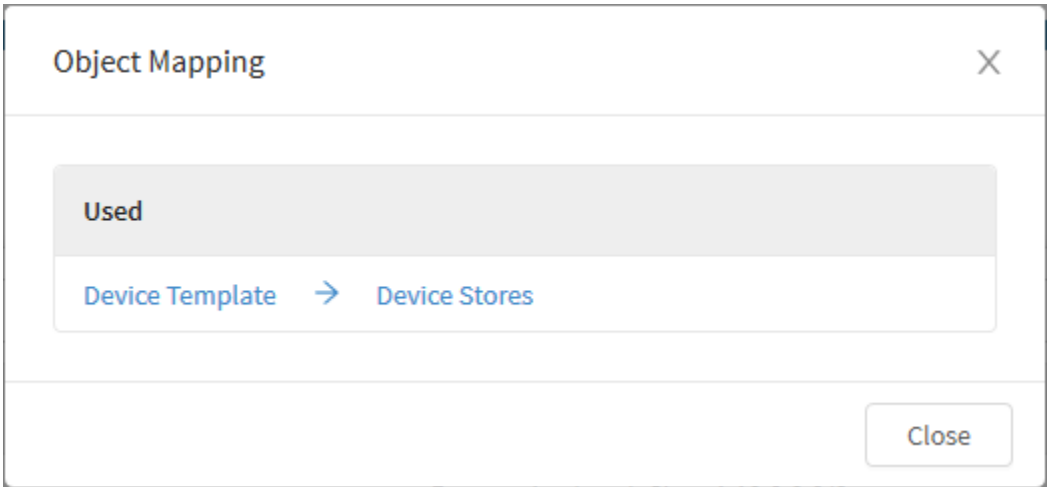


# Objects - Addresses - Object Mapping

By clicking on the icon of how many times an object was used [ 1 ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Objects - Services

On this screen we have the Services objects administrative panel, which comprises port and protocols.

In its initial configuration, by default, the system brings some pre-registered objects (ports / protocols), the objects referring to the most common protocols and services: Example: "DHCP", "DNS", "HTTP", "HTTPS".

All of these objects are available to be used in the configuration and enabling processes of the services. Service objects can be composed of a set of different protocols and services, it is also possible to create groups containing different service objects as a common resource to be applied to any Blockbit UTM functionality, eg: "Compliance policies", " Services", among others.

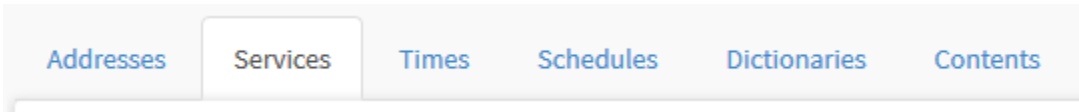
Services type objects identify protocols and applications based on their TCP, UDP, IP and ICMP ports.

To access the screen, select the "Objects" tab.



Objects button

Click on the "Services" tab.



Services tab

The "Services" screen will appear. It consists of the columns "Select", "Name", "Description", "Type", "Used" and "Actions". In addition, at the top of the screen is the [search bar](#) and the [action menu](#) on the right.

Objects

Addresses

Services

Times

Schedules

Dictionaries

Contents

51 records

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	AH		SERVICE	1	<div><div></div><div></div></div>
<input type="checkbox"/>	AOL		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	BGP		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	DHCP		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	DNS		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	ESP		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	FTP		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	GRE		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	H323		SERVICE	-	<div><div></div><div></div></div>
<input type="checkbox"/>	HTTP		SERVICE	-	<div><div></div><div></div></div>

< 1 2 3 4 5 6 >

10 / page

Objects – Services

We will explain in detail the [actions menu](#) and then the columns on the "Services" tab.

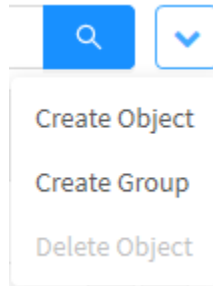
# Objects - Services - Actions Menu

At the top right of the screen we have the actions menu:



*Objects – Actions menu button*

By clicking on this button the menu below is displayed:



*Objects – Actions menu*

The menu consists of the following options:

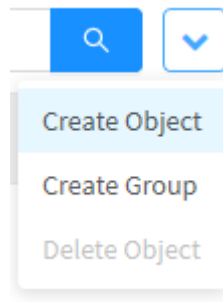
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

Next, each action menu option will be detailed.

# Objects - Services - Actions menu - Create Object

Through the option "Create Object" it is possible to configure the object according to the definitions of the policies that you want to apply for specific hosts. To create a new Object Services, follow the steps:

1. In the **actions menu** [  ], click on the option "Create Object";



Objects – Services – Create Object

2. The Create Service Objects screen will appear.

Create Services Object

X

\* Name

\* Protocol Type

TCP

▼

\* Port Type

Source/Destination

▼

Port

Source port

Destination port

+

▼

-

Description

Cancel

Save

Objects – Services – Create Service Objects

Here are some examples of how to create address objects:

- [Example 1 - Creating a service object;](#)
- [Example 2 - Creating VPN Client service object using MAC iOS.](#)

Below are some notes regarding the selection of the types of protocols in some fields of the form.

## Protocol Type

The administrator can select between the types of protocol to compose the object, this selection allows to determine different protocols and to group them in the same object:

### \* Protocol Type

TCP

TCP

UDP

IP

ICMP V4

ICMP V6

Objects – Services – Protocol Type

Here are the options for this checkbox:

- **TCP:** It is associated with ports and port ranges for the various services that run your applications under the TCP protocol. Ex .: "Vpn pptp (1723), http (80), https (443), dns (53)";
- **UDP:** It is associated with ports and port ranges referring to the various services that run their applications under the UDP protocol. Ex .: "Vpn ike-isakmp (500), Vpn l2tp (1701), Vpn Nat-t (4500), dns (53)";
- **IP:** It is associated with other IP layer protocols. Ex .: "ah, esp, gre, icmp, igmp, sctp, tcp and udp";
- **ICMP v4 and ICMP v6:** It is associated with types of treatment and / or expected response regarding the traffic of the ICMP v4 or ICMP v6 protocol. Ex .: "Echo Request", "Echo Replay", "Destination unreachable", "time exceeded".

## Port Type

The administrator can select between 2 (two) types of ports (services) that will compose the object.

### \* Port Type

Source/Destination

Source/Destination

Range

Objects – Services – Port Type

Here are the options for this checkbox:

- **Source/Destination:** Definition of the [Source port] / [Destination port] fields, referring to services that normally follow RFC's standards and perform the service on a specific port (Destination port), usually on services that run under the TCP protocol. Ex. "HTTP (80); HTTPS (443), DNS (53)". There are cases of services that also run under the UDP protocol. Ex.: "DNS (53)";
- **Range:** Definition of the ports or services that normally run within a class of ports [Initial port] / [End port], usually in services that run under the UDP protocol. Services that normally run in port ranges. Eg: "VOIP - initial port 4500 / UDP; final port 5500 / UDP .; Cameras - initial port 10000 / UDP; final port 20000 / UDP".



The **[Source port]** field is an optional field. It is usually executed under a random high [1024: 65535] port executes at the start of the service.



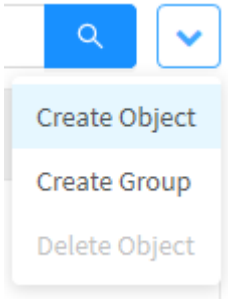
The range of ports even for applications of the same type may vary according to the specification of each application.



# Objects - Example 1 - Creating a service object

Through the option "Create Object" it is possible to create a new Object Services. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;



Objects – Services – Create Object

2. The Create Service Objects screen will appear. Fill in the fields:

Create Services Object

\*

Name

Protocol TCP/UDP

\*

Protocol Type

IP

\*

Protocol

tcp

ip/udp

ip/tcp

+

-



Description

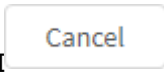

Protocol TCP/UDP


Cancel

Save

## Service Objects – Create Service Objects

- **Name:** Name of the object. Ex: HTTP;
- **Protocol Type:** Select the object's protocol, among the options: "TCP", "UDP", "IP" and "ICMP". Ex .: TCP;
- **Port Type:** Determines whether the port type will be of origin / destination or within an IP range. If you selected the range option, you will need to determine the range in the following text fields;
- **Port:** Determines the source and destination port of the addresses, to be added to the list of service objects;
- **List:** Lists the added ports. To delete any value entered, select it and click the button [  ], otherwise click on the button [  ] to make an addition to the list;
- **Description:** Description of the object. Eg HTTP Protocol.

Click on the button [  ] button To cancel. Click on the [  ] button to save.

 **Object successfully changed!**  
*Object successfully changed*

The service object was created successfully.

# Objects - Example 2 - Creating VPN Client service object using MAC iOS

Let's exemplify the registration of a Service object for VPN Client application using MAC iOS. Eg: "iOS X Server VPN - Ports 500 / UDP; 1701 / UDP; 4500 / UDP; 1723 / TCP".

Create Services Object

\* Name

VPN iOS X SERVER

\* Protocol Type

TCP

\* Port Type

Source/Destination

Port

Source port

Destination port

+

tcp/1723 Destination

udp/500 Destination

udp/1701 Destination

udp/4500 Destination

-

Description


VPN iOS X SERVER






Cancel

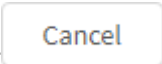
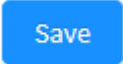
Save


Object Service - VPN iOS X Server

- **Name:** Name of the object. Ex.: iOS iOS X SERVER VPN;
- **Protocol Type:** Select the object's protocol, among the options: "TCP", "UDP", "IP" and "ICMP". In this example we will use the TCP and UDP protocol;
- **Port Type:** Determines whether the port type will be of origin / destination or within an IP range. If you selected the range option, you will need to determine the range in the following text fields. In this example, only the "Source / Destination" option will be used;
- **Port:** Determines the source and destination port of the addresses, to be added to the list of service objects. In this example we will specifically use the destination ports, as shown in the image, add:

- **Protocol Type:** TCP; **Destination Port:** 1723 and click on[  ] to add the value to the list;

- **Protocol Type:** UDP; **Destination Port:** 500 and click on[  ] to add the value to the list;
- **Protocol Type:** UDP; **Destination Port:** 1701 and click on[  ] to add the value to the list;
- **Protocol Type:** UDP; **Destination Port:** 4500 and click on[  ] to add the value to the list.
- **List:** Lists the added ports. To delete any value entered, select it and click the [  ] button, otherwise click on the [  ] button to make an addition to the list. After the previous step, we should have 4 inserts already listed, as shown in the image;
- **Description:** Description of the object. Ex .: VPN iOS X SERVER.

Click the [  ] button to cancel. Click on the [  ] button to save.

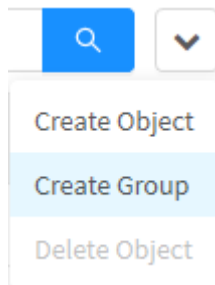
 **Object successfully changed!**  
*Object successfully changed*

The service object was created successfully.

# Objects - Services - Actions Menu - Create Group

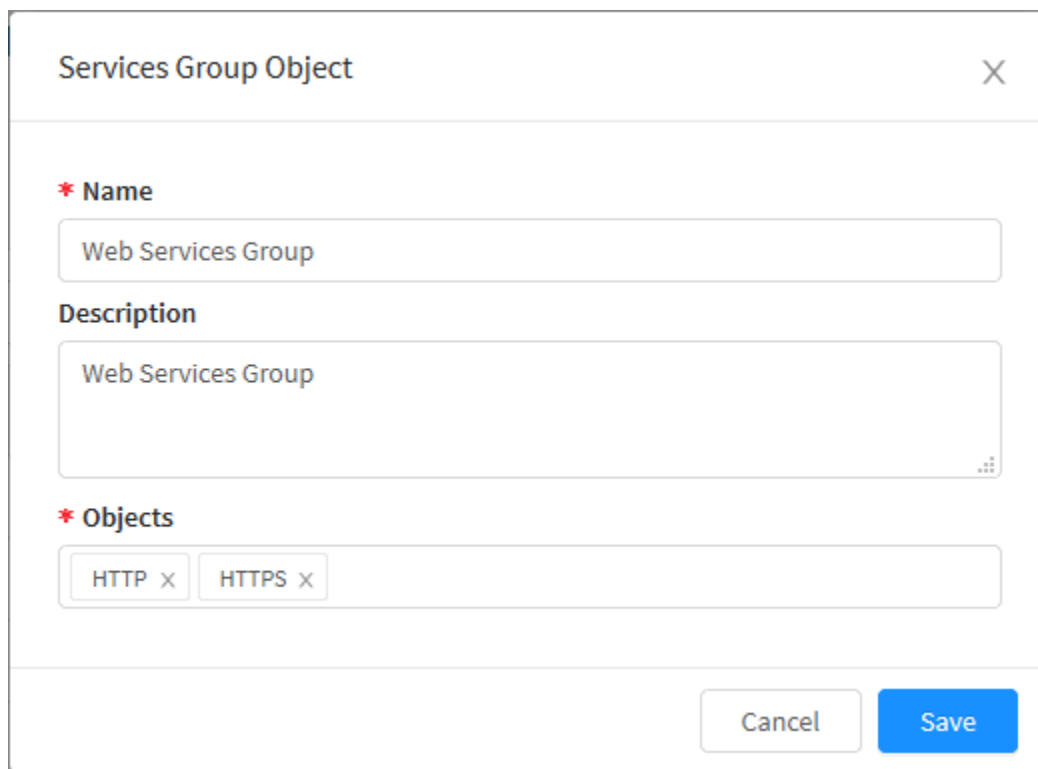
Through the button "Create Group" it is possible to create a new object group. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Group" option;



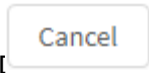
*Objects – Services – Create Group*

2. Fill in the information on the Services Group Object screen:

A screenshot of a web form titled 'Services Group Object' with a close button (X) in the top right corner. The form has three main sections. The first section is labeled '\* Name' and contains a text input field with the value 'Web Services Group'. The second section is labeled 'Description' and contains a larger text area with the value 'Web Services Group'. The third section is labeled '\* Objects' and contains a container with two tags: 'HTTP' and 'HTTPS', each with a small 'x' icon to its right. At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

*Objects – Services Group Object*

- **Name:** Name of the object group. Ex.: Web Services group;
- **Description:** This field is intended for the description of the group. Ex .: Web Services Group;
- **Objects:** Allows you to select the objects that were previously added in [Objects - Addresses - Actions Menu - Create Object](#). *The objects added in this field will be inserted as tags.*



Click on the [ ] button to Cancel or click on [ ] button to save.



Settings successfully changed!

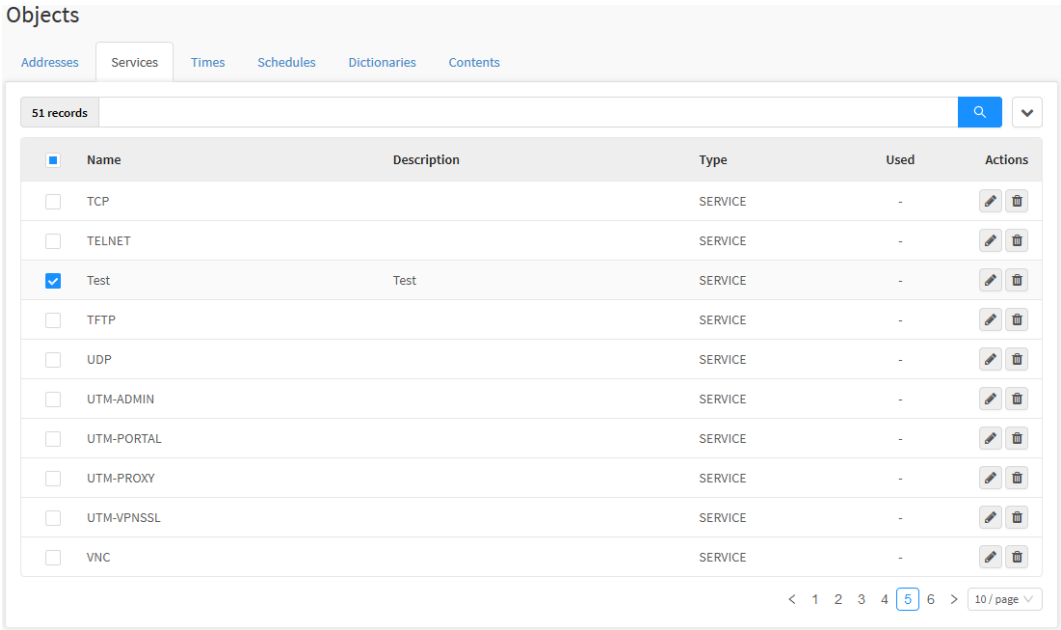
*Settings successfully changed*

The group was created successfully.

# Objects - Services - Actions menu - Delete Object

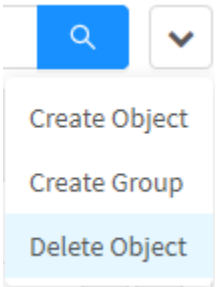
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking the **checkbox** ☐. Ex.: Test;



Objects - Objects selected for deletion

2. Enter the **actions menu**  and click on the “Delete Object” button.



Objects - Actions menu - Delete Object

3. The message will appear if you really want to delete the selected groups or objects:

Confirm delete

X


Are you sure you want to delete the object service Test?

Cancel

Delete

Objects - Are you sure you want to delete the object service?

If you want to cancel click on [  ] button. To finish, click on [  ] button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.



# Objects - Services - Columns

In the "Services" tab, you can view the actions menu and six columns:

Objects

Addresses Services Times Schedules Dictionaries Contents

51 records

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	AH		SERVICE	1	
<input type="checkbox"/>	AOL		SERVICE	-	
<input type="checkbox"/>	BGP		SERVICE	-	
<input type="checkbox"/>	DHCP		SERVICE	-	
<input type="checkbox"/>	DNS		SERVICE	-	
<input type="checkbox"/>	ESP		SERVICE	-	
<input type="checkbox"/>	FTP		SERVICE	-	
<input type="checkbox"/>	GRE		SERVICE	-	
<input type="checkbox"/>	H323		SERVICE	-	
<input type="checkbox"/>	HTTP		SERVICE	-	

< 1 2 3 4 5 6 > 10 / page

Objects – Services tab

Below we will explain each column of the Services tab:

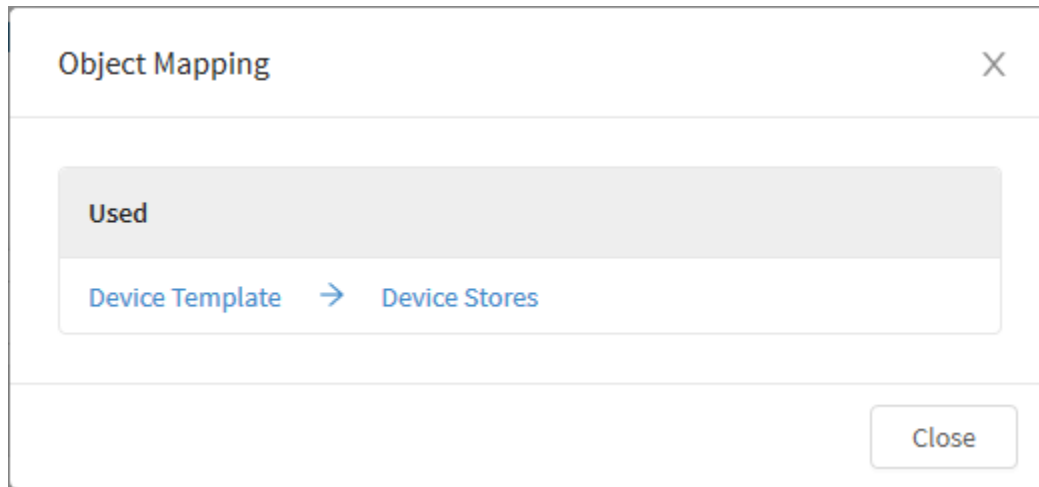
- **Checkbox**: Select the desired objects;
- **Name**: Object Name;
- **Description**: The object description;
- **Type**: Object Type;
- **Used**: Enumerates the number of times this object is being used. By clicking on this number, the [Object Mapping](#) window is displayed;
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit**: Allows you to edit the settings of the Object added in the [Create Object](#) option of the action menu;
  - **Delete**: Allows you to remove the object.

# Objects - Services - Object Mapping

By clicking on the icon of how many times an object was used [ 1 ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



*Object Mapping*

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Objects - Times

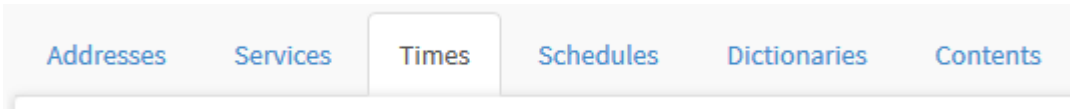
Times objects are made up of the “days of the week” and the “start and end time”. Ex .: “Business Hours - start: Monday from 8:00 AM until Friday at 6:00 PM.

To access the screen, simply select the “Objects” button.



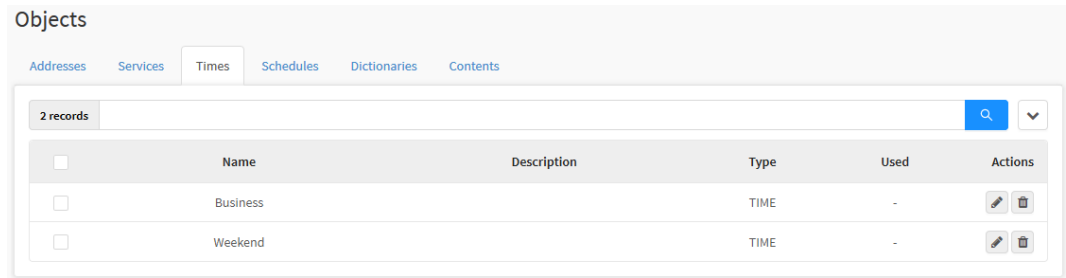
Botão “Objects”

Click on the "Times" tab.



"Times" Tab

The "Times" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the [search bar](#) and the [actions menu](#) on the right.



Objects - Times

We will explain in detail the [actions menu](#) and later the [columns](#) of the "Times" tab.

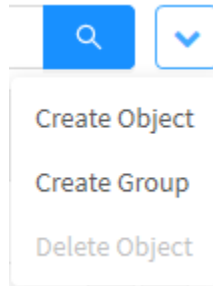
# Objects - Times - Actions Menu

At the top right of the screen we have the actions menu:



Objects - Actions menu button

By clicking on this button the menu below is displayed:



Objects - Actions menu

The menu consists of the following options:

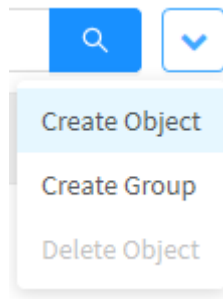
- [Create Object](#);
- [Create Group](#);
- [Delete Object](#).

Next, each action menu option will be detailed.

# Objects - Times - Actions Menu - Create Object

Through the option "Create Object" it is possible to create a new Time object. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;



Objects – Times – Create Object

2. The Create Times Objects screen will appear. Fill in the fields:

Create Times Object

\*

Name

Working hours

\*

Weekday

Monday X Tuesday X Wednesday X Thursday X Friday X

Start / End time

Select time

Select time

+

08:00-23:59

^

-

Description



Business Day/hours

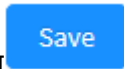
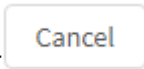
Cancel

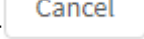
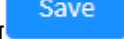
Save

## Service Objects – Create Times Object

- **Name:** Object name. Ex.: Working hours;
- **Weekday:** Allows you to select the days of the week. Ex.: "Monday", "Tuesday", "Wednesday", "Thursday" and "Friday";
- **Start / End time:** Defines the object's time periods. The end time cannot be earlier than the start time and vice versa. Ex.: "08:00 – 23:59";

- **List:** Lists the times added. To delete any value entered, select it and click the [  ] button, otherwise click the [  ] button to make an addition to the list;
- **Description:** Object description. Ex.: HTTP Protocol.



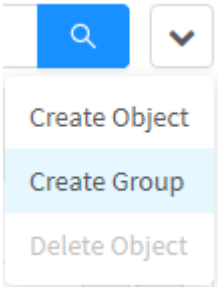
Click the [  ] button to cancel. Click the [  ] button to save.

The object time was created successfully.

# Objects - Times - Actions Menu - Create Group

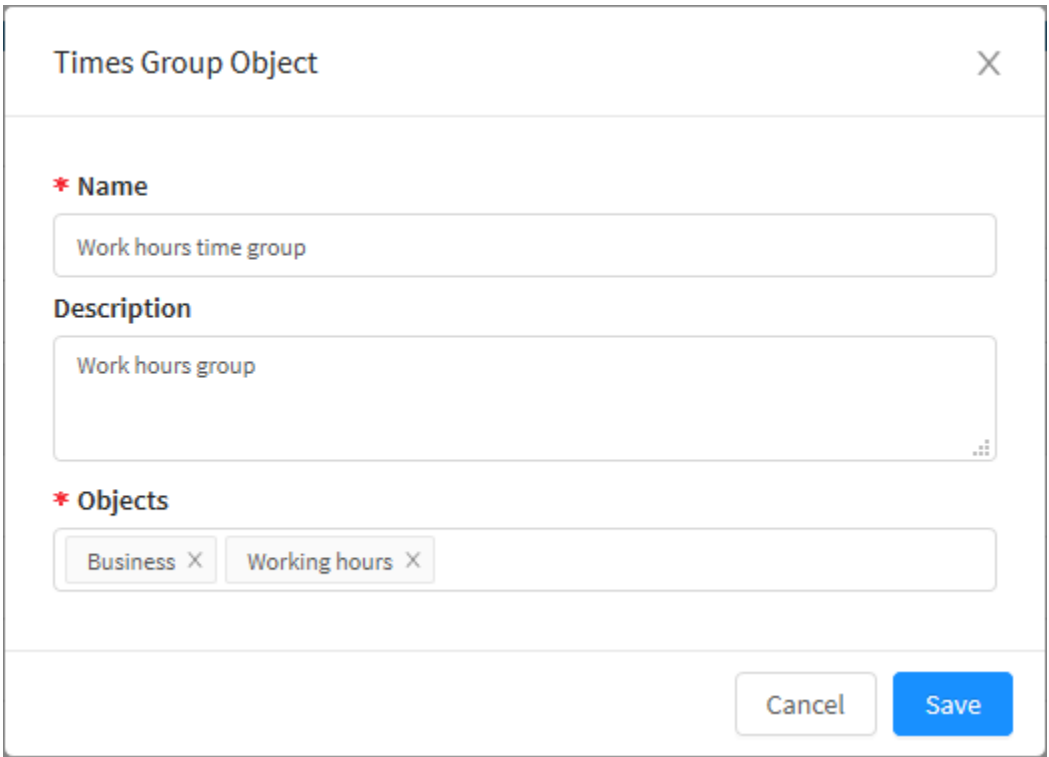
Through the button "Create Group" it is possible to create a new object group. To access, follow the steps:

1. In the **actions menu** [  ], click on the option "Create Group";



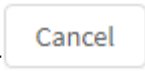
Objects – Times – Create Group

2. Fill in the information on the Times Group Object screen:

A screenshot of a form titled 'Times Group Object' with a close button (X) in the top right corner. The form contains three main sections: 1. 'Name' with a red asterisk, followed by a text input field containing 'Work hours time group'. 2. 'Description' with a text area containing 'Work hours group'. 3. 'Objects' with a red asterisk, followed by a container showing two selected items: 'Business' and 'Working hours', each with a close button (X). At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Objects – Times Group Object

- **Name:** Object group name. Ex.: Work hours time group;
- **Description:** This field is intended for the description of the group. Ex.: Work hours group;
- **Objects:** Allows you to select the objects that were previously added in [Objects - Times - Actions Menu - Create Object](#). The objects added in this field will be inserted as tags.



Click the [ ] button to Cancel or the [ ] button to save.



Saved successfully

Saved successfully

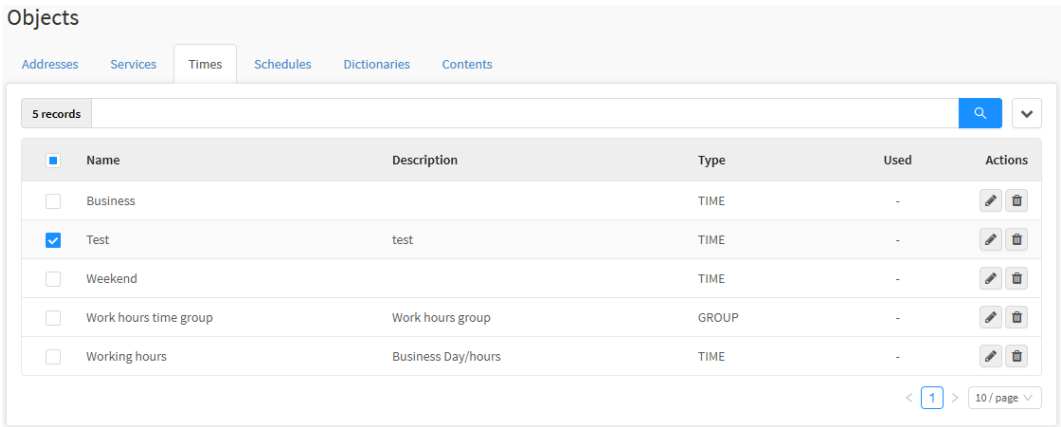
The group was created successfully.



# Objects - Times - Actions Menu - Delete Object

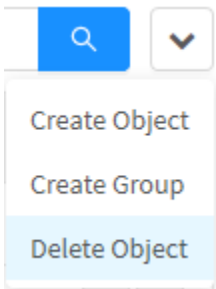
Through the button "Delete Object" it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

- 1. Select which package (s) you want to delete by clicking the **checkbox**[ ☐ ]. Ex.: Test;



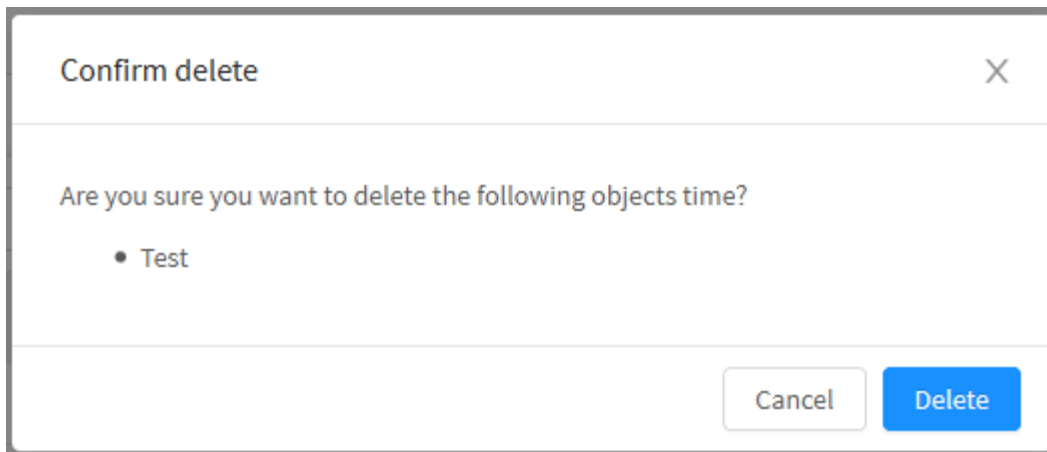
Objects - Objects selected for deletion

- 2. Enter the **actions menu** [  ] and click on the "Delete Object" button.


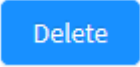



Objects - Actions Menu - Delete Object

- 3. The message will appear if you really want to delete the selected groups or objects:



Objects - Are you sure you want to delete the following object time?

If you want to cancel, click the button [  ]. To finish, click the [  ] button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.

# Objects - Times - Columns

In the "Times" tab it is possible to view the actions menu and six columns:

Objects

Addresses Services Times Schedules Dictionaries Contents

2 records

	Name	Description	Type	Used	Actions
<div></div>	Business		TIME	-	<div><div></div><div></div></div>
<div></div>	Weekend		TIME	-	<div><div></div><div></div></div>

Objects - Times Tab

Below we will explain each column of the Times tab:

- **Select**: Select the desired objects;
- **Name**: Object Name;
- **Description**: The object description;
- **Type**: Object Type;
- **Used**

1

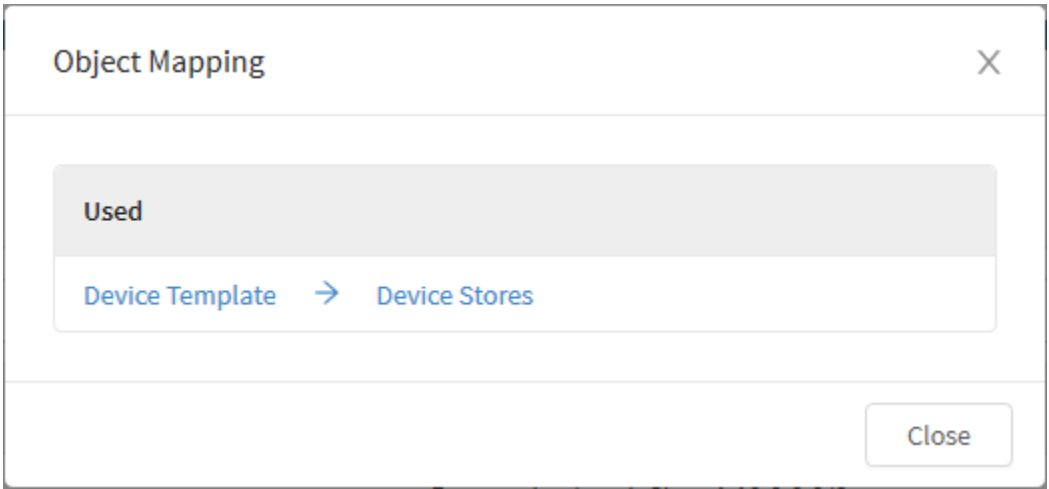
: Enumerates the number of times this object is being used. By clicking on this number, the [Object Mapping](#) window is displayed;
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit**: Allows you to edit the Object settings added in the [Create Object](#) option of the action menu;
  - **Deletar**: Allows you to remove the object.

# Objects - Times - Object Mapping

By clicking on the icon of how many times an object has been used [ 1 ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Objects - Schedules

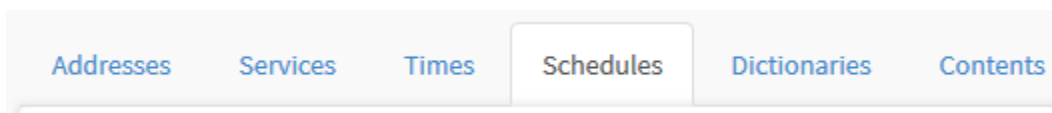
Schedules objects are made up of the definitions of a period that competes "Start date / time" and "End date / time". Ex .: 2017-05-11 8:00 AM until 2017-05-30 5:00 PM.

To access the screen, simply select the "Objects" button.



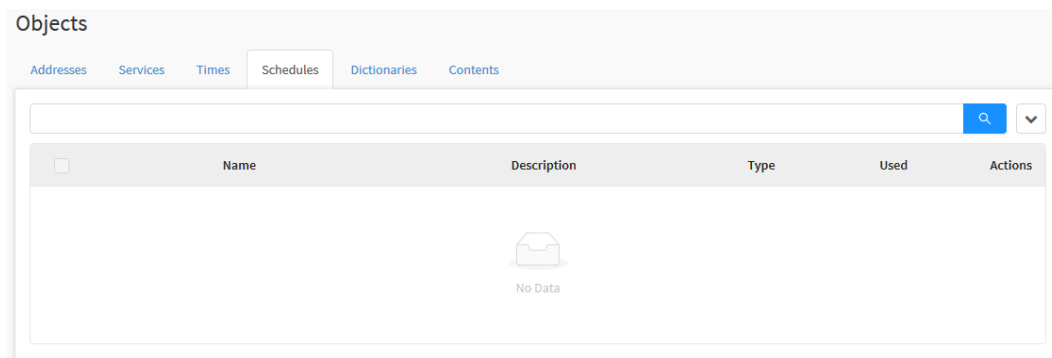
"Objects" button

Click on the "Schedules" tab.



Schedules tab

The "Schedules" screen will appear. It consists of the columns "Select", "Name", "Description", "Type", "Used" and "Actions". In addition, at the top of the screen is the [search bar](#) and the actions menu on the right.



*Objects - Schedules*

We will explain in detail the actions menu and later the columns of the "Schedules" tab.

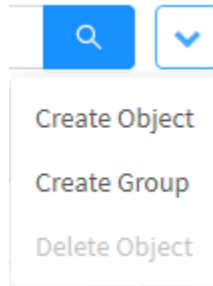
# Objects - Schedules - Actions Menu

At the top right of the screen we have the actions menu:



Objects - Actions menu button

By clicking on this button the menu below is displayed:



Objects - Actions menu

The menu consists of the following options:

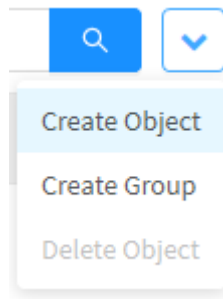
- Create Object;
- Create Group;
- Delete Object.

Next, each action menu option will be detailed.

# Objects - Schedules - Actions menu - Create Object

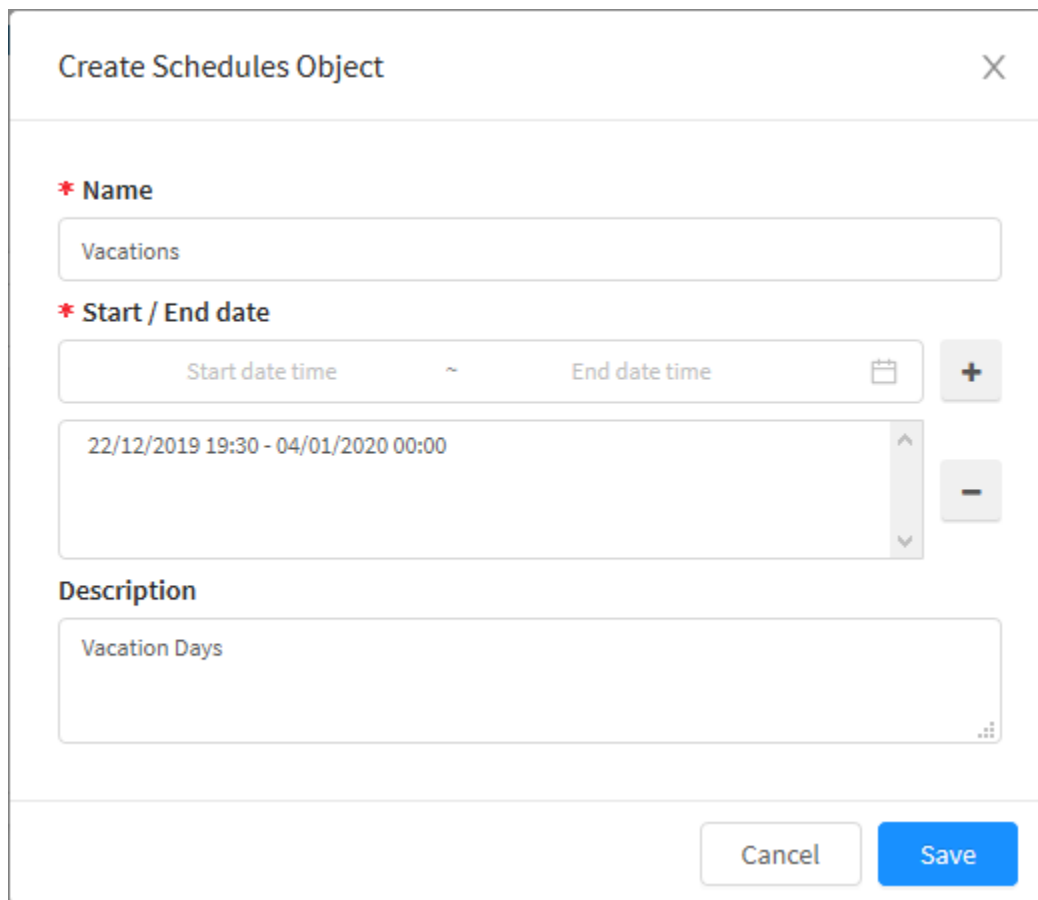
Through the option "Create Object" it is possible to create a new object Schedules. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;





*Objects – Schedules – Create Object*



2. The Create Schedule Objects screen will appear. Fill in the fields:

A screenshot of a web form titled 'Create Schedules Object'. The form has a close button (X) in the top right corner. It contains three main sections: 1. 'Name' with a red asterisk, a text input field containing 'Vacations', and a clear button (X). 2. 'Start / End date' with a red asterisk, two input fields for 'Start date time' and 'End date time' separated by a tilde (~), a calendar icon, and a plus (+) button. Below these is a text area containing '22/12/2019 19:30 - 04/01/2020 00:00' with up and down arrow buttons and a minus (-) button. 3. 'Description' with a text area containing 'Vacation Days' and a clear button (X). At the bottom right are 'Cancel' and 'Save' buttons.

*Schedules Objects – Create Schedules Object*

- **Name:** Name of the object. Ex.: *Vacations*;

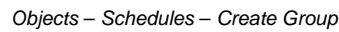
- **Start / End date:** Defines the period between the start date and time and the end date and time, to add click [  ]. Ex.: 22/12/2019 19:30 - 04 /01/2020 00:00;
- **List:** Displays the list of added periods. To delete any value entered, select it and click the button [  ];
- **Description:** Object description. Ex.: *Vacation Days*.

Click the [  ] button to Cancel. Click the [  ] button to save.

The schedule object was created successfully.

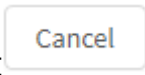


Through the button “Create Group” it is possible to create a new object group. To access, follow the steps:



## Objects – Schedules Group Object

- 421



Click the [ ] button to Cancel or the [ ] button to save.



**Saved successfully**

*Saved successfully*

The group was created successfully.

# Objects - Schedules - Actions Menu - Delete Object













Through the button "Delete Object" it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking on the **checkbox** .Ex.: *Test*;

Objects


Addresses Services Times Schedules Dictionaries Contents

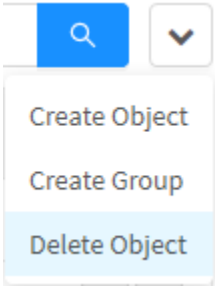
5 records

<input checked="" type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Director Visit - John	Director Visit	DATE		 
<input type="checkbox"/>	External Consultant	External Consultant	DATE		 
<input type="checkbox"/>	External visits	All external visits	GROUP	-	 
<input checked="" type="checkbox"/>	Test	Test	DATE	-	 
<input type="checkbox"/>	Vacations	Vacation Days	DATE	-	 

< 1 > 10 / page

Objects - Objects selected for deletion

2. Enter the **action menu**  and click on the "Delete Object" button.



Objects - Actions menu - Delete Object

3. The message will appear if you really want to delete the selected groups or objects:

Confirm delete

×

Are you sure you want to delete the following objects schedules?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following object schedules?


If you want to cancel, click the [ 

Cancel

 ] button. To finish, click the [ 

Delete

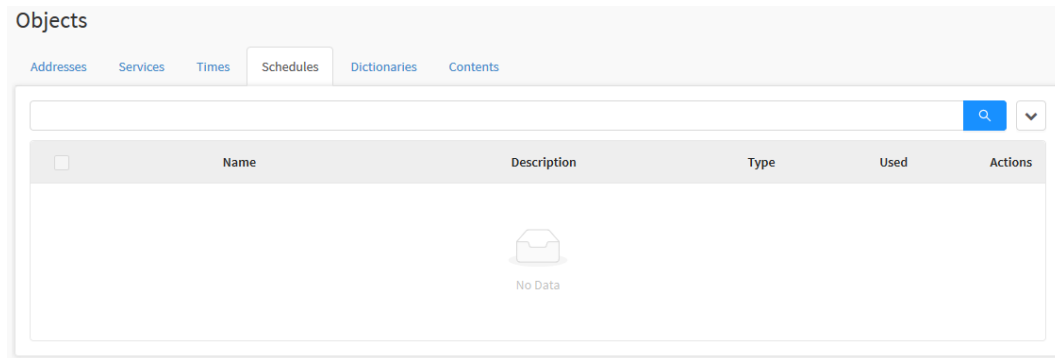
 ] button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.





# Objects - Schedules - Columns

In the “Schedules” tab, it is possible to view the actions menu and six columns:



*Objects – Schedules tabs*

Below we will explain each column of the Schedules tab:

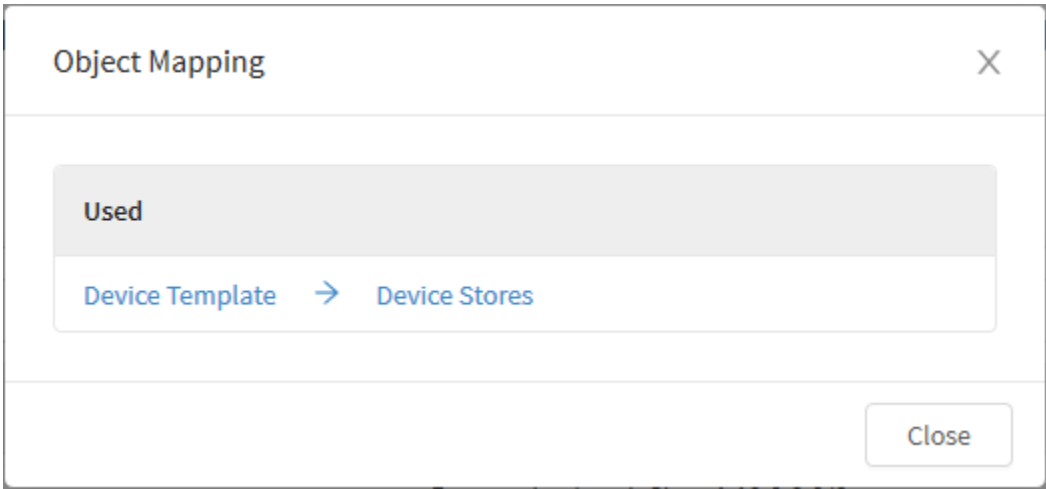
- **Select** : Select the desired objects;
- **Name**: Displays the name of the Object;
- **Description**: Displays the object description;
- **Type**: Displays the object Type;
- **Used** : Enumerates the number of times this object is being used. By clicking on this number, the Object Mapping window is displayed.
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit** : Allows you to edit the Object settings added in the Create Object option of the action menu;
  - **Delete** : Allows you to remove the object.

# Objects - Schedules - Object Mapping

By clicking on the icon of how many times an object has been used [ 1 ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



Object Mapping

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Objects - Dictionaries

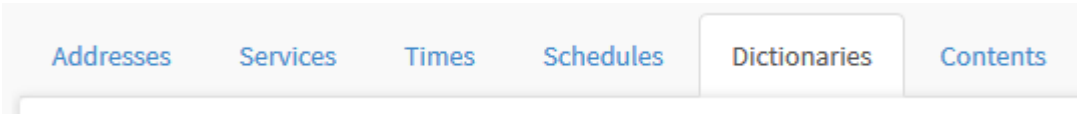
Dictionaries-type objects are made up of “word lists” or a set of “regular expression” combinations. Eg: "Alphanumeric", "E-mail address", "HTML link", "URL", etc.

To access the screen, simply select the “Objects” button.



“Objects” button

Click on the "Dictionaries" tab.



Dictionaries Tab

The "Dictionaries" screen will appear. It consists of the columns “Select”, “Name”, “Description”, "Type", "Used" and "Actions". In addition, at the top of the screen is the [search bar](#) and the action menu on the right.

Objects

AddressesServicesTimesSchedulesDictionariesContents

7 records

Search icon

Dropdown arrow

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Alphanumeric	Regular expression to match alphanumeric (letters...	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Credit Card	Regular expression to match credit card numbers	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Email Address	Regular expression to match a email address	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	IP Address	Regular expression to match a IP address	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Link HTML	Regular expression to match HTML links (a href)	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	URL	Regular expression to match FTP and HTTP URLs	DICTIONARY	-	<div><div></div><div></div></div>
<input type="checkbox"/>	URL Image	Regular expression to match image URLs	DICTIONARY	-	<div><div></div><div></div></div>

Objects – Dictionaries

We will explain in detail the action menu and then the columns of the "Dictionaries" tab.

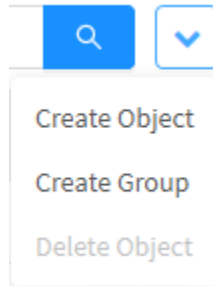
# Objects - Dictionaries - Actions Menu

At the top right of the screen we have the actions menu:



Objects - Actions menu button

By clicking on this button the menu below is displayed:



Objects - Actions menu

The menu consists of the following options:

- Create Object;
- Create Group;
- Delete Object.

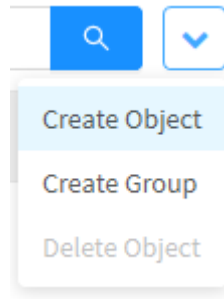
Next, each actions menu option will be detailed.



# Objects - Dictionaries - Menu de ações - Create Object

Through the option "Create Object" it is possible to create a new object Dictionaries. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;



*Objects – Dictionaries – Create Object*

2. The Create Dictionaries Objects screen will appear. Fill in the fields:

Create Dictionaries Object

X

\* Name

Alphanumeric

Expressions

.

\.

^

\$

+

\* Word

+

List

[a-zA-Z\s0-9]+

-

Description





Regular expression to match alphanumeric.

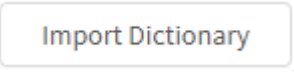
Cancel

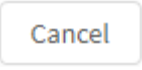

Import Dictionary

Save

Objects – Create Dictionaries Object

- **Name:** Displays the Object Name. Ex.: *Alphanumeric*;
- **Expressions:** Refers to the list of "regex", which we can combine to build a regular expression and add to the list of keywords. Select the code  and click [  ] to add it to the Word field;
- **Word:** This field defines the regular expression to identify the desired item. To add click [  ]. Eg: [a-zA-Z \s0-9] +;
- **List Extensions:** Displays the list of regular expressions. To delete any value entered, select it and click the button [  ];
- **Description:** Object description. Ex.: *Regular expression to match alphanumeric*.

If you prefer to import a list of regular expressions, click the [  ] button, the file must contain one item per line.

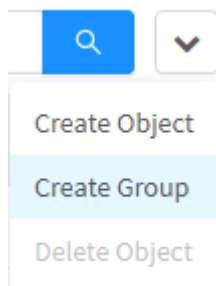
Click the [  ] button to Cancel or click the [  ] button to Save.

The dictionaries object was created successfully.

# Objects - Dictionaries - Menu de ações - Create Group

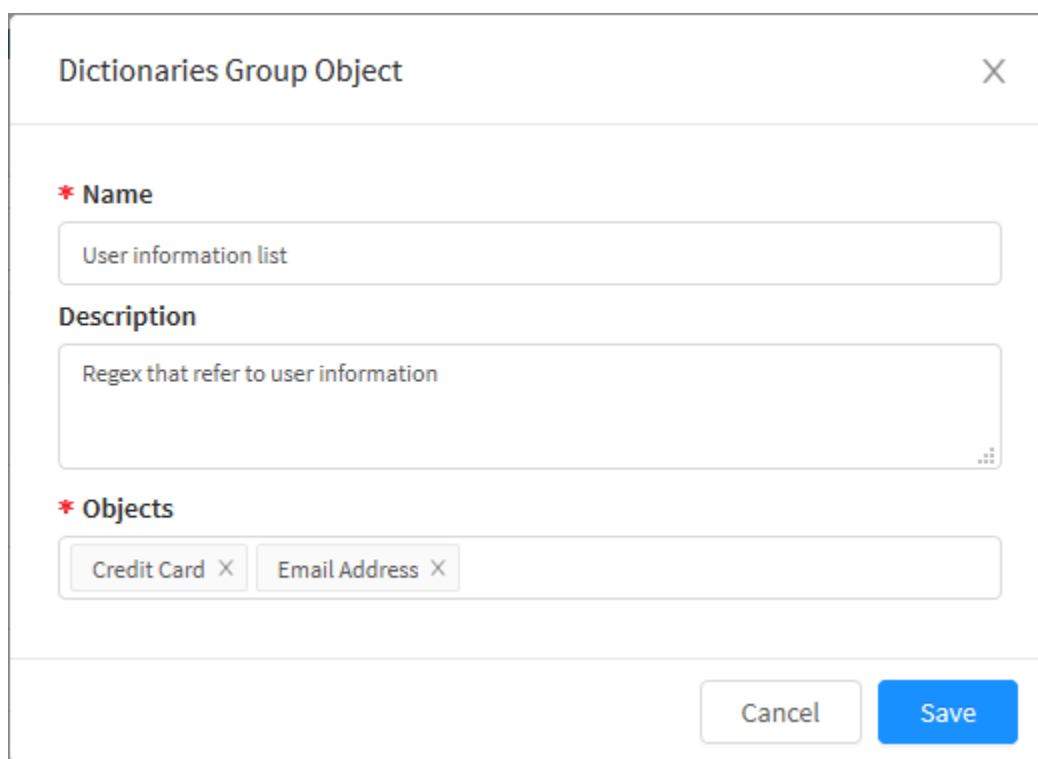
Through the button "Create Group" it is possible to create a new object group. To access, follow the steps:

1. In the **actions menu** [  ], click on the option "Create Group";



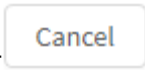
Objects – Dictionaries – Create Group

2. Fill in the information for the Dictionaries Group Object screen:

A screenshot of a web form titled 'Dictionaries Group Object' with a close button (X) in the top right corner. The form contains three main sections: 1. 'Name' with a red asterisk, followed by a text input field containing 'User information list'. 2. 'Description', followed by a larger text area containing 'Regex that refer to user information'. 3. 'Objects' with a red asterisk, followed by a container showing two tags: 'Credit Card' and 'Email Address', each with a small 'X' to remove it. At the bottom right of the form are two buttons: 'Cancel' and 'Save'.

Objects – Dictionaries Group Object

- **Name:** Displays the object group name. Ex.: *Dictionaries Group Object*;
- **Description:** This field is intended for the description of the group. Ex.: *Regex that refer to user information*;
- **Objects:** Allows you to select the objects that were previously added in [Objects - Dictionaries - Menu de ações - Create Object](#). The objects added in this field will be inserted as tags.



Click the [ ] button to Cancel or the [ ] button to save



Saved successfully

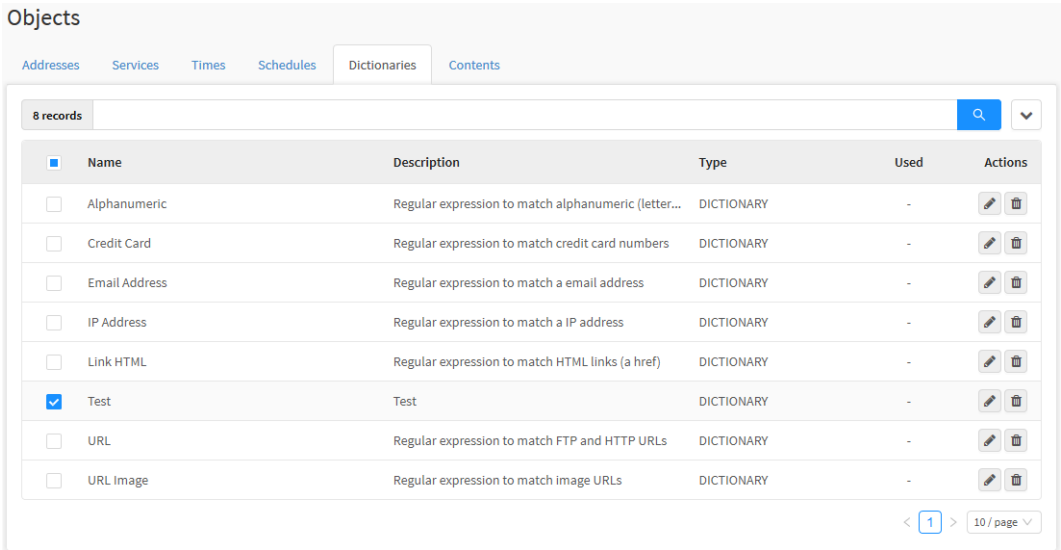
*Saved successfully*

The group was created successfully.


# Objects - Dictionaries - Actions Menu - Delete Object

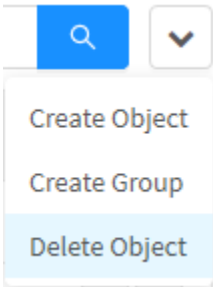
Through the button “Delete Object” it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking the **checkbox**[ ☐ ].Ex.: *Test*;



Objects - Objects selected for deletion

2. Enter the **actions menu** [  ] and click on the “Delete Object” button



Objects - Actions menu - Delete Object

3. The following message will appear:

Confirm delete

X

Are you sure you want to delete the following objects dictionaries?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following object dictionaries?


If you want to cancel click on the [ 

Cancel

 ] button. To finish, click the button [ 

Delete

 ] button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.















# Objects - Dictionaries - Columns

In the “Dictionaries” tab it is possible to view the actions menu and six columns:

Objects





Addresses Services Times Schedules Dictionaries Contents

7 records

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	Alphanumeric	Regular expression to match alphanumeric (letters...	DICTIONARY	-	 
<input type="checkbox"/>	Credit Card	Regular expression to match credit card numbers	DICTIONARY	-	 
<input type="checkbox"/>	Email Address	Regular expression to match a email address	DICTIONARY	-	 
<input type="checkbox"/>	IP Address	Regular expression to match a IP address	DICTIONARY	-	 
<input type="checkbox"/>	Link HTML	Regular expression to match HTML links (a href)	DICTIONARY	-	 
<input type="checkbox"/>	URL	Regular expression to match FTP and HTTP URLs	DICTIONARY	-	 
<input type="checkbox"/>	URL Image	Regular expression to match image URLs	DICTIONARY	-	 

Objects - Dictionaries Tab

Below we will explain each column of the Dictionaries tab:

- **Select** : Select the desired objects;
- **Name**: Displays the object Name;
- **Description**: Displays the object description;
- **Type**: Displays the object type;
- **Used** : Enumerates the number of times this object is being used. By clicking on this number, the Object Mapping window is displayed.
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit** : Allows you to edit the Object settings added in the Create Object option of the action menu;
  - **Delete** : Allows you to remove the object.

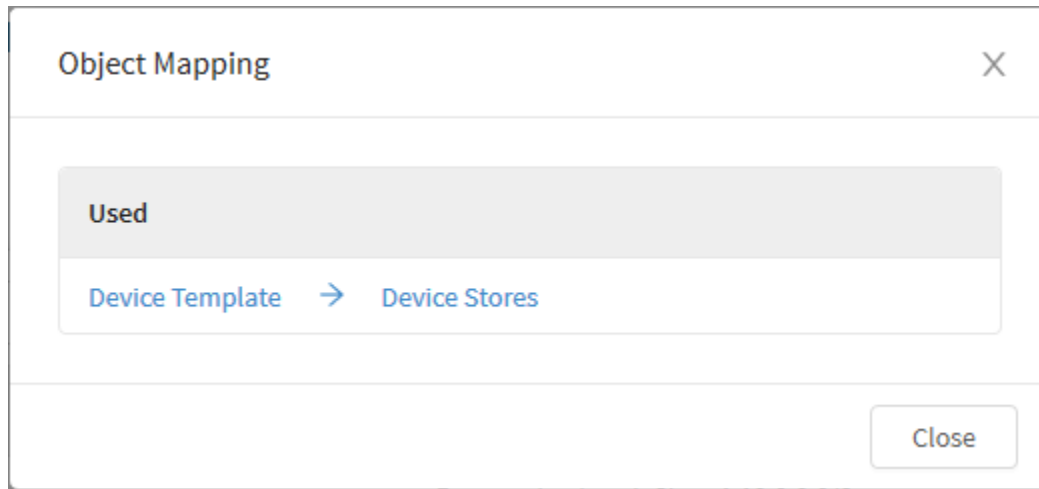


# Objects - Dictionaries - Object Mapping

By clicking on the icon of how many times an object has been used [ <sup>1</sup> ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



*Object Mapping*

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Objects - Contents

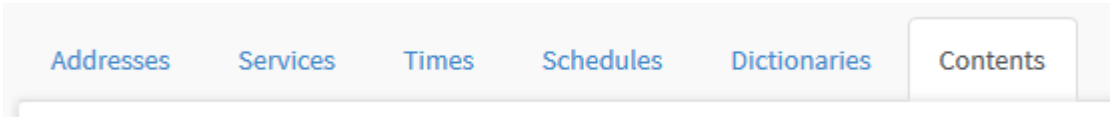
Contents objects are composed of groupings of application types based on the type of content that specify their characteristic. Eg: "ActiveX", "Compressed", "Executables", "Images", "Javascript", "Multimedia" and "Office".

To access the screen, simply select the "Objects" button.



"Objects" button

Click on the "Contents" tab.



Objects – Contents

The "Contents" screen will appear. It consists of the columns "Select", "Name", "Description", "Type", "Used" and "Actions". In addition, at the top of the screen is the search bar and the action menu on the right.

Objects

Addresses Services Times Schedules Dictionaries Contents

7 records

Search icon

Dropdown arrow

<input type="checkbox"/>	Name	Description	Type	Used	Actions
<input type="checkbox"/>	ActiveX	ActiveX Applications	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Compressed	Compressed Files	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Executables	Executable Files	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Images	Bitmaps Images and Vetorials Files	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Javascript	Javascript Files	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Multimedia	Audio and Video Files	MIME	-	<div><div></div><div></div></div>
<input type="checkbox"/>	Office	Microsoft Office Files	MIME	-	<div><div></div><div></div></div>

Objects - Contents

We will explain in detail the action menu and later the columns of the "Contents" tab.

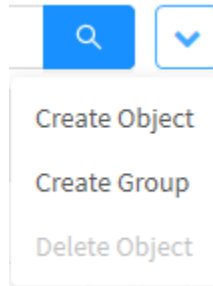
# Objects - Contents - Actions Menu

At the top right of the screen we have the actions menu:



Objects – Actions menu button

By clicking on this button the menu below is displayed:



Objects - Actions menu

The menu consists of the following options:

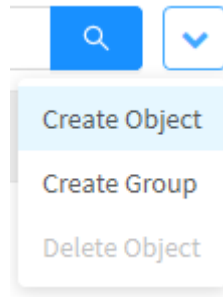
- *Create Object;*
- *Create Group;*
- *Delete Object.*

Next, each action menu option will be detailed.

# Objects - Contents - Actions menu - Create Object

Through the option "Create Object" it is possible to create a new object Contents. To access, follow the steps:

1. In the **actions menu** [  ], click on the "Create Object" option;



*Objects – Contents – Create Object*

2. The Create Contents Objects screen will appear. Fill in the fields:

Create Contents Object

X

\* Name

Image List

\* List Mime-Types

+

image/bmp

image/gif

image/jpeg

image/png

-

\* List Extensions

+

bmp

gif

jpeg

png

-





Description


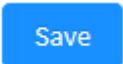
List of image types

Cancel

Save

Objects – Create Contents Object

- **Name:** Displays the object name. Ex.: Images;
- **List Mime-Types:** Displays the list of mime-types for the object. To add, click [  ], to delete any value entered, select it and click the [  ] button;
- **List Extensions:** Displays the list of object extensions. To add, click [  ] to delete any value entered, select it and click the [  ] button;
- **Description:** Displays the object description. Ex.: "Bitmaps Images and Vector Files".

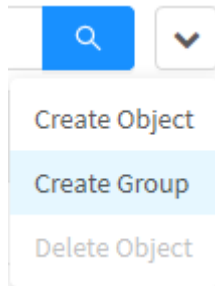
Click the [  ] button to cancel. Click the [  ] button to save.

The contents object was created successfully.

# Objects - Contents - Actions Menu - Create Group

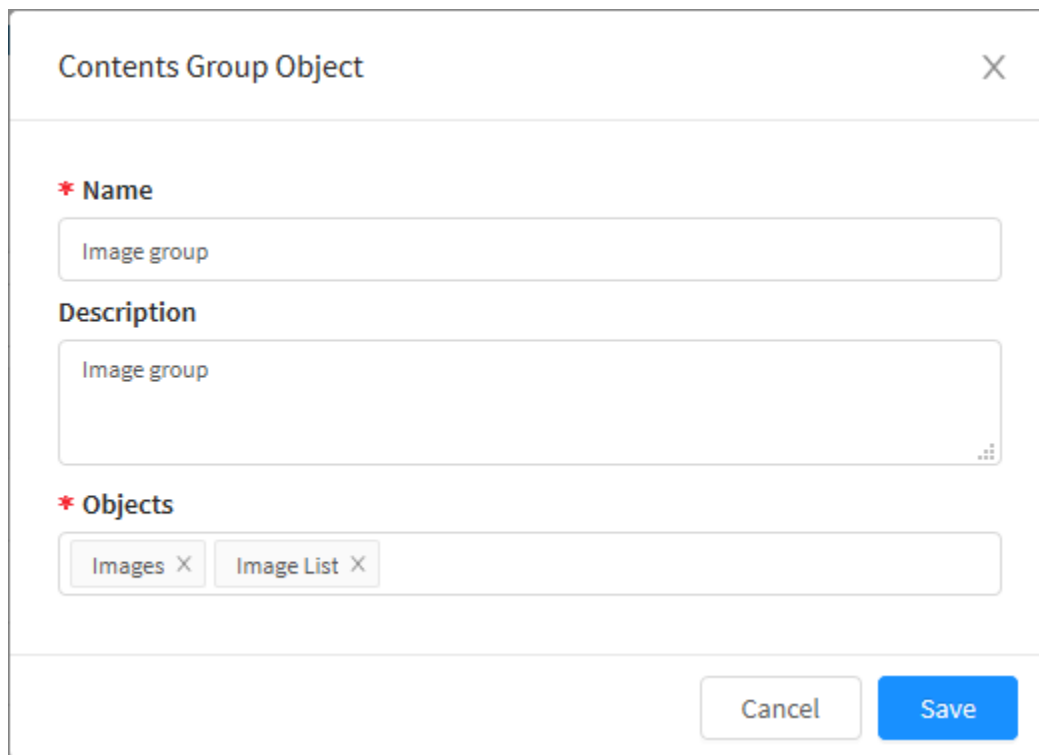
Through the button "Create Group" it is possible to create a new object group. To access, follow the steps:

1. In the **actions menu** [  ], click on the option "Create Group";



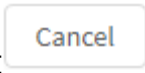
*Objects – Contents – Create Group*

2. Fill in the information on the Contents Group Object screen:

A screenshot of a form titled 'Contents Group Object' with a close button (X) in the top right corner. The form contains three main sections: 1. 'Name' (marked with a red asterisk) with a text input field containing 'Image group'. 2. 'Description' with a larger text input field containing 'Image group'. 3. 'Objects' (marked with a red asterisk) with a multi-select input field showing 'Images' and 'Image List' as selected items, each with a close (X) button. At the bottom right of the form are 'Cancel' and 'Save' buttons.

*Objects – Contents Group Object*

- **Name:** Displays the name of the object group. Ex.: *Image group*;
- **Description:** This field is intended for the description of the group. Ex.: *Image group*;
- **Objects:** It allows selecting the objects that were previously added in [Objects - Contents - Actions menu - Create Object](#). The objects added in this field will be inserted as tags.



Click the [ ] button to Cancel or the [ ] button to save.



Saved successfully

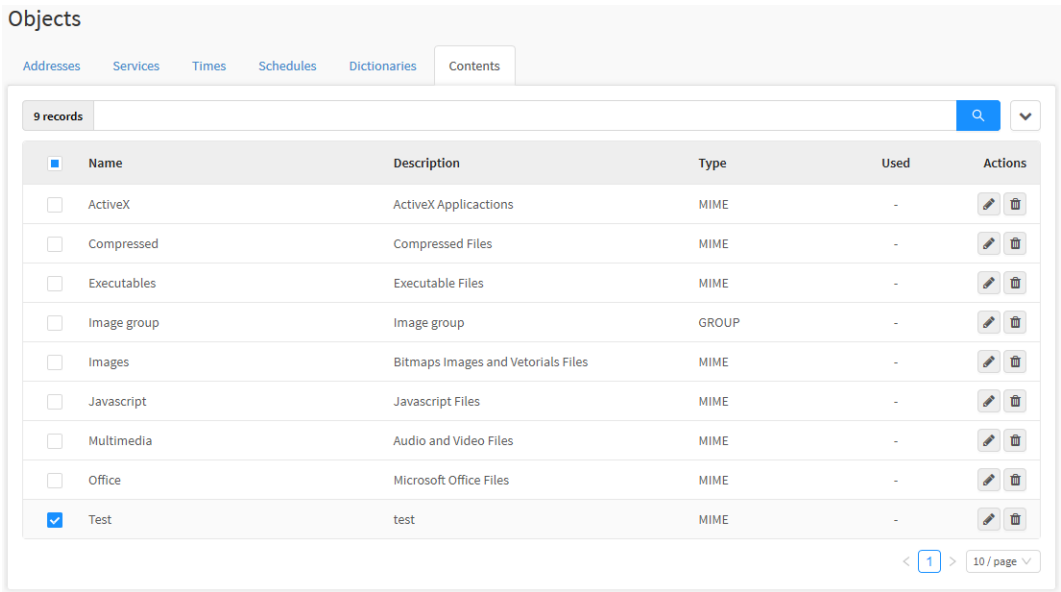
*Saved successfully*

The group was created successfully.

# Objects - Contents - Actions Menu - Delete Object

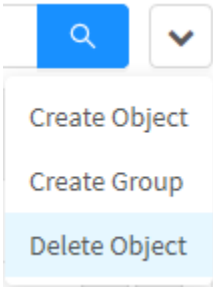
Through the button "Delete Object" it is possible to delete objects or groups of objects. To delete from the actions menu, follow these steps:

1. Select which package (s) you want to delete by clicking the **checkbox** ☐. Ex.: *Test*;



Objects - Objects selected for deletion

2. Enter the **actions menu**  and click on the "Delete Object" button.



Objects - Actions Menu - Delete Object

3. The message will appear if you really want to delete the selected groups or objects:



Confirm delete

×

Are you sure you want to delete the following objects contents?

- Test

Cancel

Delete

Objects - Are you sure you want to delete the following object contents


If you want to cancel, click the [ 

Cancel

 ] button. To finish, click the [ 

Delete

 ] button.

 **Object deleted successfully!**  
Object deleted successfully

After performing these procedures, the packages will have been successfully deleted.

# Objects - Contents - Columns

In the “Contents” tab, you can view the actions menu and six columns:

Objects

Addresses Services Times Schedules Dictionaries Contents

7 records

	Name	Description	Type	Used	Actions
<div><div></div><div></div></div>	ActiveX	ActiveX Applications	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Compressed	Compressed Files	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Executables	Executable Files	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Images	Bitmaps Images and Vetorials Files	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Javascript	Javascript Files	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Multimedia	Audio and Video Files	MIME	-	<div><div></div><div></div></div>
<div><div></div><div></div></div>	Office	Microsoft Office Files	MIME	-	<div><div></div><div></div></div>

Objects – Contents tab

Below we will explain each column of the Contents tab:

- **Select**: Select the desired objects;
- **Name**: Displays the object name;
- **Description**: The object description;
- **Type**: Displays the object type;
- **Used**

1

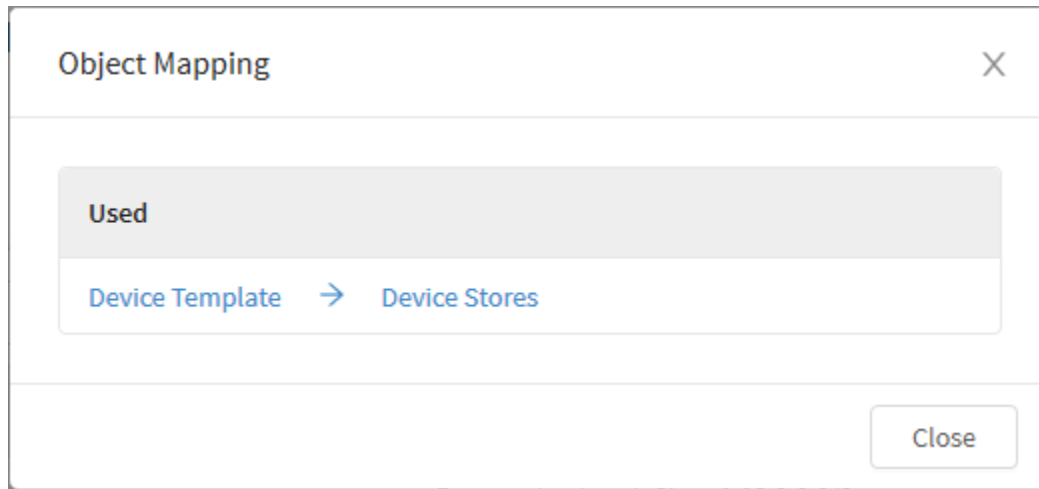
: Enumerates the number of times this object is being used. By clicking on this number, the Object Mapping window is displayed.
- **Actions**: Allows you to edit, select and delete the object;
  - **Edit**: Allows you to edit the settings of the Object added in the Create Object option of the actions menu;
  - **Delete**: Allows you to remove the Object.

# Objects - Contents - Object Mapping

By clicking on the icon of how many times an object was used [ **1** ] the Object Mapping window is displayed.

The function of the object mapping window is to display where the object was used.

In the example below, the object was used in the Device template named Device Stores.



*Object Mapping*

In addition, when clicking on the link, a redirection is made directly to where the object is being used.

# Users

The Users menu allows you to manage UTM users connected to GSM and to sort them by groups. This feature is intended to facilitate the definition and administration of compliance policies that will be applied later.

To access the screen, simply select the "Users" menu;



Management – Users

The screen below will be displayed:

Users

UsersGroups

24 records

<input type="checkbox"/>	Login	Name	E-mail	Device	Used
<input type="checkbox"/>	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
<input type="checkbox"/>	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
<input type="checkbox"/>	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
<input type="checkbox"/>	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
<input type="checkbox"/>	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
<input type="checkbox"/>	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
<input type="checkbox"/>	user16@blockbit.com	user16	user16@blockbit.com	Webfilter 1	-
<input type="checkbox"/>	user17@blockbit.com	user17	user17@blockbit.com	Webfilter 1	-
<input type="checkbox"/>	user18@blockbit.com	user18	user18@blockbit.com	Webfilter 1	-
<input type="checkbox"/>	user19@blockbit.com	user19	user19@blockbit.com	Webfilter 2	-

< 1 2 3 > 10 / page

Users - Users

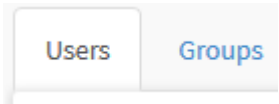
The Users screen has the following tabs:

- Users;
- Groups.

Next, the components of the Users tab will be analyzed.

# Users tab

This tab is used to manage UTM users. The "Users" tab should already be selected automatically, otherwise, click on it:



"Users" tab

The Users Screen will appear. It consists of the columns "Login", "Name", "E-mail", "Device" and "Used". In addition, the search bar and the actions menu are located at the top right of the screen.

Users

UsersGroups

15 records

	Login	Name	E-mail	Device	Used
<input type="checkbox"/>	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
<input type="checkbox"/>	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
<input type="checkbox"/>	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
<input type="checkbox"/>	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
<input type="checkbox"/>	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
<input type="checkbox"/>	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
<input type="checkbox"/>	user1@blockbit.com	user1	user1@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user2@blockbit.com	user2	user2@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user3@blockbit.com	user3	user3@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user4@blockbit.com	user4	user4@blockbit.com	Cluster Head Office	-

Users - Users main screen

In the next section, we will explain in detail the components of this screen.

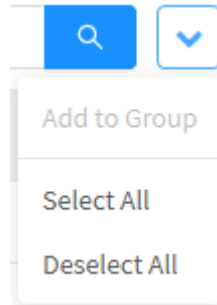
# Users - Actions Menu

At the top right of the screen we have the actions menu:



*Users – Actions Menu button*

By clicking on this button the menu below is displayed:



*Users – Actions menu*


Next, the action menu will be detailed. It consists of:

- Add to Group;
- Select All and Deselect All.

Next, each action menu option will be detailed.

# Users - Actions Menu - Add to Group

Through the option “Add to Group” it is possible to add a new user to the Group. To access it, follow the steps:

1. Select the user (s) you want to add. To select, click with the mouse on the checkbox next to the “Used” column. In selected users the checkbox will change to blue [  ]. Ex.: `user1@blockbit.com` and `user2@blockbit.com`;


Users

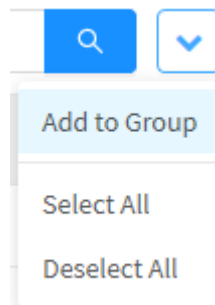
Users Groups

15 records

<input type="checkbox"/>	Login	Name	E-mail	Device	Used
<input type="checkbox"/>	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
<input type="checkbox"/>	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
<input type="checkbox"/>	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
<input type="checkbox"/>	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
<input type="checkbox"/>	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
<input type="checkbox"/>	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
<input checked="" type="checkbox"/>	user1@blockbit.com	user1	user1@blockbit.com	Cluster Head Office	-
<input checked="" type="checkbox"/>	user2@blockbit.com	user2	user2@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user3@blockbit.com	user3	user3@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user4@blockbit.com	user4	user4@blockbit.com	Cluster Head Office	-

Users – Selection of users to be added

2. In the **actions menu** [  ] click on the “Add to group” option;



Users – Add to group.

3. Define which group you want to add. You can select one or more groups to add. Ex .: Administrators;


Add users to group


Administrators X

Cancel

Save

*Users – Add users to group.*

Click on the  button to Save.

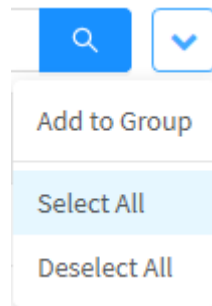
 **Users added successfully to group**  
Users added successfully to group

The user has been successfully added to the Group.



# Users - Actions Menu - Select All and Deselect All

By clicking on "Select All" in the action menu all users will be selected.



*Users – Select All*

This allows for easy implementation of an action that affects all users.

The "Deselect All" function is just the opposite: Remove all selections previously made.

# Users - Columns

A tela é composta pelo menu de ações e seis colunas. Segue uma breve descrição das colunas:

Users

UsersGroups

15 records

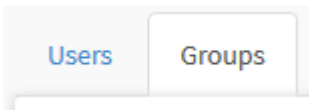
	Login	Name	E-mail	Device	Used
<input type="checkbox"/>	user10@blockbit.com	user10	user10@blockbit.com	Branch Office	-
<input type="checkbox"/>	user11@blockbit.com	user11	user11@blockbit.com	Store 1	-
<input type="checkbox"/>	user12@blockbit.com	user12	user12@blockbit.com	Store 1	-
<input type="checkbox"/>	user13@blockbit.com	user13	user13@blockbit.com	Store 1	-
<input type="checkbox"/>	user14@blockbit.com	user14	user14@blockbit.com	Store 1	-
<input type="checkbox"/>	user15@blockbit.com	user15	user15@blockbit.com	Store 1	-
<input type="checkbox"/>	user1@blockbit.com	user1	user1@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user2@blockbit.com	user2	user2@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user3@blockbit.com	user3	user3@blockbit.com	Cluster Head Office	-
<input type="checkbox"/>	user4@blockbit.com	user4	user4@blockbit.com	Cluster Head Office	-

Users – Users.

- **Select**☐: Select the desired users;
- **Login**: Displays the user login. Ex.: [user1@blockbit.com](#);
- **Name**: Displays the Username. Ex.: user1;
- **E-mail**: Displays the User email. Ex.: [user1@blockbit.com](#);
- **Device**: Shows which device the User was registered on. Ex.: Branch Office;
- **Used**: Lists the number of times this group has been used in Policies Manager.

# Groups Tab

This tab has the function of creating and editing UTM user groups. To access the screen, just select the "Groups" tab.



Users – User Groups

The User Groups Screen will appear. It consists of the actions menu and the User Groups already created, and these will be ordered in the columns "Name", "Type", "Device Name", "Used" and "Actions". In addition, the search bar and the actions menu are located at the top right of the screen.

Users

UsersGroups

3 records

	Name	Type	Device Name	Used	Actions
<input type="checkbox"/>	Administrators	global		-	<div></div> <div></div>
<input type="checkbox"/>	Stores	global		-	<div></div> <div></div>
<input type="checkbox"/>	Webfilter	global		-	<div></div> <div></div>

<1>

10 / page

Users - Groups

Next, the menu of actions will be analyzed and later we will delve into the content of the panel's columns.

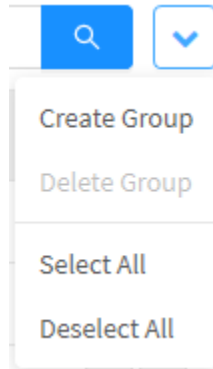
# Groups - Actions Menu

At the top right of the screen we have the actions menu:



Groups - Actions Menu button

By clicking on this button the menu below is displayed:



*Groups - Actions menu*


The menu consists of the following options:

- Create Group;
- Delete Group;
- Select All and Deselect All.

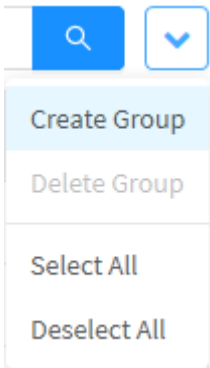
Next, each action menu option will be detailed.

# Groups - Actions Menu - Create Group

This section will demonstrate how to create user groups. This feature facilitates the definition and administration of compliance policies that will be applied later.

Through the button “Create Group” it is possible to create a new Group. To access, click on the **actions menu** [  ].

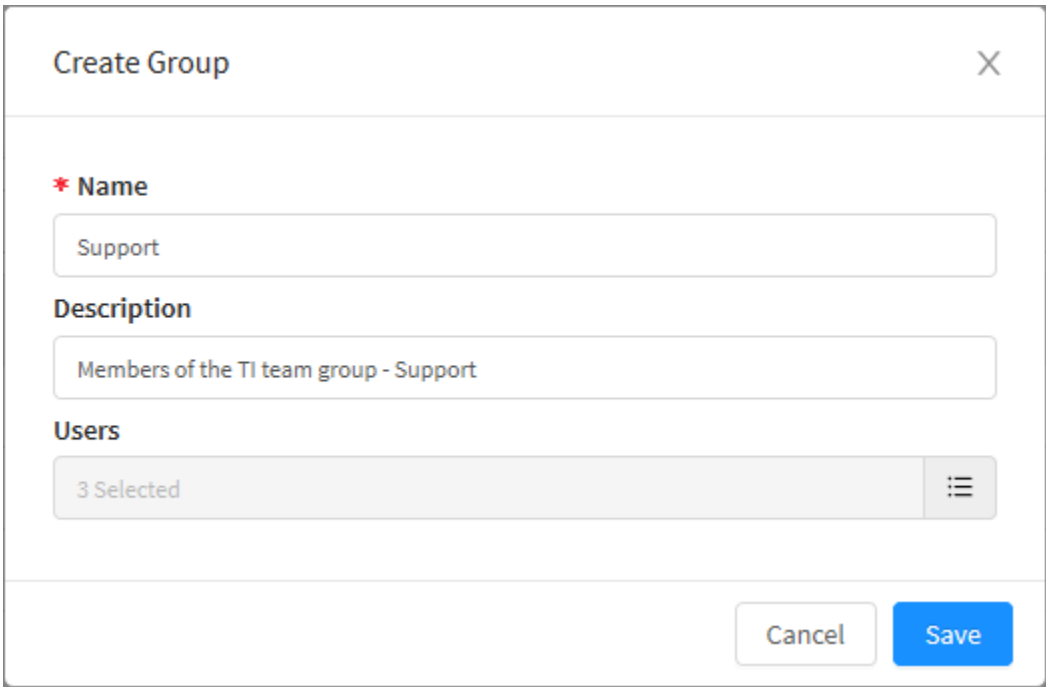
1. Click on the “Create Group” option;




Groups – Actions menu - Create Group

2. Fill in the Create Group screen;

- **Name:** Displays the name of the Group. Ex.: *Support*;
- **Description:** Displays the group description. Ex.: *Members of the TI team group - Support*;
- **Users:** Determines the users who will be part of the group being created.

A screenshot of a 'Create Group' dialog box. The title bar says 'Create Group' with a close button (X) on the right. The form has three sections: 1. 'Name' with a red asterisk and a text input field containing 'Support'. 2. 'Description' with a text input field containing 'Members of the TI team group - Support'. 3. 'Users' with a selection bar showing '3 Selected' and a list icon (three horizontal lines). At the bottom right are 'Cancel' and 'Save' buttons.

Groups – Create Group.

To add new users to the group, click on the [  ] button, as shown below:

Add Users

All

<input checked="" type="checkbox"/>	Users	Device Name
<input type="checkbox"/>	user10@blockbit.com	
<input type="checkbox"/>	user11@blockbit.com	
<input type="checkbox"/>	user12@blockbit.com	
<input checked="" type="checkbox"/>	user13@blockbit.com	
<input type="checkbox"/>	user14@blockbit.com	
<input checked="" type="checkbox"/>	user15@blockbit.com	
<input checked="" type="checkbox"/>	user16@blockbit.com	
<input type="checkbox"/>	user17@blockbit.com	
<input type="checkbox"/>	user18@blockbit.com	
<input type="checkbox"/>	user19@blockbit.com	

<

1

2

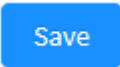
3

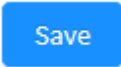
>


Cancel

Save

Groups - Create Group - Add Users


Select the users you want to add to the group and click the [  ] button.


Finally, click the [  ] button again to Save.

 **Group saved successfully**  
Group saved successfully

The group was created successfully.

# Groups - Actions Menu - Delete Group

Through the button "Delete Group" it is possible to delete created groups. To access, click on the **Actions Menu**  .

1. Select the Group you want to delete. To select, click on the checkbox next to the Name column. In the selected group, the checkbox will change from gray to blue  . Ex.: *Administrator* and *Store Managers*;

Users

UsersGroups

5 records

Name

Type

Device Name

Used



Actions

☐

Administrators

global

-





☐

Stores

global

-





☐

Support

global

-





☒

Test

global

-





☐

Webfilter

global


-



<1>

10 / page

Users - Groups - Groups you want to delete

2. In the **actions menu**  , click on the option "Delete Groups"

Create Group

Delete Group

Select All

Deselect All

Users - Groups – Actions Menu - Delete Groups

3. The message will appear if you want to delete the item(s):



Are you sure?

×


Are you sure you want to delete the groups: Test?

Cancel

Delete

User - Groups – Message if you want to delete the groups

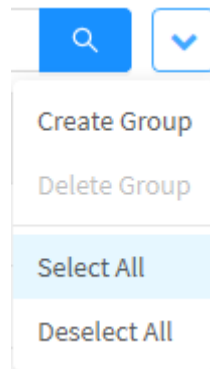
Click the [] button to cancel. Click the [] button to delete the selected groups.

 **Groups deleted successfully**  
*Groups deleted successfully*

The group (s) have been successfully deleted.

# Groups - Actions Menu - Select All and Deselect All

By clicking on "Select All" in the action menu all user groups will be selected.



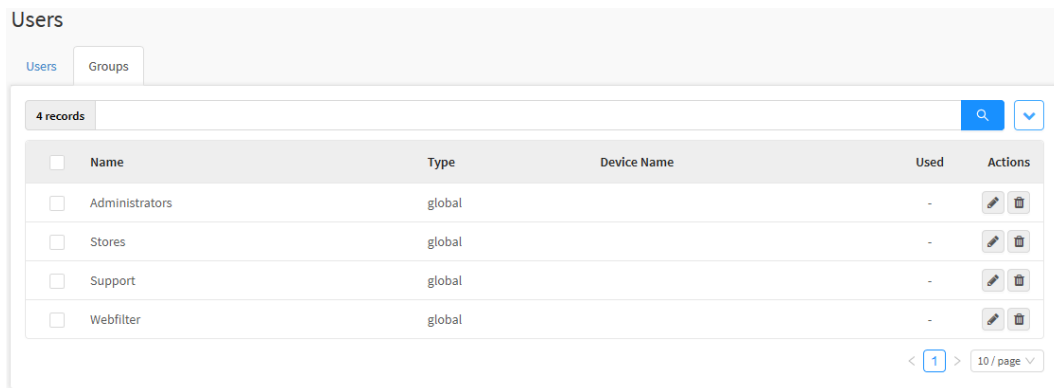
*Groups – Select All*

This allows for easy implementation of an action that affects all user groups.

The "Deselect All" function is just the opposite: Remove all selections previously made.

# Groups - Columns









The User Groups Screen will appear. It consists of the Actions Menu and the User Groups already created in the UTM, and these will be ordered by the Actions Menu and six columns. A brief description of the columns follows:



Users




Users Groups

4 records

<input type="checkbox"/>	Name	Type	Device Name	Used	Actions
<input type="checkbox"/>	Administrators	global		-	 
<input type="checkbox"/>	Stores	global		-	 
<input type="checkbox"/>	Support	global		-	 
<input type="checkbox"/>	Webfilter	global		-	 


< 1 > 10 / page


Users – Groups

- **Select** : Select the desired groups;
- **Name**: Displays the Group's name;
- **Type**: Determines the type of IP;
- **Device Name**: Shows which device the Group was registered on;
- **Used**: Lists the number of times this group has been used in Policies Manager.
- **Actions**: Contains the following buttons:
  - **Edit** : It allows to edit the settings of the group added in the Create Object option of the actions menu;
  - **Delete** : Removes the group.

In the session ahead we will explain in detail the menu of actions.

# Groups - Edit Group

Using the **Edit**  button it is possible to edit a created group.

1. Determine the Group you want to edit;
2. In the Actions column, click the **Edit**  button;
3. The screen below will appear. In this screen it is possible to edit the Settings (group name and description) and Users (group users) information;

Create Group

\*

Name


Administrators

Description

Admin user group

Users



4 Selected



Cancel

Save

Groups – Edit Group

- **Name:** Displays a group name. Ex.: *Administrators*;
- **Description:** Set a description for the group. Ex.: *Admin user group*;
- **Users:** Determines the users who will be members of this group. To select the categories, click the  button, choose the desired categories by checking the checkboxes , as shown below:


Add Users
✕

All
▼

<input type="checkbox"/>	Users	Device Name
<input type="checkbox"/>	user10@blockbit.com	
<input type="checkbox"/>	user11@blockbit.com	
<input type="checkbox"/>	user12@blockbit.com	
<input type="checkbox"/>	user13@blockbit.com	
<input type="checkbox"/>	user14@blockbit.com	
<input checked="" type="checkbox"/>	user15@blockbit.com	
<input checked="" type="checkbox"/>	user16@blockbit.com	
<input checked="" type="checkbox"/>	user17@blockbit.com	
<input type="checkbox"/>	user18@blockbit.com	
<input type="checkbox"/>	user19@blockbit.com	

<
1
2
3
>

Groups – Edit Group

If it is necessary to make a configuration on all items, just select the desired option in the **action menu** [  ]:

Select All  
Deselect All

SSL Inspection - Add Category - Actions Menu

Cancel

Save

To exit this panel, click the [ ] button or click the [ ] button to complete this process.



**Group saved successfully**

*Group saved successfully*

The group was successfully edited.

# Policies

This section will demonstrate how to create policy packages that will later be installed on devices.

With policy packages, you can manage the following services on Blockbit UTM: "Web Content Filter", "WEB Filtering and Application Control", "SSL Intercept", "IPS Inspection", "ATP Inspection", "Routing", "Traffic Shaping", "Traffic Priority and Warranty", "Traffic Quota Control and Time", "File Size Control", "Header Filters and Content", "link ", " Multiple services ", " NAT "and" Proxy ".

To access the screen, simply select the "Policies" button.



Management – Policies

The screen below will de displayed:

Policies

Policy Packages

Policy Templates

4 records

Name

Description

Type

Version

Policies

Actions

Branch Office Policies

Policies and Rules - Branch Office

ipv4

1.5

0

Head Office Policies

Policies and Rules - Head Office

ipv4

1.5

0

Store Policies

Policies and Rules - Stores

ipv4

1.5

1

Webfilter Policies

Webfilter Policies

ipv6

1.5

1

<

1

>

10 / page

Policies – Policy Packages

The Policies screen has the following tabs:

- [Policy Packages](#);
- [Policy Templates](#).

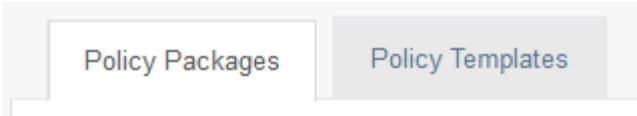
Next, the components of the [Policy Package](#) tab will be analyzed.

467

# Policy Packages Tab

This section will demonstrate how to create policy packages that will later be installed on devices.

If it is not already selected, click on the "Policy Packages" tab;



"Policy Packages" tab

The "Policy Packages" screen will be displayed. It is composed by the columns "Name", "Description", "Type", "Version", "Policies" and "Actions". In addition, at the top right of the screen is the [search bar](#) and the [action menu](#).

Policies

Policy Packages

Policy Templates

4 records

Q

<input type="checkbox"/>	Name	Description	Type	Version	Policies	Actions
<input type="checkbox"/>	Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Store Policies	Policies and Rules - Stores	ipv4	1.5	1	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Webfilter Policies	Webfilter Policies	ipv6	1.5	1	<div><div></div><div></div><div></div></div>

< 1 >

10 / page

Policies – Policy Packages

This section will demonstrate how to:

- [Register](#) and [Remove](#) policy packages;
- [Administer policy groups](#);
- Etc.

Next, we'll look at each component of this panel.



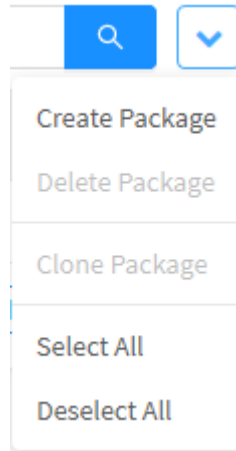
# Policy Packages - Actions menu

At the top right of the screen we have the actions menu:



Policy Package – Actions menu button

Clicking this button displays the menu below.:



Policy Packages – Actions menu


The menu consists of the following options:

- [Create Package](#);
- [Delete Packages](#);
- [Clone Packages](#);
- [Select All](#) and [Deselect All](#).

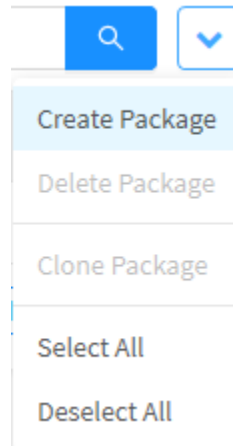
Next, each option in the action menu will be detailed.

# Policy Packages - Actions menu - Create Package



Through the option "Create Package" it is possible to create a new package. To access, click on the **actions menu** [  ].

1. Click on the "Create Package" option;



Policy Packages - Create Package

2. The "Create Policy Package" screen will be displayed. Fill it with the following data:

- **Name:** Package name. Ex.: *Branch Office Policies*;
- **Description:** Package description. Ex.: *Policies and Rules - Branch Office*;
- **Version:** Defines the version to be used in the package. It is important that the package version is the same as the UTM;



**ATTENTION:** If the package version is different from the UTM, they will not be compatible.

Always create packages with the same version of the UTMs to which they will be applied.

- **Type:** Select the type of IP protocol to be used, among the options: "IPv4" and "IPv6".

Create Policy Package

X

\* Name

Branch Office Policies

Description

Policies and Rules - Branch Office

\* Version

1.5



\* Type


IPv4

Cancel

Save

Policy Packages – Create Policy Package

If you want to cancel click on the [  ] button. To complete the creation of the policy package click on the [  ] button.

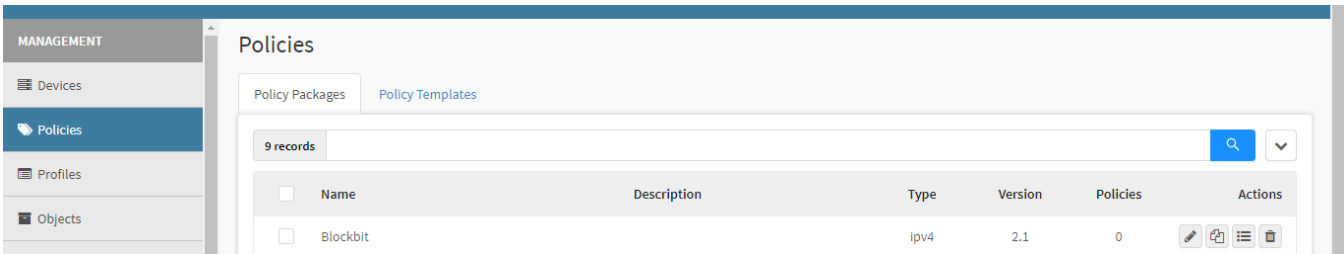
 **Package created successfully**  
Package created successfully

The package was created successfully.

# Policy Packages - Actions Menu - Clone Packages

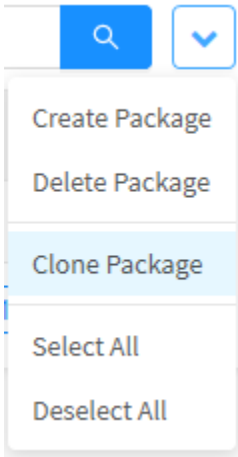
Through the button "Clone Packages" it is possible to clone existing packages. To clone packages follow the steps:

1. Select which package (s) you want to clone by clicking on the **checkbox** [ ] located in the action menu. Ex.: *Policies Branch office*;



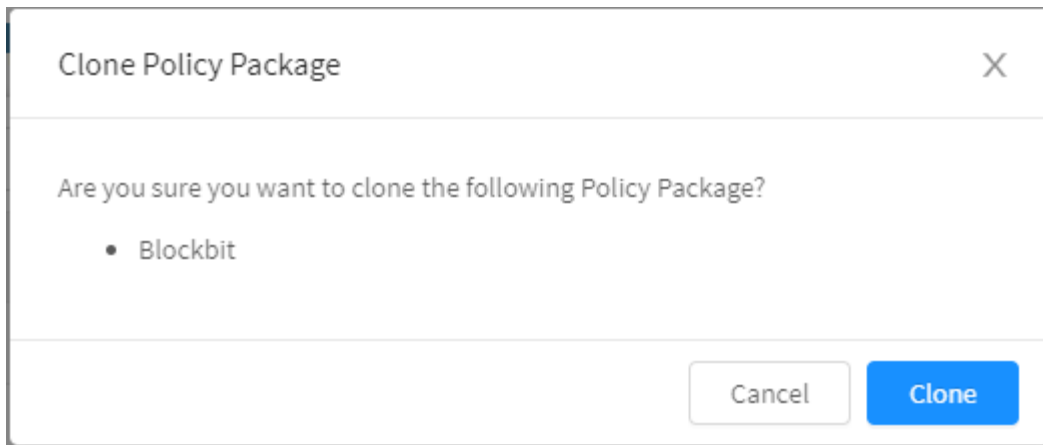
Policy Packages - Package selection

2. In the **action menu** [ ], click on the option "Clone Packages".



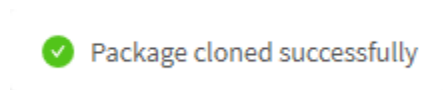
Policy Manager - Actions menu - Clone Package

3. A message will appear asking if you want to clone the selected item.



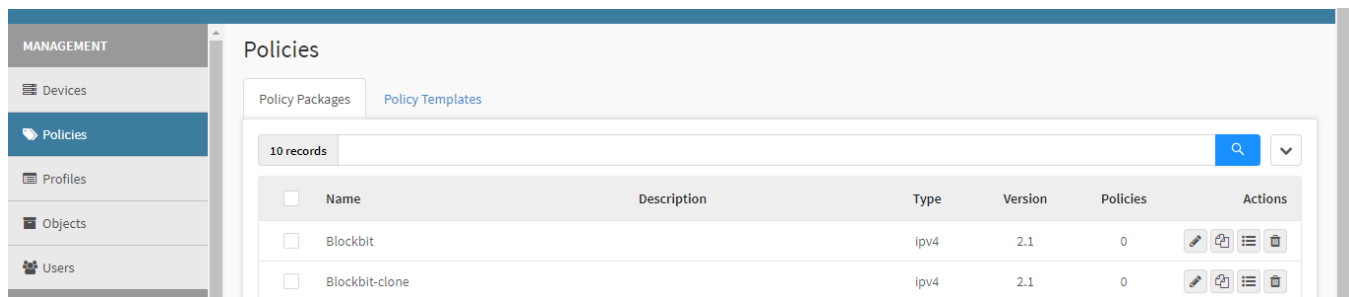
Policy Package – Clone Policy Package

If you wish to cancel click the [  ] button. To conclude, click the [  ] button.




Package cloned successfully

After performing these procedures the packages will have been successfully duplicated. As noted in the image below:



Policy Package - Cloned Package

It's also possible to clone a Policy Package by clicking the Clone button [  ].

# Policy Packages - Actions menu - Delete Packages

Trough the “Delete Packages” button it is possible to delete several installed packages at the same time. To delete from the action menu, follow these steps:

- 1. Select which package (s) you wish to delete by clicking the **checkbox** [  ] located in the action menu. Ex.: Policies Branch office;

Policies

Policy Packages

Policy Templates

5 records

<div><div></div></div> Name	Description	Type	Version	Policies	Actions
<div><div></div></div> Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	<div><div></div><div></div><div></div></div>
<div><div></div></div> Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	<div><div></div><div></div><div></div></div>
<div><div></div></div> Store Policies	Policies and Rules - Stores	ipv4	1.5	1	<div><div></div><div></div><div></div></div>
<div><div><div></div></div></div> Test	Test	ipv6	2.0	0	<div><div></div><div></div><div></div></div>
<div><div></div></div> Webfilter Policies	Webfilter Policies	ipv6	1.5	1	<div><div></div><div></div><div></div></div>

<

1

>

10 / page

Policy Packages – Delete Packages

- 2. Access the **actions menu** [  ] and click the "Delete Packages" button.

Create Package

Delete Package

Clone Package

Select All

Deselect All

Policy Packages – Actions menu – Delete Packages

- 3. The message asking if you really want to delete the selected packages will be displayed:

Delete Policy Package

X

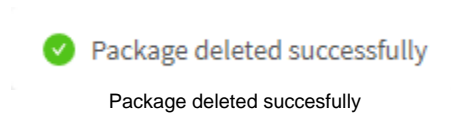
Delete "Test" Policy Package?

Cancel

Delete

Policy Packages – Delete Policy Package?

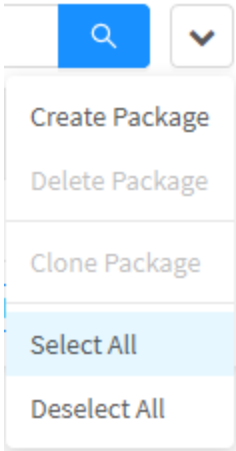
If you wish to cancel click on the [  ] button. To conclude click on the [  ] button.



After performing these procedures the packages will have been successfully deleted.

# Policy Packages - Actions menu - Select All and Deselect All

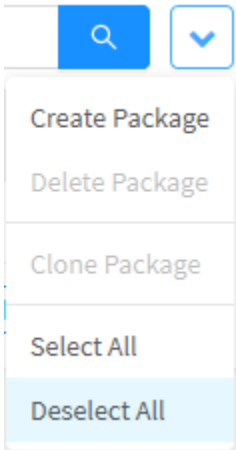
By clicking on "Select All" in the action menu all policies will be selected.



Policy Packages – Select All

This allows changes that affect all policies to be easily implemented.

The function of "Deselect All" is simply the opposite: Remove all previously made selections.



Policy Packages - Deselect All















# Policy Packages - Columns

Below we will explain each column of the Policy Packages tab:

Policies

Policy PackagesPolicy Templates





4 records

<input type="checkbox"/>	Name	Description	Type	Version	Policies	Actions
<input type="checkbox"/>	Branch Office Policies	Policies and Rules - Branch Office	ipv4	1.5	0	  
<input type="checkbox"/>	Head Office Policies	Policies and Rules - Head Office	ipv4	1.5	0	  
<input type="checkbox"/>	Store Policies	Policies and Rules - Stores	ipv4	1.5	1	  
<input type="checkbox"/>	Webfilter Policies	Webfilter Policies	ipv6	1.5	1	  

< 1 > 10 / page

Policies – Policy Packages

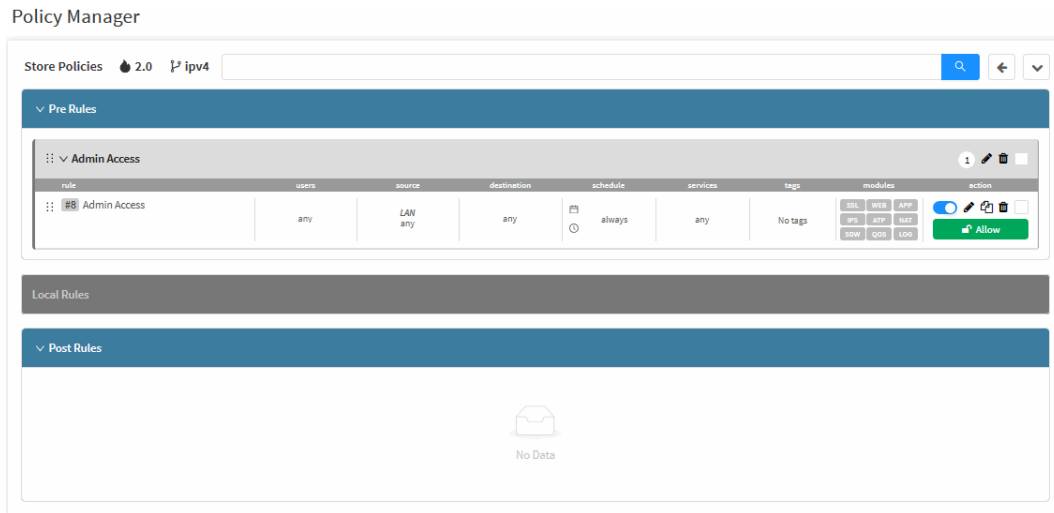
Next we will explain each column:

- **Checkbox** : Select the Policy Package;
- **Name**: Displays the name of the registered Policy Package;
- **Description**: Displays the description of the registered Policy Package;
- **Type**: Represents the type of IP. Ex.: "IPv4";
- **Version**: Displays the version in which the Policy Package was created. It is extremely important to create Policy Packages of the same version as UTM, otherwise the package will not be compatible;
- **Policies**: Displays the amount of policies the package has. Ex.: "100";
- **Actions**: The "Actions" column is made up of several buttons:
  - **Edit** : Allows you to edit the Policy Package settings added in the [Create Package](#) option of the action menu;
  - **List Group Policies** : Allows you to view, edit and add more specific Policy Package options. For more information, go to the [Policy Packages - Policy Manager](#);
  - **Delete** : Deletes the Policy Package.

Next, the functions of the List Group Policies button will be explained and exemplified.

# Policy Packages - Policy Manager

The Policy Manager screen displays more detailed information of the created Policy Packages.



Policy packages – Policy Manager

The Policy Manager dashboard is divided into:



- **Package Name:** Displays the name of the registered Policy Package;
- **System Version** [🔥]: Displays the version in which the Policy Package was created. It is extremely important to create Policy Packages of the same version as UTM, otherwise the package will not be compatible;
- **IP** [🔑]: Represents the type of IP used in Policy Packages created. Ex.: "IPv4";
- **Search bar:** Its function is to make it possible to locate specific items, it is possible to click on some column fields within the policy group to serve as a filter in a more specific search;

- **Botão Back** [⬅️]: Return to previous panel;
- **Actions menu** [⌵]: Displays the following set of contextual options:
  - [Create Group](#);
  - [Delete Groups](#);
  - [Import Template](#);
  - [Save Template](#);
  - [Create Policy](#);
  - [Delete Policies](#);
  - [Expand All and Collapse All](#).
- **Pre Rules:** Represents all policy groups created as "Header", when installed in Blockbit UTM it will be installed above existing policy groups in Blockbit UTM, therefore it will have priority over the rules created in the UTM itself;
- **Local Rules:** Represents the default rules for existing policy groups in Blockbit UTM;
- **Post Rules:** All policy groups created as "Footer", when installed in Blockbit UTM will be installed below existing policy groups in Blockbit UTM, therefore it will have priority over the rules created in UTM and it will have priority over rules applied in the Footer.











It is important to remember that policies are ordered by "Priority", and they are enforced considering the "First Match Wins" method (which literally means "1st among competitors wins"). Therefore, the policies located above have priority while those below have lower priority.

Each policy group contains the following buttons:

- [⋮] Clicking and dragging moves the group order and allows you to rearrange the priority according to which group is above (First Match Wins);
- [➤] Expands to display the policies created in the group;
- [0] Informs how many policies there are in the group;
- [🔧] Allows you to edit the settings added in the [Create Group](#) option in the action menu;

- [  ] Delete the group;
- [  ] Select the group to interact with the action menu.

The columns within each policy group are divided into:

- **Move** [  ]: Clicking and dragging moves the order of the policy and allows you to rearrange the priority according to which policy is above (First Match Wins);
- **Id** [  #8 ]: Displays the identification number of the policy, it is possible to click on it to serve as a filter in the search field;
- **Rule**: Displays the name of the policy;
- **Users**: It determines which users are affected by the policy, it is possible to click on this field to serve as a filter in the search field;
- **Source**: Displays if the source of this rule will be the Network zone, IP address, network interface, Mac Address or any of these, it is possible to click on this field to serve as a filter in the search field;
- **Destination**: It determines the destination of the rule, the IP address or service, it is possible to click on this field to serve as a filter in the search field;
- **Schedule**: Displays if the rule depends on a period of time or scheduling, you can click on this field to serve as a filter in the search field;
- **Services**: Displays the services that the rule affects, you can click on this field to serve as a filter in the search field;
- **Tags**: Displays the tags that have been added to this rule, you can click on this field to serve as a filter in the search field;
- **Modules**: Determines which UTM modules the rule will interact with, it is possible to click on this field to serve as a filter in the search field;
- **Action**: Displays some contextual buttons and what action the rule takes.
  - **Enabled** [  ] ou **Disabled** [  ]: Through this selector, activates or deactivates the rule;
  - **Edit** [  ]: Allows you to edit the settings added in the [Create Policy](#) option of the actions menu;
  - **Delete** [  ]: Removes the policy;
  - **Select** [  ]: Allows the selection of policies in order to interact with the actions menu;
  - **Action**: Determines the behavior of the policy in question, having as possible outcomes:
    - [  ]: As the name says, this option grants access;
    - [  ]: Access is denied;
    - [  ]: Access is denied, but a rejection message is displayed to the user.

## Validate Policies

In *Policies IPv4*, on the actions menu, there is the "Validate Policies" option for the system to check for conflicts and redundancies among current Policies. When validating policies it's important to check the notifications on the upper right corner of the screen to check the result. After, one must also refresh the page on the browser.

The Policies Validation can display as a result, one the following Policies' statuses:

**Same parameters with different actions:** In case two Policies name the same origin and same destination, but the actions contradict each other. For instance, the allow action over browsing in a certain Policy and the restrict action over the very same browsing on another, but for the same origin and same destination.

**Duplicity:** Happens when two Policies comprehend the same actions, origin and destination.

**Obscuring:** Happens when a Policy overlaps another in terms of action, when the described action is already carried out by a previous Policy.

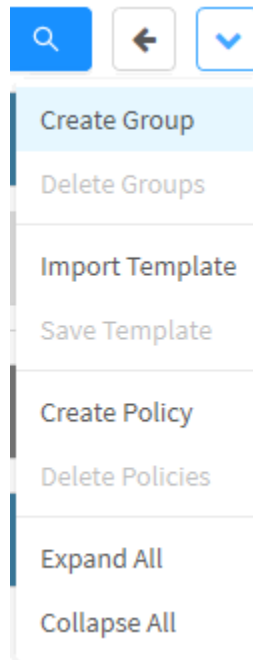
It's important to remember that the rules' prioritization is top-down within the Firewall.

For more information on policies, see the chapter about [policies](#) on the UTM Manual.

# Policy Manager - Actions menu - Create Group

This button creates policy group, to do so, follow the steps:

1. In the Actions Menu, click on the "Create Group" option;



Policy Packages – Actions menu – Create Group


2. The "Create Group" screen will appear;

A screenshot of a 'Create Group' dialog box. The title bar says 'Create Group' with a close button (X) on the right. Inside the dialog, there are two required fields marked with a red asterisk: 'Name' and 'Position'. The 'Name' field contains the text 'Administrator Access'. The 'Position' field is a dropdown menu currently showing 'Pre Rules'. At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

Policy Manager – Create a Policy Group – New Group

- **Name:** Determines the name of the policy group;
- **Position:** Determines the priority of the policy group by following the "First Match wins" rule;
  - **Pre Rules:** It is above the other rules, so this rule group will have higher priority;
  - **Post Rules:** It is below the other rules, so this rule set will have lower priority.

3. If you wish to cancel click the [  ] button. To conclude, click the [  ] button;

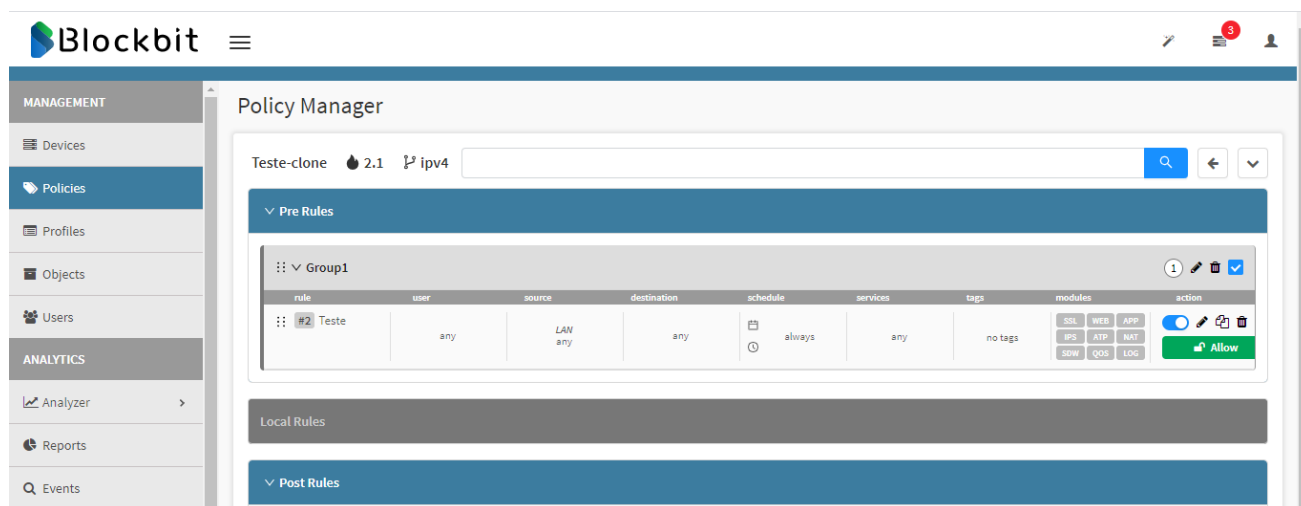
 Group created successfully

Group created successfully


4. The group was created successfully;

5. The Policy Manager screen will display a new gray item with the name previously entered (in the case of the example: "Administrator Access");

6. The dark gray "Local Rules" bar represents the standard UTM rules. The policy group that was created will be positioned according to the previously selected priority, in this example "Pre Rules" therefore, it will be located above the rules, as shown below.




Policy Manager – Rules

The Policy Packages priority can also be edited, just hold the Drag button [  ] and move the Pre Rules down or the Post Rules up.


For more information on the components of this panel, check the [Policy Packages - Policy Manager](#) page.

# Policy Manager - Actions menu - Delete Groups

The “Delete Policies” button deletes the selected Policy Groups.

**Attention:** When deleting the group, all policies that are within it will be deleted as well.

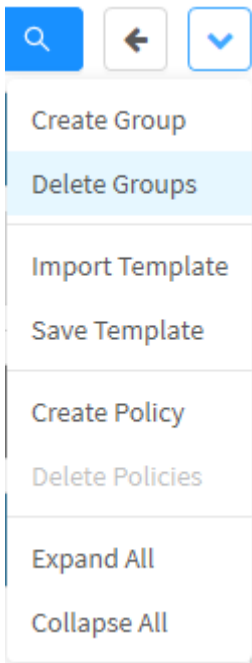
To delete, follow the steps:

1. Select the Policy group (s) you wish to delete. To select, click with the mouse in the checkbox. In the selected groups the checkbox will change from gray to blue . Ex.: *Administrator CLI*;



Policy selected to be deleted

2. In the Actions Menu, click on the option “Delete Groups”;



Policy Manager - Actions menu - Delete Policies

3. The screen will appear asking if you want to delete the group:

Are you sure?

X

Are you sure you want to delete the group Group 1?

Cancel

Delete

*Policy Manager – Delete*

If you want to cancel, click the [] button. To finish, click the [] button.

The group was successfully removed.

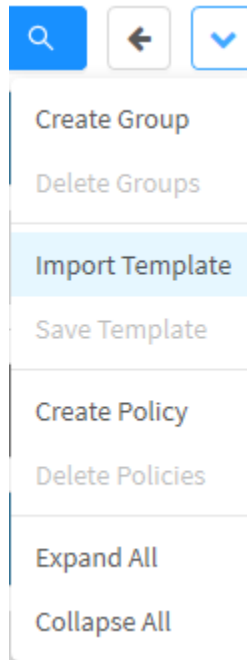
# Policy Manager - Actions menu - Import Template

The "Import Template" button is intended to import an existing Template into a specific package where it can be imported into the "Header" or "Footer" of the selected package. To import a template, follow these steps:

1. Select the location where the template will be imported: "Header" or "Footer";

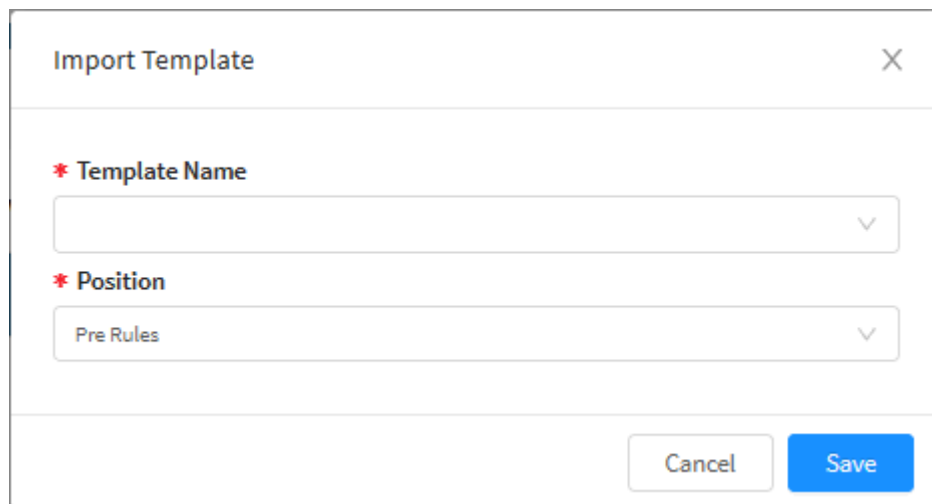


2. In the **actions menu** [ ], click on the "Import Template" option;



Policy Manager – Actions menu – Import Template.

3. The Import Template screen will be displayed;

A screenshot of the 'Import Template' dialog box. The dialog has a title bar with 'Import Template' and a close button (X). Inside, there are two required fields: '\* Template Name' and '\* Position'. The 'Template Name' field is empty, and the 'Position' field has 'Pre Rules' selected. At the bottom right, there are 'Cancel' and 'Save' buttons.

Policy Manager – Template Name



4. As shown below, select the desired Template Name and the position in which you want it to be imported. Ex.: Productivity Loss;

Import Template

\* Template Name

Productivity Loss

\* Position

Pre Rules

Cancel

Save

Policy Manager – Selected template

If you wish to cancel, click the 

Cancel

 button. To conclude click on the 

Save

 button. The imported template will display “\_import” in front of your name, as exemplified by the image below.

Policy Manager

Head Office Policies 2.0 ipv4

Pre Rules

> Admin Access

> Productivity Loss\_import

Local Rules

Post Rules

No Data

Policy Manager – Imported Template

The template was imported successfully.

# Policy Manager - Actions menu - Save Template

The “Save Template” button has the purpose of saving a certain group of selected policies and transforming it as a Template to be reused later.



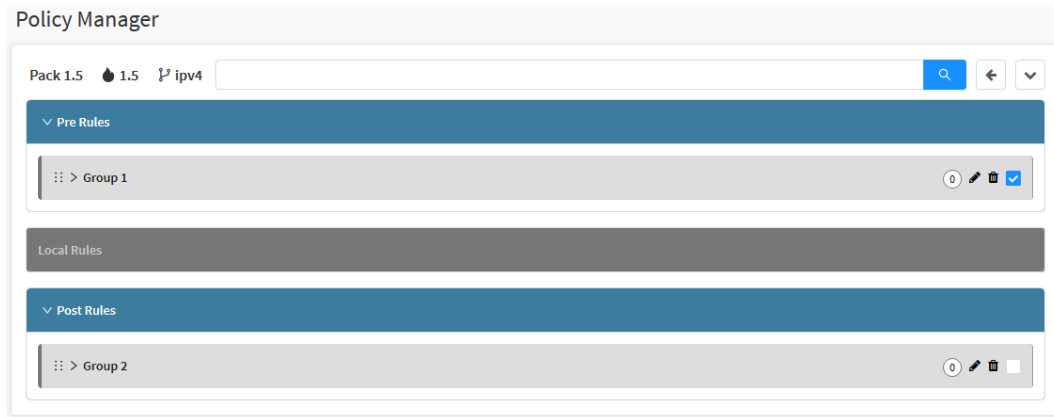
The group cannot have the same name as a template already created.

To save a Template, follow these steps:

1. Select the group you want to save. To select, click the mouse on the checkbox. In the selected packages the checkbox will change from gray to blue [



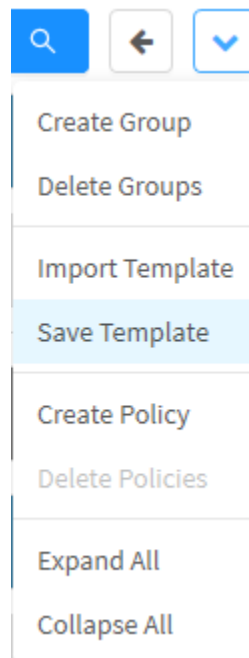
]. Ex.: Access Administrator;



Group selection - Save Template

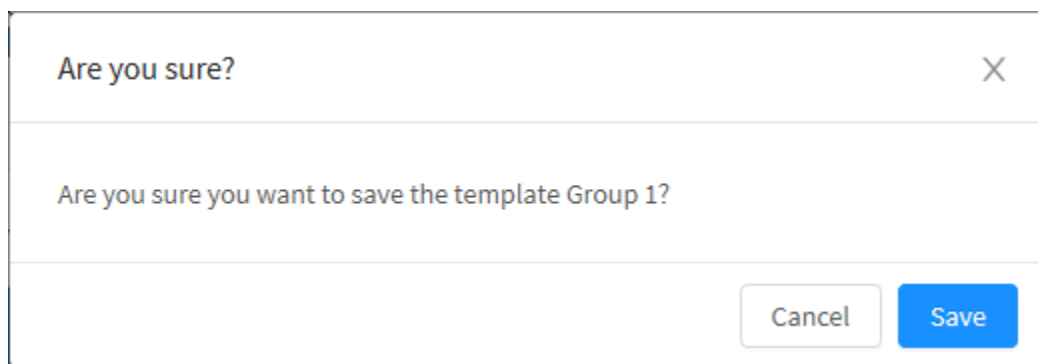


2. In the **actions menu** [ ], click on the “Save Template” option;

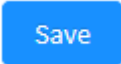
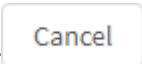


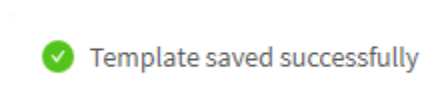
Policy Manager – Actions Menu – Save Template

3. The confirmation message will be displayed:



Policy Manager – Actions menu – Save Template

4. Click on the [  ] **button** to complete the operation or click the [  ] **button** to return to the previous panel:



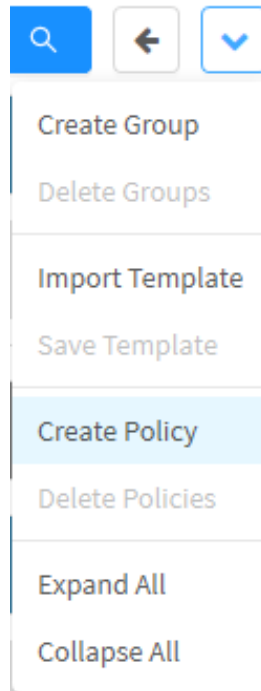
Template saved successfully.

The template has been saved successfully, it will be available on [Policy Templates Tab](#).

# Policy Manager - Actions Menu - Create Policy

The "Create Policy" button creates the policies in the policy group of your choice. It is necessary that a group has been previously created (check [Policy Packages - Actions Menu - Create Group](#) for more information). In the following we will exemplify how to create a new policy.

1. In the **actions menu** [  ], click on the option "Create Policy";



Policy Manager - Actions menu - Create Policy

2. The "Create Policy" screen will appear;

Properties

Connection

Inspection

Routing

Advanced

General

\* Name

Description

\* Action

Allow

Tags

\* Policy Group

☐ Traffic Monitor

☐ Traffic Logging

Schedule

☐ Time

☐ Schedule

Cancel

Save

## Policy Manager - Actions menu - Properties

3. Fill in the fields of **Properties** tab:

- **Name:** Policy name. Ex.: Admin Access;
- **Description:** Policy description. Ex.: Full *Administrator Access*;
- **Tags:** Create tags to make it easier to filter the policy search. Ex.: admin, access, port\_98;
- **Action:** Determines the action of this policy "Allow", "Deny" and "Reject". Ex.: *Allow*;
- **Policy Group:** Select the group in which the policy will be created: Ex.: *Administrator Access*;
- **Traffic Logging** ☐: If you want to enable traffic logging for this rule, activate the checkbox;
- **Time** ☐: If the checkbox is selected, it determines whether the rule will apply on working days ("Business"), weekends ("Weekend") or on any other object of the type "Time" that has been created;
- **Schedule** ☐: If the checkbox is selected, it allows to determine if the rule will apply in relation to a "Period / Date" object.

Select ☐ the services you need in your settings.

4. Fill in the fields of **Connection** tab:

Properties
Connection
Inspection
Routing
Advanced

\* Source

☐ Network Zone
☐ Network Interface
☐ Country

☐ IP Address
☐ MAC Address

Destination

☐ IP Address
☐ Service
☐ Country

Identification

☐ Authenticated
☐ Users
☐ Groups

Cancel
Save

## Policy Manager - Actions menu - Connection

- **Source**
  - **Network Zone:** This field is only available by checking the checkbox. This field allows you to select network zones that can be used. E. g. *WAN, LAN, DMZ*
  - **Network Interface:** This field is only available by checking the checkbox. This field allows to select network interfaces to be used as source filter.
  - **IP Address:** This field is only available by checking the checkbox. This field allows to select IP Address Object (s) (IPs, networks or sets) to be used as source filter.
  - **MAC Address:** This field is only available by checking the checkbox. This field allows to select Mac Address Address Object (s) to be used as source filter.
  - **Country:** This field is only available by checking the checkbox. This field allows you to select Countries to be used as a source filter.
- **Destination**
  - **IP Address:** This field is only available by checking the checkbox. This field allows you to select IP Address object (s) (IPs, networks or sets) to be used as a destination filter.
  - **Service:** This field is only available by checking the checkbox. This field allows you to select Service object (s) (protocols and ports) used as the destination filter.
  - **Country:** This field is only available by checking the checkbox. This field allows you to select Countries to be used as a destination filter.
- **Identification**
  - **Authenticated:** If enabled, this check box determines whether the policy requires authentication;
  - **Users:** This field is only available by checking the checkbox and the option Authenticated. Allows you to specify the user (s) to whom the policy will be applied.
  - **Groups:** This field is only available by checking the checkbox and the option Authenticated. Allows you to specify the group (s) to which the policy applies.

Select ☐ the services you need in your settings.



For additional information on how to fill in the fields, check the "**Connection**" tab in Blockbit UTM

4. Fill in the fields of **Inspection** tab:

Properties
Connection
Inspection
Routing
Advanced

Inspection

☐ SSL Inspection

☐ Intrusion Prevention

☐ Threat Protection

☐ Application Control

☐ Web Filter

Cancel
Save

## Policy Manager - Actions menu - Inspection

- **SSL Inspection:** This field is only available by enabling the checkbox. This field allows the interception of SSL traffic allowing the inspection of its content. The options that appear in this menu are created in [Proxy - SSL Inspection](#);
- **Intrusion Prevention:** This field is only available by enabling the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in [Services - Intrusion Prevention](#);
- **Threat Protection:** This field is only available by checking the checkbox. This field allows you to apply IPS to policies. The profiles displayed in this menu are created in [Services - Threat Protection](#);
- **Application Control:** This field is only available by checking the checkbox. This field allows you to select a profile to apply access control to applications. The profiles displayed in this menu are created in [Services - Application Control](#);
- **Web Filter:** This field is only available by checking the checkbox. This field allows you to select a profile to perform content filtering. The profiles displayed in this menu are created in [Services - Web Filter](#).

Select ☐ the services you need in your settings.

5. Fill in the fields of **Routing** tab:

Create Policy

X

Properties

Connection

Inspection

Routing

Advanced

Gateway

☐ NAT  
☐ policy.form.routing.cgnat

☐ SD-WAN

Application Routing

☐ Applications
 

SD-WAN Profile

QoS e Traffic Shaping

☐ Traffic Shaping
 

Flag Packets (TOS)

Cancel

Save

#### Policy Manager - Actions menu - Routing

- **Gateway**
  - **NAT:** Allows you to activate NAT and choose the address for source translation, by default the IP of the Default Gateway link is configured.
  - **CGNAT:** It allows to set up the use of CGNAT in a policy. It is a NAT solution in a provider-level, where the same IP address can be assigned to different hosts at the same time, with different traffic ports. In order to use CGNAT, available ports must start from port 2000 (TCP and UDP).
  - **SD-WAN:** It allows configuring the use of SD-WAN in the policy, being able to choose profiles that apply to the policy.
- **Application Routing**
  - **Application:** This field is only available by checking the checkbox. This field allows you to select applications so that requests received through the SD-WAN profile that is selected in the field below are routed, so that it is possible to obtain greater control over the consumption and bandwidth consumption of the selected applications. When clicking on the button [], the screen below will be displayed to select one or more IP address objects that will compose the policy. In order to set up the applications, it is required to enable the **SSL Inspection**.



The 'Add Application' dialog displays a grid of application categories, each with an icon and a count in a blue badge:

- ads (7), business (132), cloud (19), collaboration (35)
- download (3), email (19), games (43), mobile (22)
- p2p (25), portal (10), protocol (6), proxy (10)
- remote (39), social (83), storage (34), streaming (470)
- update (8), voip (3), web (249)

On the right, there is a search bar labeled 'Todos' and a list of items to select:

Item
<input type="checkbox"/> Ad_Master
<input type="checkbox"/> Core_Audience
<input type="checkbox"/> Doubleclick
<input type="checkbox"/> GoDaddy
<input type="checkbox"/> Google_Adsense
<input type="checkbox"/> OptMD
<input type="checkbox"/> Webtrends
<input type="checkbox"/> 1-800-Flowers
<input type="checkbox"/> 5pmweb
<input type="checkbox"/> 6.pm

At the bottom right, there are 'Cancel' and 'Salvar' buttons. Below the grid, there is a pagination bar showing '< 1 2 3 4 5 ... 122 >'.

## Policy Manager - Actions menu - Application Routing

- **SD-WAN Profile:** This field is required. It is used to determine which SD-WAN profile will be used to balance the routes used by the selected applications. The profiles displayed in this menu are created in Services - SD-WAN.
- **QoS and Traffic Shaping**
  - **Traffic Shaping:** It allows to activate and select the traffic priority, the values can be adjusted in **Settings >> Network >> Traffic Shaping**;
  - **Flag packets (TOS):** Activating allows the package to be marked according to the options: Minimum wait, Maximum processing, Maximum reliability, Minimum cost and normal priority;
  - **Flag packets (DSCP):** Activating allows the package to be marked according to the options.

Select ☐ the services you need in your settings.

6. Fill in the fields of **Advanced** tab:

Properties

Connection

Inspection

Routing

Advanced

## DoS Protection

☐ Packet Rate (packets/seconds)

Burst Rate

2000

10

## Options

☐ TCP MSS

Cancel

Save

## Policy Manager - Actions menu - Advanced

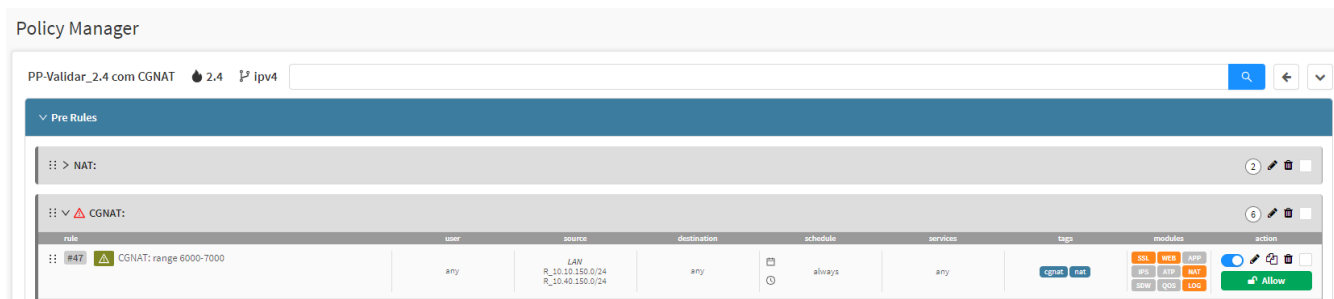
- **DoS Protection:** With this option checked ☒ it's possible to limit the maximum quantity of packages per second in the Firewall, avoiding distributed attacks or traffic anomalies caused by possible malwares in the network.
  - **Packet Rate:** The Packet Rate option sets up the Firewall in order to limit the connections to a maximum amount of packages per second.
  - **Burst Rate:** The Burst Rate option sets up the Firewall initially in order to allow a maximum quantity of packages per second without validating the Packet Rate, as to make the traffic control flexible in occasional traffic peaks.
- **Options**
  - **TCP MSS:** Allows the definition of a value that specifies the major quantity of data, in bytes, that a computer or communication device can receive in a single TCP segment.

Select ☐ the services you need in your settings.

Save

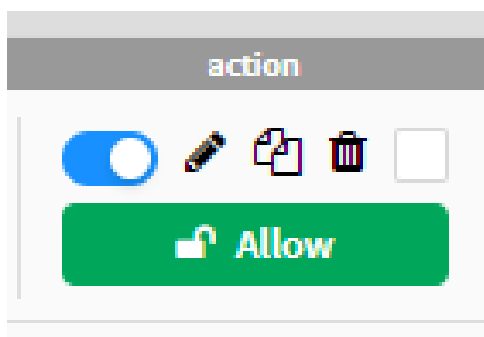
7. After completing the settings, click the  button;

After saving the settings the "Policy Manager" screen will appear again and it will be possible to verify your new policy.











Policy Manager

After the New Policy created in the group we can see that there are six action buttons created, as shown in the image below:




Policy Manager - Actions

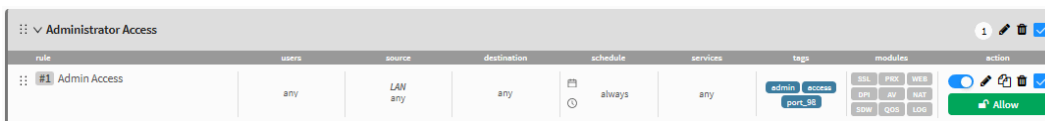
Here is a description of each of these buttons from left to right:

- **Mover** [  ]: Click and drag to move the policy. If it falls below another policy, it will have lower priority, if it is above, it will have higher priority;
- **Policy status** [  ]: Determines whether the policy will be enabled [  ] or disabled [  ];
- **Edit** [  ]: Edit the created policy;
- **Copy** [  ]: Copies the created policy;
- **Delete** [  ]: Removes the created policy;
- **Checkbox** [  ]: Select Policy;
- **Policy Action**: Displays what action the policy will take, which may be: **Allow**, **Block** or **Reject**.

# Policy Manager - Actions menu - Delete Policies

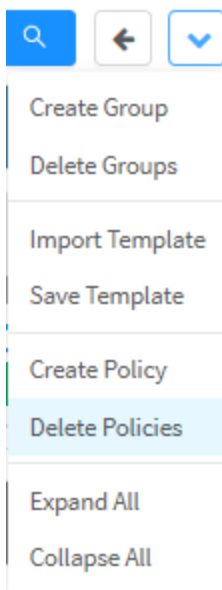
The “Delete Policies” button deletes the selected Policies. To delete, follow the steps:

1. Select the Policy (s) you want to delete. To select, click with the mouse in the checkbox. In selected packages the checkbox will change from gray to blue . Ex.: *Administrator CLI*;



Política seleccionada para ser deletada

2. In the actions menu [  ],, click on the option “Delete Policies”;



Policy Manager - Actions menu - Delete Policies

3. The screen will appear asking if you want to delete the items:

Are you sure?

Confirm

- Admin Access

Cancel

Delete

*Policy Manager – Delete itens policies*


If you want to cancel, click the [

Cancel

] button. To finish, click the [

Delete

] button.

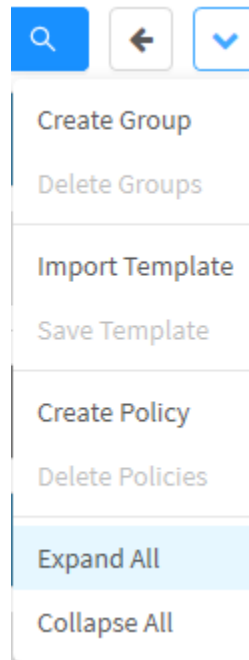
 **Policy deleted successfully**  
*Policy Deleted successfully*

Policy has been successfully removed.

# Policy Manager - Actions menu - Expand All and Collapse All

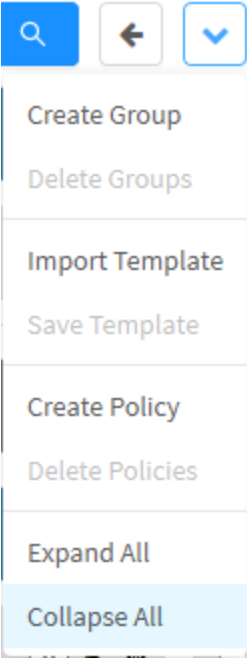
The “Expand All” button is intended to expand the policy group. To expand the policy group, follow these steps:

1. In the action menu, click on the “Expand All” option to expand the expanded policy groups;



Policy Manager - Actions menu - Expand All

2. When you click on “Collapse All” in the action menu, the opposite is the case.

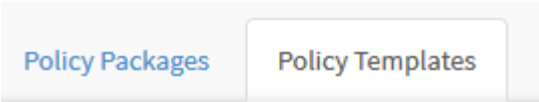


Policy Manager - Actions menu - Collapse All

# Policy Templates tab

This section will demonstrate how to create Policies Templates that can be reused later for a new policy package.

Click on the “Policy Templates” tab.



Policy Templates

The “Policy Templates” Screen will appear. It is composed of the “Name”, “Type”, “Version” and “Actions” columns. In addition, the [search bar](#) and the [actions menu](#) are located at the top right of the screen.

Policies

[Policy Packages](#) [Policy Templates](#)

3 records

<input type="checkbox"/>	Name	Description	Type	Version	Actions
<input type="checkbox"/>	Administrator Access	Administrator Access Policy Template	ipv4	2.0	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	Web Access	Web Access Policy Template	ipv4	2.0	<div><div></div><div></div><div></div></div>

< 1 >

10 / page

Policies – Policy Templates

This section will demonstrate how:

- [Register](#) and [Remove](#) Policy Packages;
- [Administer policy groups](#);
- Etc.

Next, the Policy Template columns will be explained and later the menu actions will be analyzed.



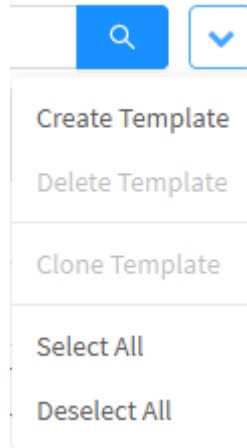
# Policy Templates - Actions Menu

At the top right of the screen we have the actions menu:



Policy Package - Actions Menu button

By clicking on this button the menu below is displayed:



Policy Packages - Actions Menu

The menu consists of the following options:

- [Create Template](#);
- [Delete Templates](#);
- [Clone Templates](#);
- [Select All and Deselect All](#).

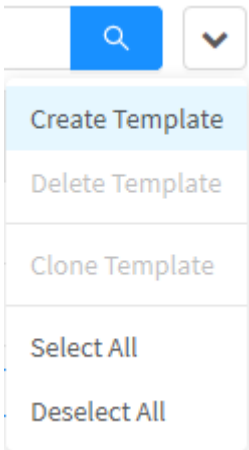
Next, each action menu option will be detailed.

# Policy Templates - Actions menu - Create Template



Through the option “Add Template” it is possible to create a new Policy Template. To access, click on the **Actions menu** [  ].

1. Click on the “Add Template” option;



Policy Templates - Actions menu

2. Fill in the “New Template” screen:

- **Name:** Template name. Ex.: *Productivity Loss*;
- **Type:** IP type;
- **Version:** Defines the version in which the template will be made, it is important that the template has the same version as the UTM;



**ATTENTION:** If the version of the template is different from the UTM, they will not be compatible.

Always create templates with the same version of the UTMs to which they will be applied.

Create Policy Template

\*

Name

Productivity Loss

Description

Productivity Loss Policy Template

\*

Version

2.0

\*

Type


IPv4

Cancel

Save

Policy Template – Create Policy Template


Click the  button.

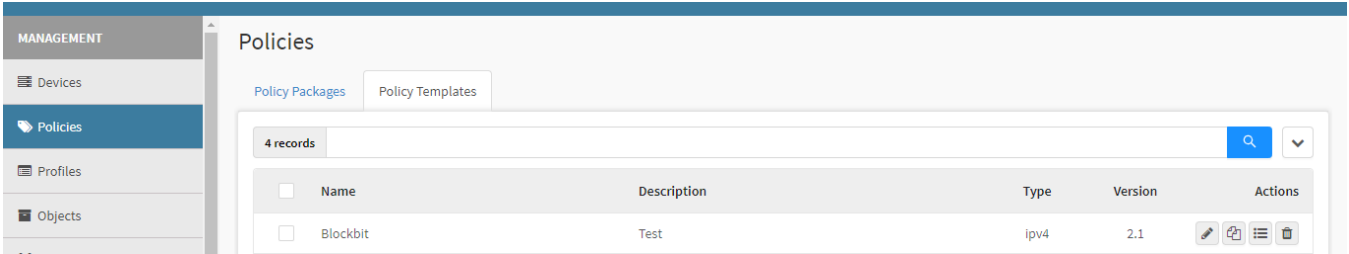
 **Package created successfully**  
*Package created successfully*

The Template was created successfully.

# Policy Templates - Actions menu - Clone Templates

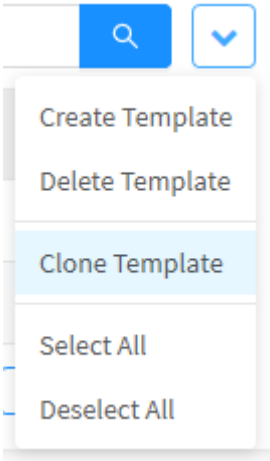
Through the button “Clone Templates” it is possible to duplicate an existing Template. To clone Templates, follow the steps:

- 1. Select which Template (s) you want to clone. To select, just click with the mouse on the checkbox located next to the Template Name description. In selected packages the checkbox will change from gray to blue [  ]. Ex.: Administrator Access;



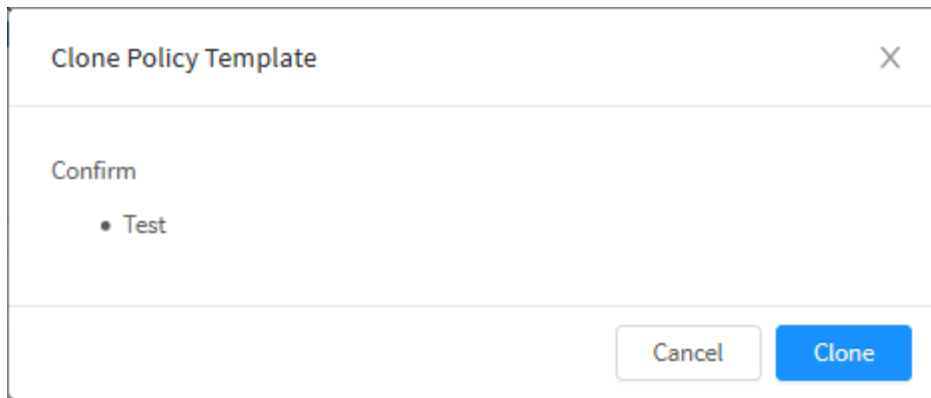
Policy Templates - Template selection

- 2. In the **action menu** [  ], click on the option “Clone Templates”;



Policy Templates – Clone Templates

A message will appear asking if you want to clone the selected item:

A dialog box titled "Clone Policy Template" with a close button (X) in the top right corner. The main content area has the heading "Confirm" followed by a bulleted list containing the item "Test". At the bottom right, there are two buttons: "Cancel" and "Clone".

Clone Policy Template


Confirm

- Test


Cancel Clone

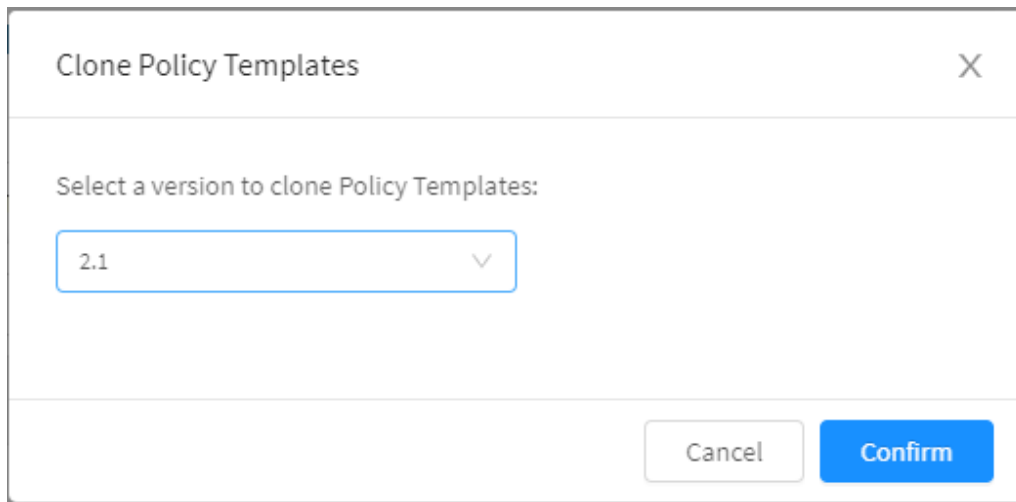
Policy Templates - Template cloning message

If you want to cancel, click the [  ] button. To finish, click on the [  ] button.

 **Package cloned successfully**  
*Package cloned successfully*

The Policy Templates screen will appear again with the cloned package.

It's also possible to clone policies by clicking the Clone button [  ]. When clicking, the following screen will appear:


A dialog box titled "Clone Policy Templates" with a close button (X) in the top right corner. The main content area has the heading "Select a version to clone Policy Templates:" followed by a dropdown menu showing "2.1" with a downward arrow. At the bottom right, there are two buttons: "Cancel" and "Confirm".

Clone Policy Templates

Select a version to clone Policy Templates:


2.1

Cancel Confirm

Click "Confirm" and a confirmation message will show up [  **Package cloned successfully** ]. The clone will have the same name, but with "-clone" next to it.

# Policy Templates - Actions menu - Delete Templates













Through the button "Delete Templates" it is possible to delete the selected Templates. To delete through the actions menu, follow these steps:

1. Select which Template (s) you want to delete. To select, just click with the mouse on the checkbox located next to the Template Name description. In selected packages the checkbox will change from gray to blue . Ex.: *Administrator Access*;

Policies


Policy Packages Policy Templates



4 records

<input checked="" type="checkbox"/>	Name	Description	Type	Version	Actions
<input type="checkbox"/>	Administrator Access	Administrator Access Policy Template	ipv4	2.0	  
<input type="checkbox"/>	Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	  
<input checked="" type="checkbox"/>	Test	Test	ipv4	2.0	  
<input type="checkbox"/>	Web Access	Web Access Policy Template	ipv4	2.0	  

< 1 > 10 / page

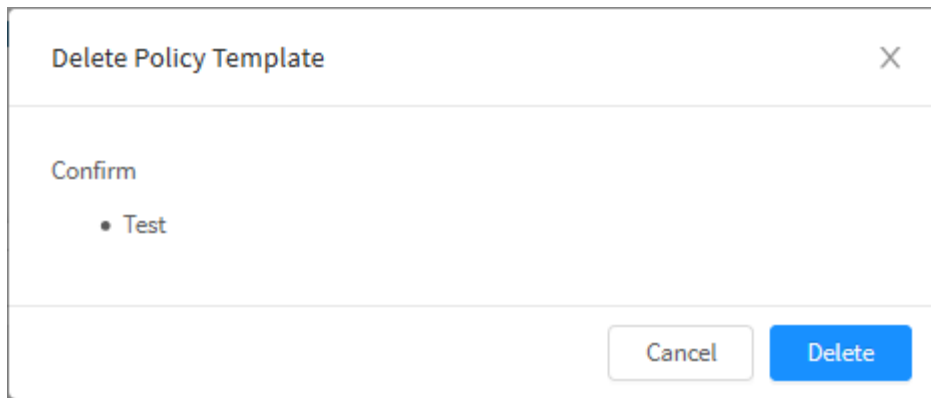
Policy Templates - Selection of Templates to delete

2. Enter the actions menu  and click on the option "Delete Templates".

	
Create Template	
Delete Template	
Clone Template	
Select All	
Deselect All	


Policy Templates – Delete Templates

3. The notification message will appear asking if you really want to delete the selected Templates:



Policy Templates - Message if you want to delete the Templates

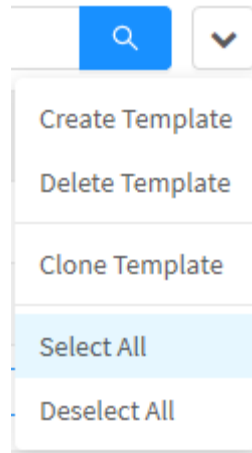
If you want to cancel click on the [  ] button. To finish, click the [  ] button.

 **Package deleted successfully**  
*Package deleted successfully*

After performing these procedures, the Templates will have been successfully deleted.

# Policy Templates - Actions menu - Select All and Deselect All

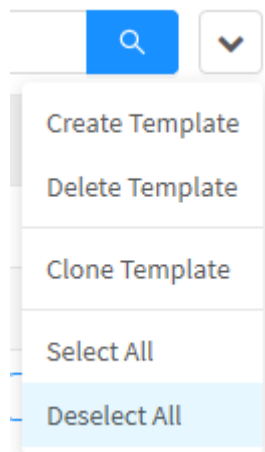
By clicking on "Select All" in the action menu, all templates will be selected.



*Policy Templates – Select All*

This allows for easy implementation of an action that affects all templates.

The "Deselect All" function is just the opposite: Remove all selections previously made.



*Policy Templates – Deselect All*












# Policy Templates - Columns

In the “Policy Templates” tab, it is possible to view the actions menu and five columns:

Policies

[Policy Packages](#) [Policy Templates](#)





3 records

<input type="checkbox"/>	Name	Description	Type	Version	Actions
<input type="checkbox"/>	Administrator Access	Administrator Access Policy Template	ipv4	2.0	  
<input type="checkbox"/>	Productivity Loss	Productivity Loss Policy Template	ipv4	2.0	  
<input type="checkbox"/>	Web Access	Web Access Policy Template	ipv4	2.0	  

< 1 > 10 / page

*Policies – Policy Templates*

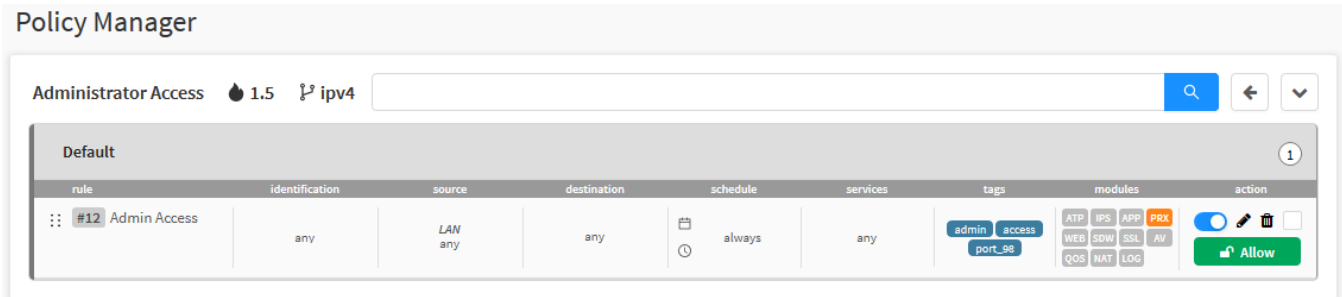
In the following we will explain each column of the Policy Templates tab:

- **Checkbox** : Select the Template;
- **Name**: The Template name;
- **Description**: Determines the description of the Template;
- **Type**: The IP type;
- **Version**: The UTM version;
- **Actions**: A set of essential actions:
  - **Edit** : By clicking on this icon it is possible to rename the template;
  - **Listar** : Visualizes the content of the template, making it possible to insert or remove tags, create, move and delete policies, validate them and, finally, perform searches, this option offers possibilities similar to those available in Policy Manager, with the exception of determining its location in the “Header” or “Footer”. For more information, see [Policy Templates - Policy Manager](#);
  - **Delete** : Removes the Template.

Next we will analyze the functions of the list button: [Policy Templates - Policy Manager](#).

# Policy Templates - Policy Manager





When clicking on the **List**  button in Policy Templates the following screen will be displayed:



*Policy Templates – Policy Manager*






The Policy Manager screen displays more detailed information on the Policy Packages created.






The Policy Manager panel is divided into:

- **Package Name:** Displays the name of the registered Policy Package;
- **System Version** : Displays the version in which the Policy Package was created. It is extremely important to create Policy Packages of the same version as UTM, otherwise the package will not be compatible;
- **IP** : Represents the type of IP used in the Policy Packages created. Ex.: "IPv4";
- **Search Bar:** Its function is to make it possible to locate specific items, it is possible to click on some column fields within the policy group to serve as a filter in a more specific search;
- **Back** : Returns to the previous panel;
- **Actions menu** : Features a set of contextual options:
  - [Create Template](#);
  - [Delete Templates](#);
  - [Clone Templates](#);
  - [Select All and Deselect All](#).

It is important to remember that the policies are ordered by "Priority", being that they are applied considering the "First Match Wins" method (which literally means "The 1st among the VENCE competitors"). Therefore, the policies located above have priority while those below have a lower priority.

Policy Manager columns are divided into:

- **Move** : Clicking and dragging moves the order of the policy and allows you to rearrange the priority according to which policy is above (First Match Wins);
- **Id** : Displays the identification number of the policy, you can click it to serve as a filter in the search field;
- **Rule:** Displays the policy name;
- **Users:** Determines which users are affected by the policy, you can click on this field to serve as a filter in the search field;
- **Source:** Displays if the source of this rule will be the Network zone, IP address, network interface, Mac Address or any of these, you can click on this field to serve as a filter in the search field;
- **Destination:** Determines the destination of the rule, the IP address or service, you can click on this field to serve as a filter in the search field;
- **Schedule:** Displays if the rule depends on a period of time or scheduling, you can click on this field to serve as a filter in the search field;
- **Services:** Displays the services that the rule affects, you can click on this field to serve as a filter in the search field;
- **Tags:** Displays the tags that have been added to this rule, you can click on this field to serve as a filter in the search field;
- **Modules:** Determines which UTM modules the rule will interact with, you can click on this field to serve as a filter in the search field;
- **Action:** Displays some contextual buttons and what action the rule takes.
  - **Enabled**  or **Disabled** : Through this selector, activates or deactivates the rule;
  - **Edit** : Allows you to edit the settings added in the [Create Policy](#) option of the actions menu;

- **Delete** : Removes the policy;
- **Select** : Allows the selection of policies in order to interact with the actions menu;
- **Action**: Determines the behavior of the policy in question, having as possibilities:
  - : As the name says, this option is to grant access;
  - : Access is denied;
  - : Access is denied, but a rejection message is displayed to the user.

## Validate Policies

In Policies IPv4, on the actions menu, we have the “*Validate Policies*” option that verifies conflicts and redundancies among the existing policies. When running the validation, it's important to check the notifications on the upper right corner of the screen to check the result. After, we must also refresh the browser page.

The validation of policies can provide one of the following statuses of the policies, as a result:

**Same parameters with different actions:** In case two or more policies nominate the same origin and the same destination, but the actions are contradictory. For instance, an action to allow browsing within a policy and the action to restrict browsing within another, but for the same destination and origin.

**Duplicity:** It occurs when two policies comprehend the same actions, origin and destination.

**Obscuring:** It occurs when a policy overlaps another one in terms of action, the described action is already done by a previous policy.

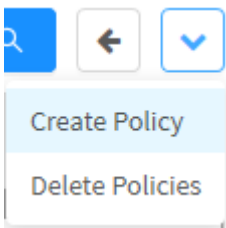
It's important to remember that the rules' prioritization is top-down from within the Firewall.

For more information on policies, see the [POLICIES](#) chapter of the UTM Manual.

# Policy Templates - Actions menu - Create Policy

The “Create Policy” button creates the policies in the policy group by selecting. To create a Policy, follow the steps:

1. In the **action menu** [  ], click on the option “Create Policy”;



Policy Manager - Actions menu - Create Policy

2. The New Policy screen will appear;

Policy Form

Properties

Connection

Content

Control

Security

Routing

General

Name

Description

Action

Allow

Tags

Policy Group

Traffic Logging

Schedule

Time

Period / Date

Cancel


Save

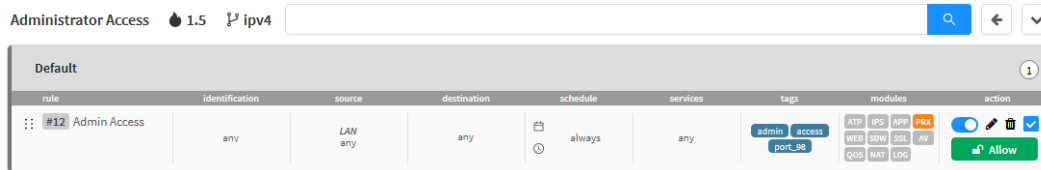
Policy Manager – New Policy

For more information on how to create new policies, see [Policy Manager - Actions Menu - Create Policy](#).  
After completing the creation of the policy, it will be added to the policy package.

## Policy Templates - Actions menu - Delete Policies

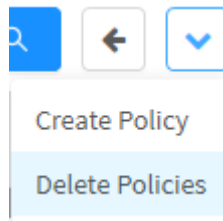
The “Delete Policies” button deletes the selected Policies. To delete, follow the steps:

1. Select the Policy(s) you want to delete. To select, click with the mouse in the checkbox. In selected packages the checkbox will change from gray to blue . Ex.: *Administrator CLI*;



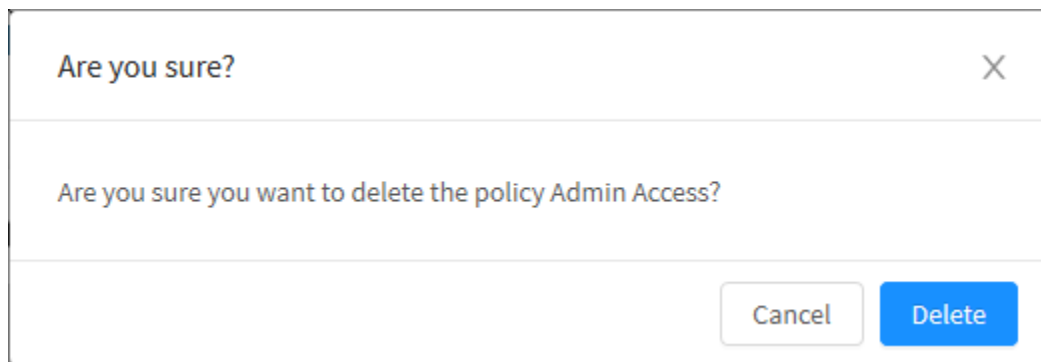
Policy selected to be deleted

2. In the **Actions** menu [  ], click on the option “Delete Policies”;



## Policy Manager - Actions menu - Delete Policies

3. The screen will appear asking if you want to delete the items:



*Policy Manager – Are you sure you want to delete the policy*

- If you want to cancel, click the  button. To finish, click the  button.

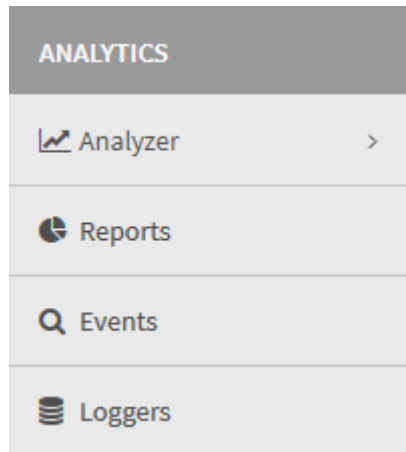
✔ Package deleted successfully

Package deleted successfully

Policy has been successfully removed.

# GSM - ANALYTICS

Through the "Analytics" menu it is possible to analyze reports, events and manage loggers.



Menu Analytics.

Contains the options:

- [Analyzer](#);
- [Reports](#);
- [Events](#);
- [Loggers](#).

# Analyzer

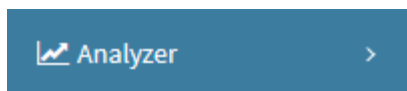
The Blockbit GSM - Analyzer is a module for evaluating and creating advanced reports, providing a holistic perspective on detection, when performing network traffic monitoring in real time at multiple points and network segments, the analyzer enables the investigation and execution of actions aimed at combating threats, intrusion attempts and use of unauthorized applications.

The Blockbit GSM - Analyzer works by receiving the data emitted by the UTMs, which are managed in the [Management](#) menu option, generating different types of reports and logs.

The analyzer offers the following features:

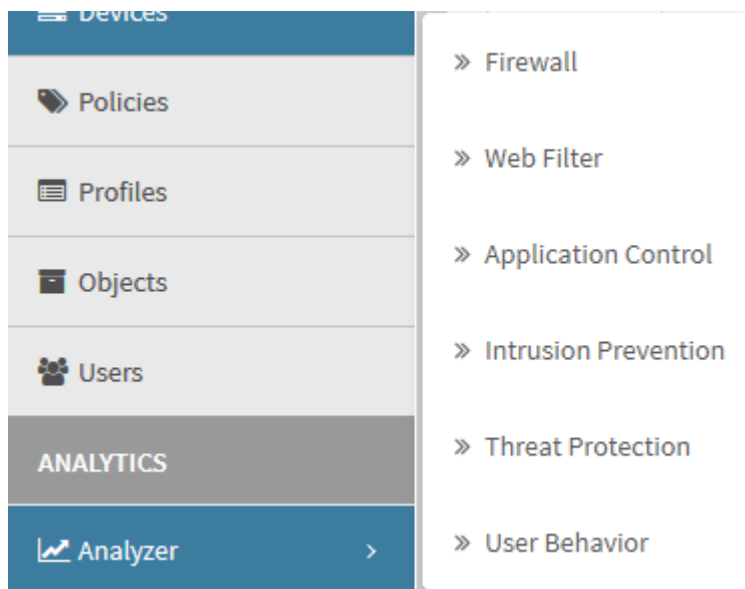
- To have a record of all activities performed by your users;
- To have a summary of the performance of the appliances and loggers used;
- To view any security threats and intrusion prevention;
- To have a mechanism that displays reports in realtime in a detailed way (Drill-Down);
- Effectiveness of web filters and application of policies;
- And more...

To access it, select the "Analyzer" option:



Analytics - Analyzer

When performing this action the following menu will be displayed:



Analyzer – Submenu

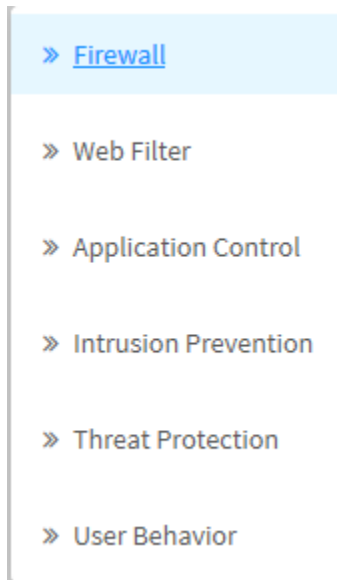
Select the desired option. The available options are:

- Firewall;
- Web Filter;
- Application Control;
- Intrusion Prevention;
- Threat Protection;
- User Behavior.



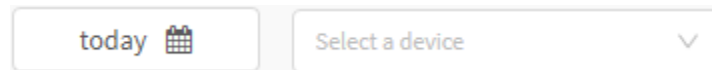
# Firewall

To access the network traffic reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “Firewall” option.



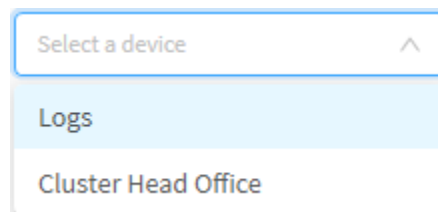
Firewall

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:



Firewall – Selection box

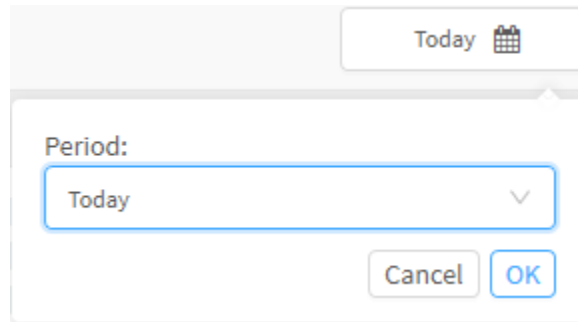
In this checkbox will be listed all devices (or groups of devices) previously registered in [Device Manager](#), to create a report, select the desired device.




Firewall – Selecting the Device


Right on the right side where we just selected the devices, it is possible to see a date selection box, the purpose of which is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.




Today 

Period:

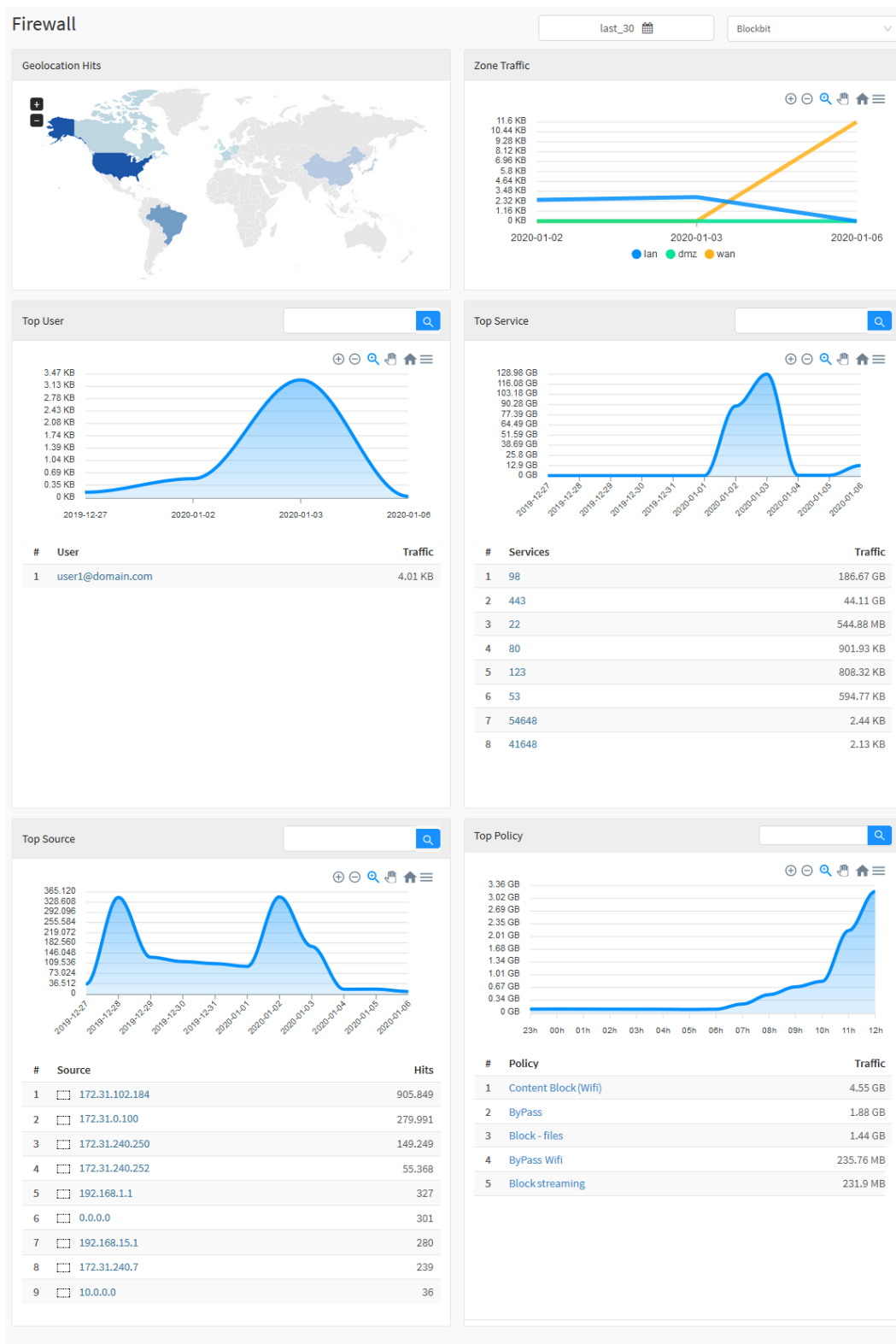
Today 

Cancel OK

Firewall – Date Selection

Select the desired date and click [  ];

The screen below will appear:








## Analyzer - Firewall


Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- : It serves to zoom in;

- [  ]: Its function is to remove the zoom;
- [  ]: It serves to make a selection zoom;
- [  ]: It serves to move the graph;
- [  ]: Reset the graph to the starting position;
- [  ]: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

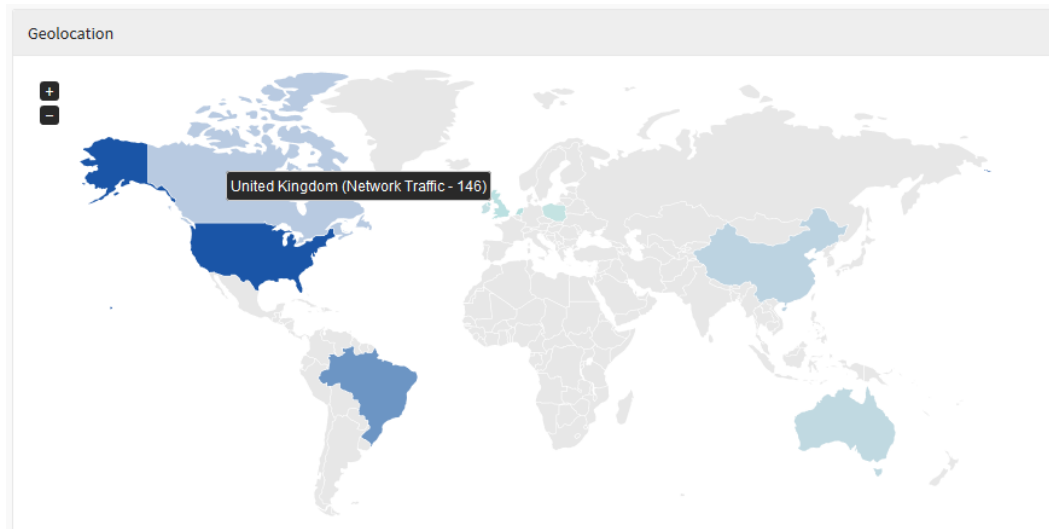
To perform a search, type a term in the search bar and click the **search button** [  ].

Next, we will analyze in detail the components of "Firewall":

- [Geolocation](#);
- [Zone Traffic](#);
- [Top User](#);
- [Top Service](#);
- [Top Source](#);
- [Top Policy](#).

# Firewall – Geolocation

In “Geolocation” the destination of the connections of the network users is displayed, the global map shows in a colored legend the amount of accesses made by the users. When hovering the mouse over the countries a total number of accesses is displayed, in addition, the country referring to this value is highlighted on the map.

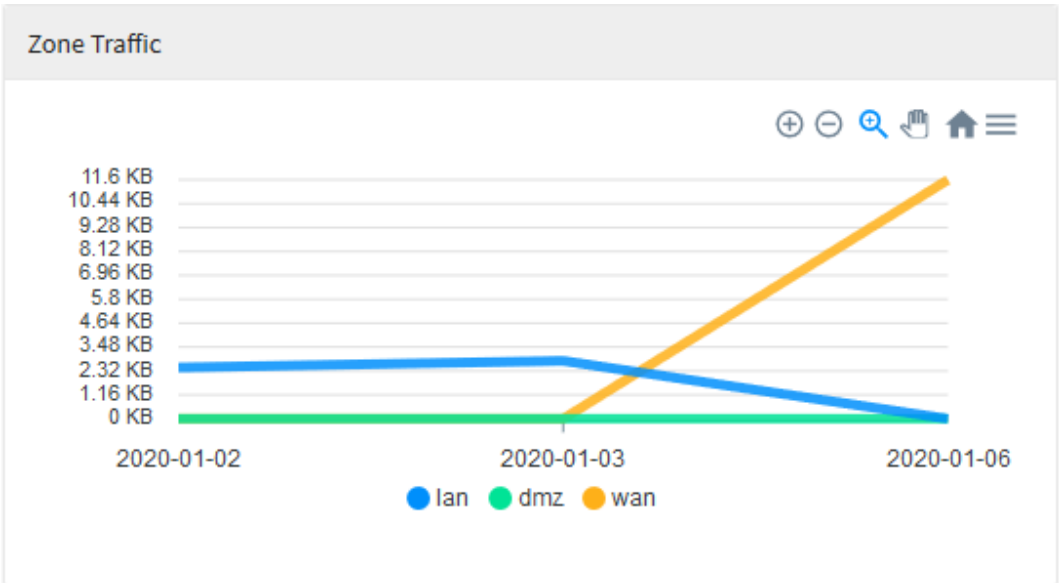


Firewall – Geolocation

# Firewall – Zone Traffic

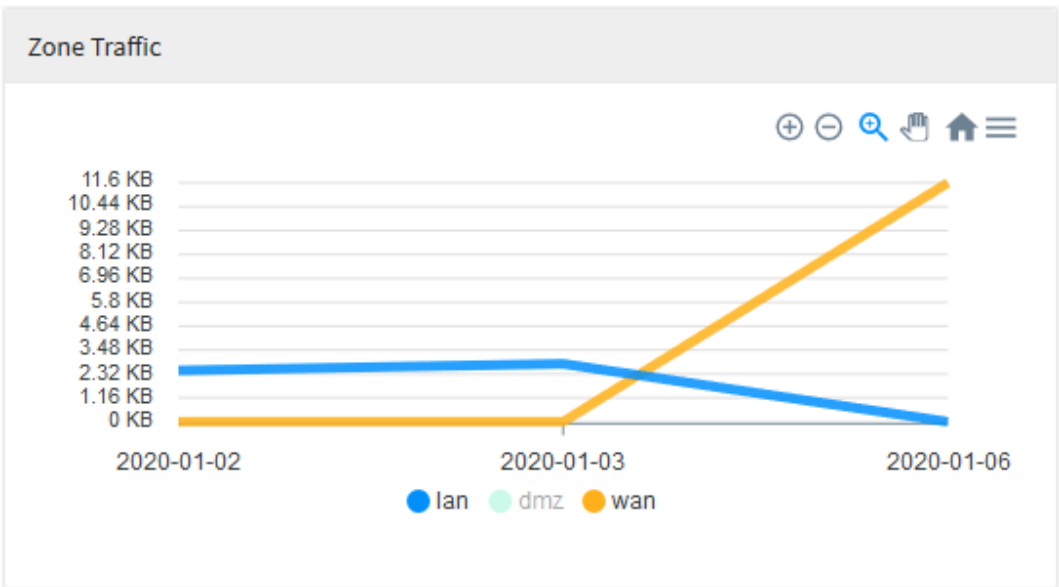
In "Zone Protection" we have a graph showing the amount of traffic in a given zone, through a line graph it is possible to observe these amounts being illustrated over a period of time. When clicking on the type of network used (for example: "LAN", "DMZ", "WAN" and etc.), the diagram is changed in order to display the selected option, which allows to analyze the traffic in more detail according to with the selected dates.

For more information about the navigation menu at the top of this graph check this [page](#).



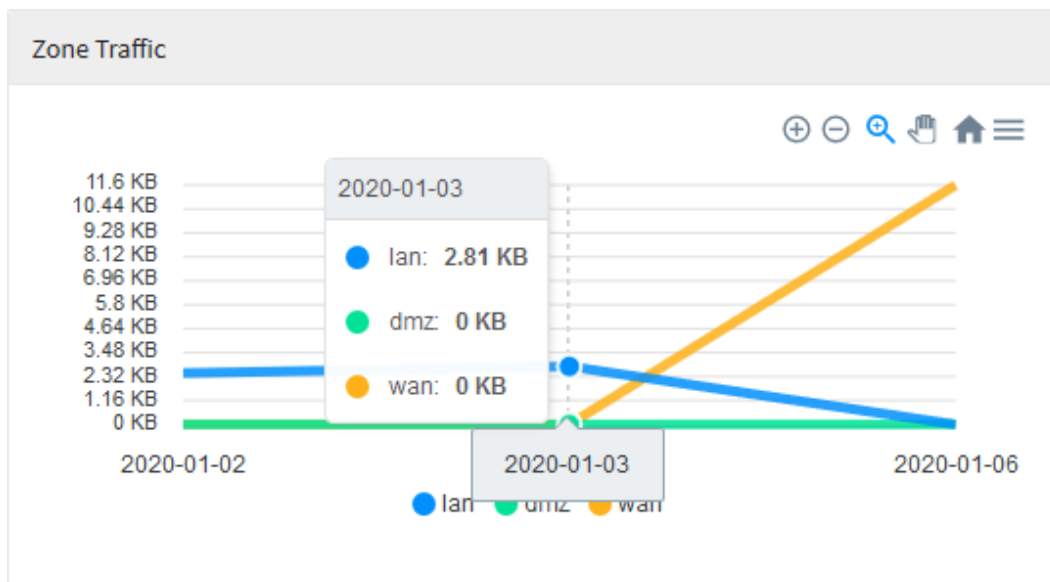
Firewall – Zone Traffic

You can click on the legends below the graph to hide any of the lines in order to illustrate the relevant information, as shown below:



Firewall – Zone Traffic - Hidden DMZ line

When you move your mouse over the graph, a summary of all traffic for the period is displayed, as shown in the image below:



Firewall – Zone Traffic - Summary of results

## Firewall – Top User

In "Top User" there is a diagram showing by date when there was the highest network traffic and a list showing ten users classified by order of use of Gigabytes. When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below. Finally, when you click on one of these users or IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



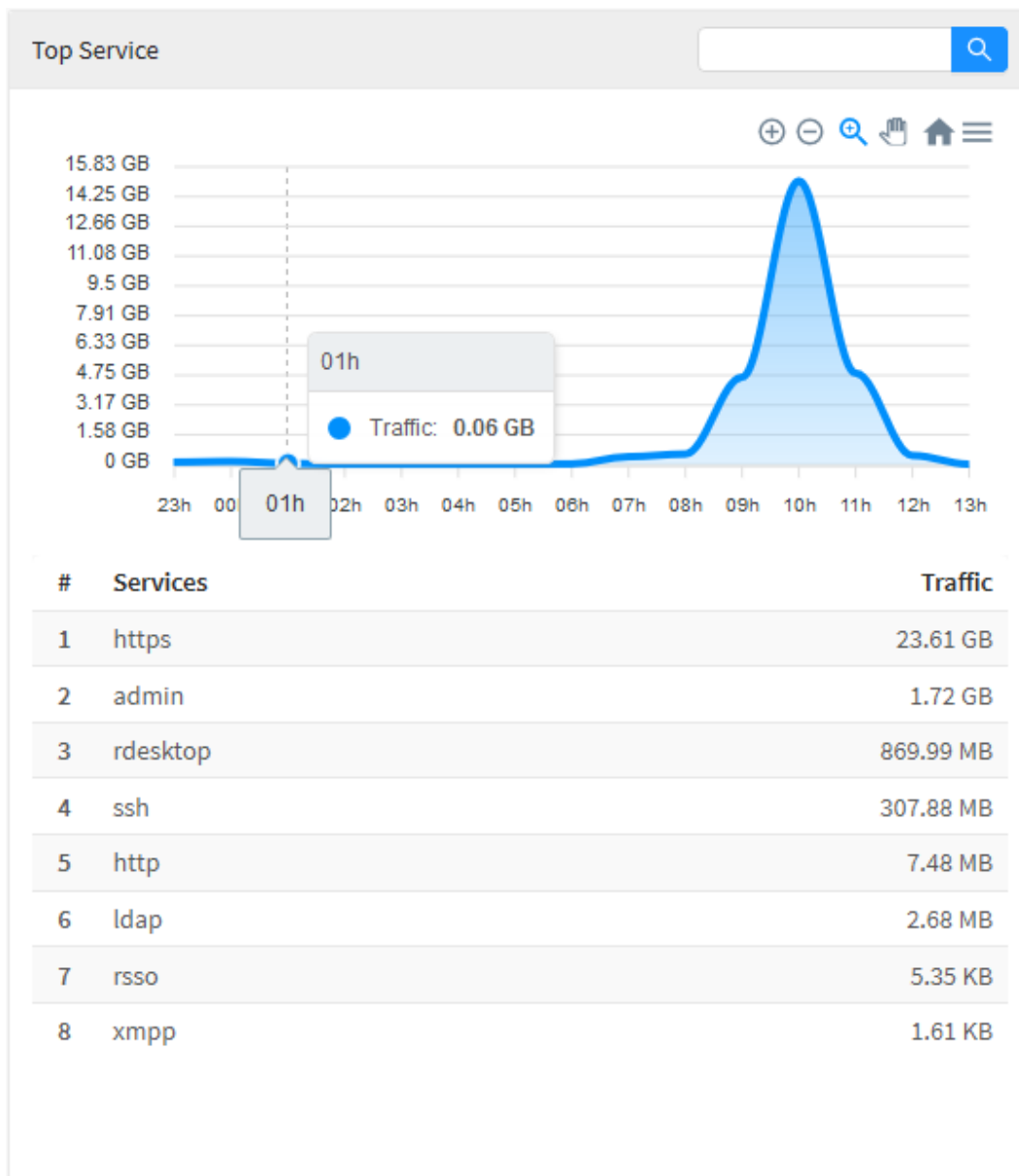
### Firewall – Top User



# Firewall – Top Service

In “Top Service” there is a diagram showing by date when there was more network traffic and a list showing the ten most used types of services, these being classified in order of use of Gigabytes. When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



Firewall - Top Service

# Firewall – Top Source

In “Top Source” there is a diagram showing by date when there was more network traffic and a list showing the ten largest sources of network traffic classified by order of use. When you hover your mouse over the graph, the network traffic for a given period is displayed, as shown in the image below. Finally, when you click on one of these IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected IP.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).

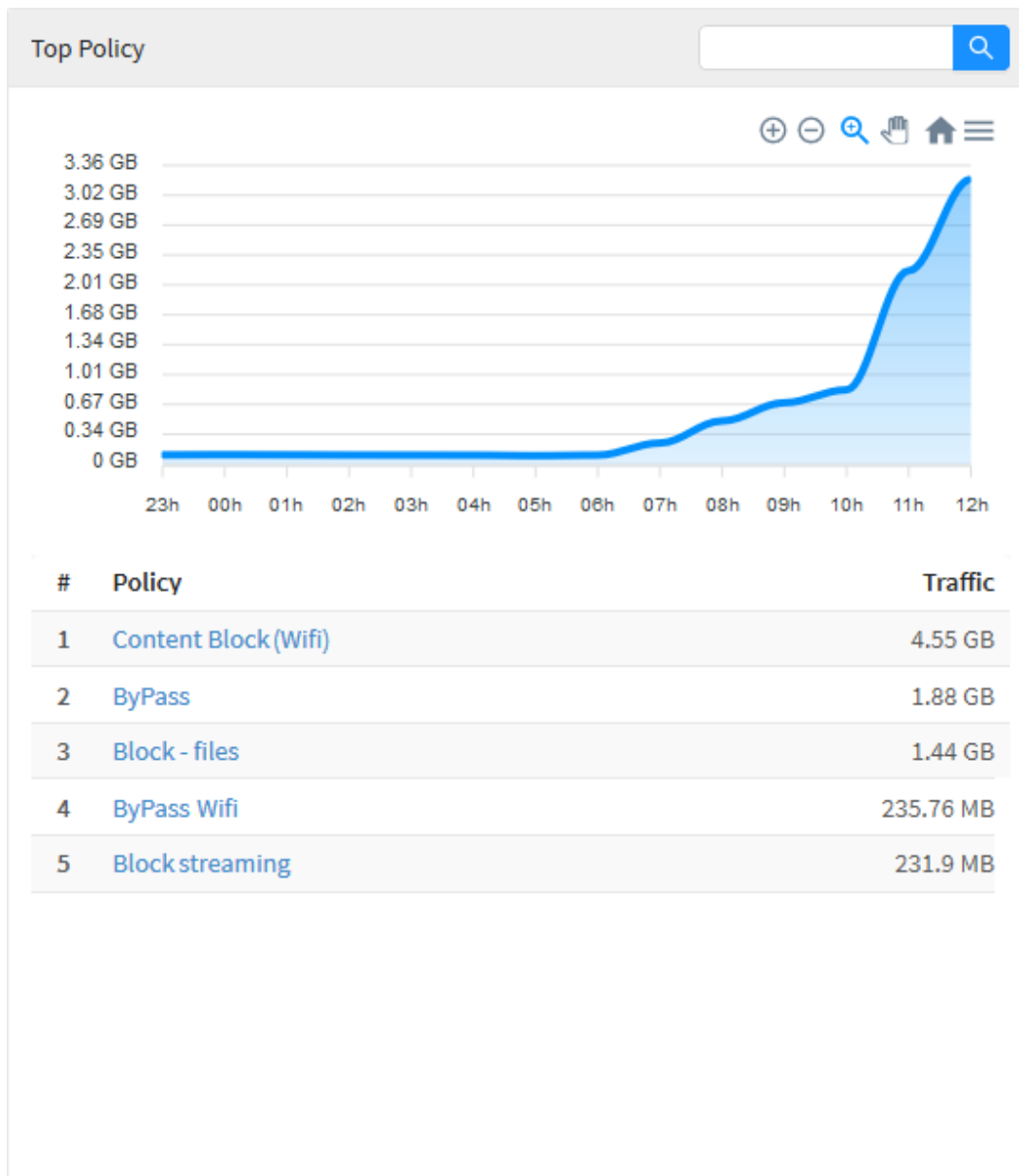


Firewall – Top Source

# Firewall – Top Policy

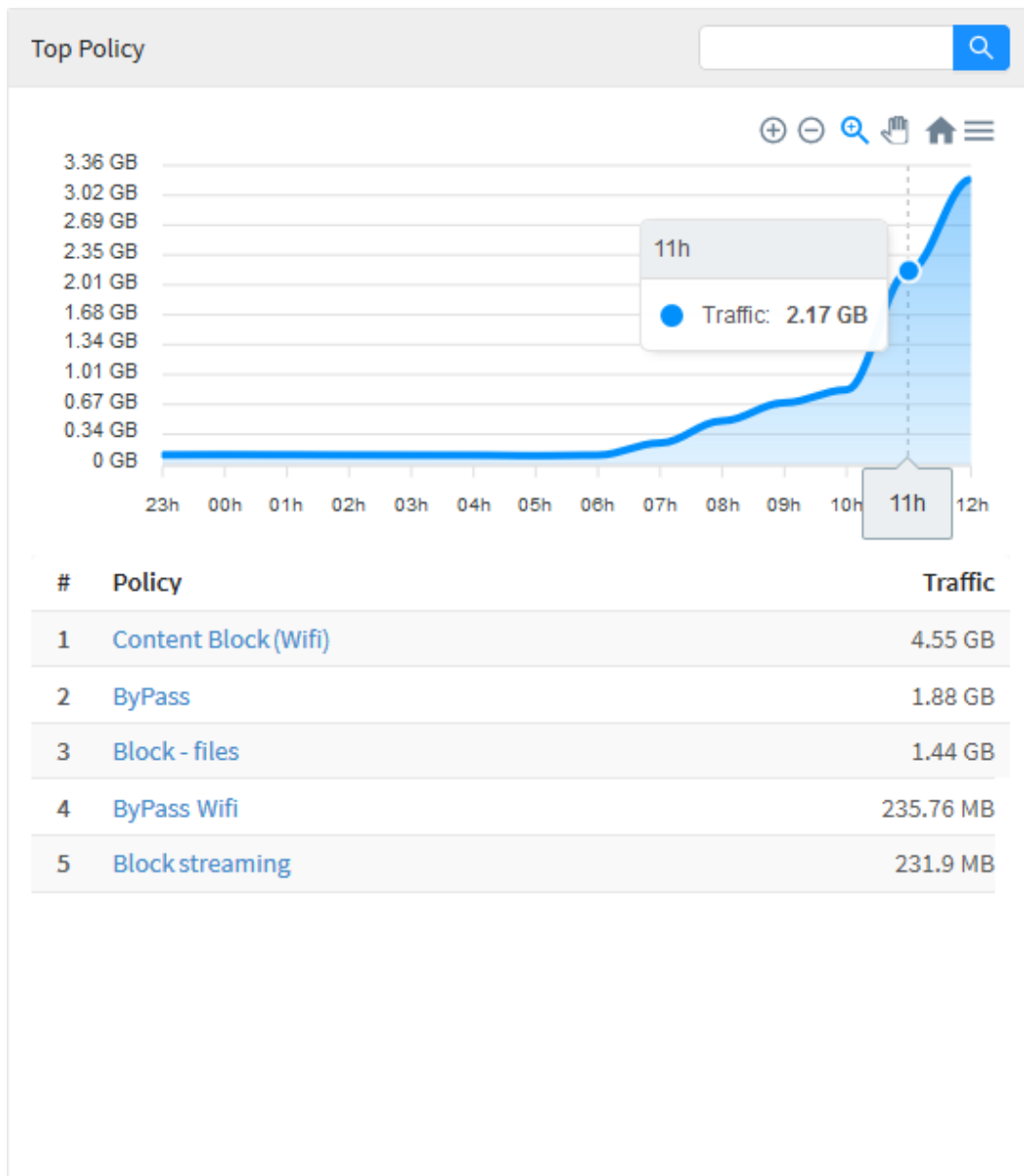
In “Top Policy” there is a diagram showing by date when there was more network traffic and a list showing the ten most used types of policies, which are classified in order of use of Gigabytes.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



Firewall – Top Policy

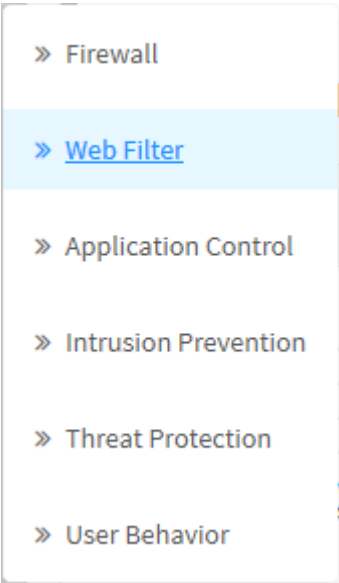
When hovering the mouse over the graph, the network traffic in Gigabytes for a given period is displayed, as shown in the image below.



Firewall – Top Service - Traffic summary for a period

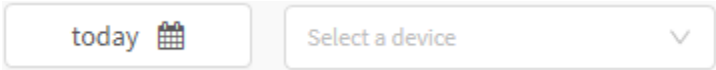
# Web Filter

To access the web filter reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “Web Filter” option.



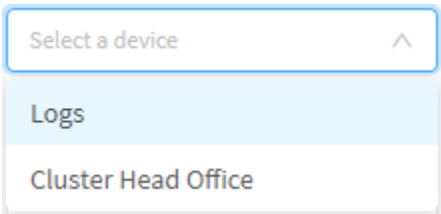
Web Filter

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:



Selection box


In this checkbox will be listed all devices (or groups of devices) previously registered in [Device Manager](#), to create a report, select the desired device.




Selecting Device

Right next to where we just selected the devices, you can see a date selection box, the purpose of which is basically to allow even more accurate results filtering, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.

Today 


Period:

Today 

Cancel

OK

Date Selection

Select the desired date and click on [  ];

## Web Filter

today 📅

Blockbit

Total Traffic

📶 544.35 MB

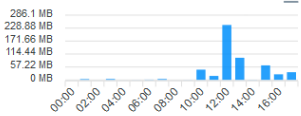
Allowed Sites

✓ 6.528

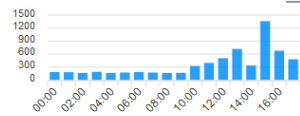
Denied Sites

🚫 87

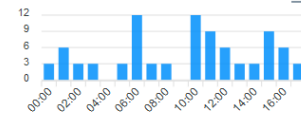
History



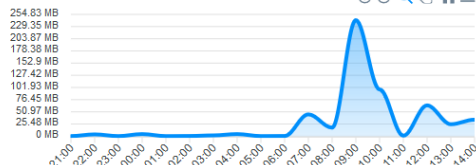
History



History



Users



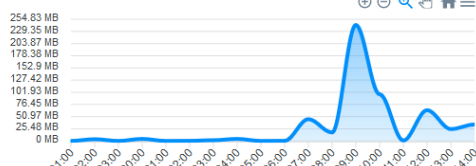
📶 Total Traffic  
544.35 MB

📶 Total Hits  
6.615

Top Users

#	Name	Hits	Traffic
1	172.32.250.24	84	205.75 MB
2	172.32.250.40	1,353	91.02 MB
3	ccsantos@blockbit.com	262	80.51 MB
4	172.32.250.41	139	43.23 MB
5	172.32.250.8	46	39.52 MB
6	172.32.250.99	166	39.18 MB
7	172.32.250.46	351	18.15 MB
8	172.32.250.1	80	12.29 MB
9	doliveira@blockbit.com	166	3.02 MB
10	172.32.250.49	506	2.74 MB

History Profiles



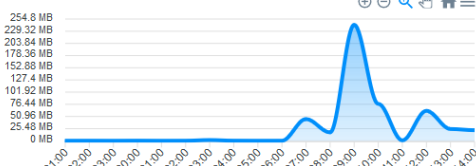
📶 Total Traffic  
544.35 MB

📶 Total Hits  
6.615

Top Profiles

#	Name	Hits	Traffic
1	Content Filtering (Wifi)	3,847	347.06 MB
2	ByPass SSL (Wifi)	2,681	197.29 MB
3	Block - filestreamingservice	87	0 Bytes

History Categories



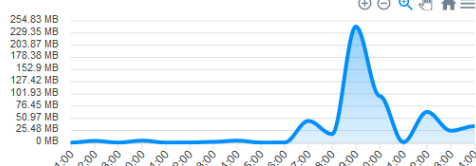
📶 Total Traffic  
497.46 MB

📶 Total Hits  
6.296

Top Categories

#	Name	Hits	Traffic
1	Proxy Avoidance	52	276.34 MB
2	Information Technology	4,375	185.8 MB
3	Streaming Media	17	21.13 MB
4	Restaurants and Dining	93	6.86 MB
5	Business and Economy	190	1.93 MB
6	Government	20	1.56 MB
7	Search Engines and Portals	613	1.04 MB
8	News and Media	12	690.69 KB
9	Travel	7	657.2 KB
10	Freeware and Software Download	626	469.41 KB

History Domains



📶 Total Traffic  
544.35 MB

📶 Total Hits  
6.615

Top Domains

#	Name	Hits	Traffic
1	http://officecdn.microsoft.com.edgesuite.net	526	88.26 MB
2	http://br.archive.ubuntu.com	59	44.11 MB
3	http://e-cdn-proxy-b.deezer.com	7	42.47 MB
4	http://e-cdn-proxy-f.deezer.com	7	40.42 MB
5	http://e-cdn-proxy-a.deezer.com	6	31.51 MB
6	http://e-cdn-proxy-8.deezer.com	4	26.08 MB
7	http://e-cdn-proxy-7.deezer.com	4	25.01 MB
8	http://au.download.windowsupdate.com	63	23.96 MB
9	http://e-cdn-proxy-5.deezer.com	5	22.92 MB
10	http://e-cdn-proxy-4.deezer.com	2	22.06 MB

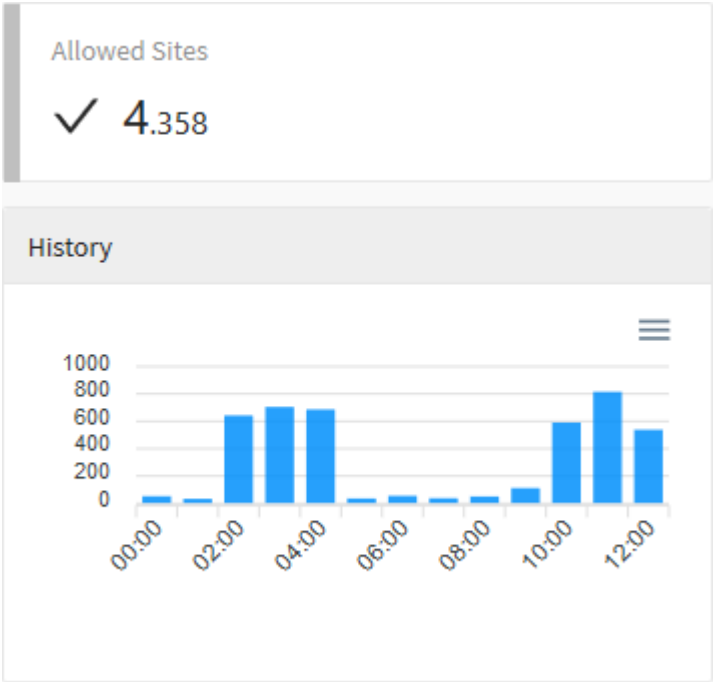




# Web Filter - Allowed Sites and History

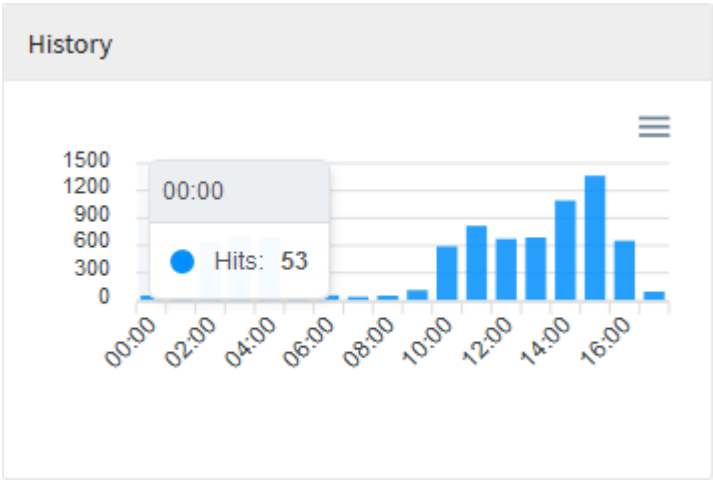
The "Allowed Sites" panel displays a total of pages that have been authorized following the policies. Just below, the history is shown in a bar graph showing the amount of accesses per day.

For more information about the navigation menu at the top of this graph check this [page](#).



Web Filter – Allowed Sites

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

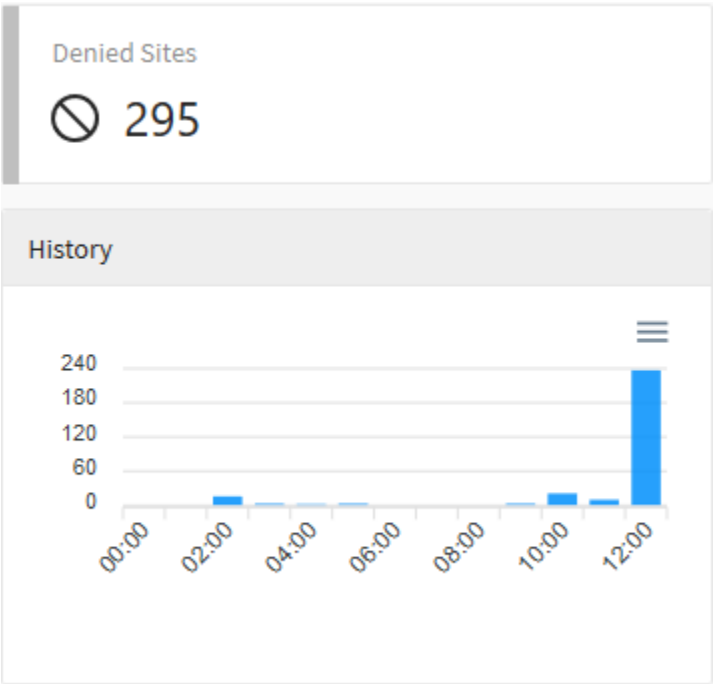


Web Filter – Allowed Sites - Period Summary

# Web Filter - Denied Sites and History

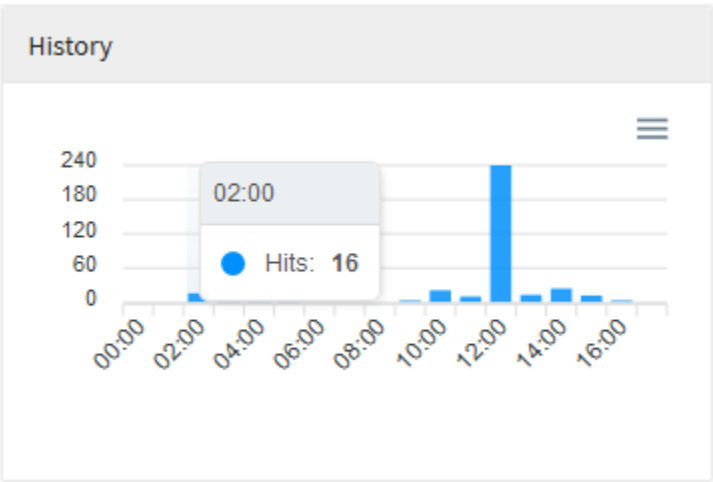
The “Sites Denied” panel shows a sum of all pages that, following the policies, were denied access. Below, the history is shown in a bar graph showing the amount of accesses per day.

For more information about the navigation menu at the top of this graph check this [page](#).



Web Filter – Denied Sites

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

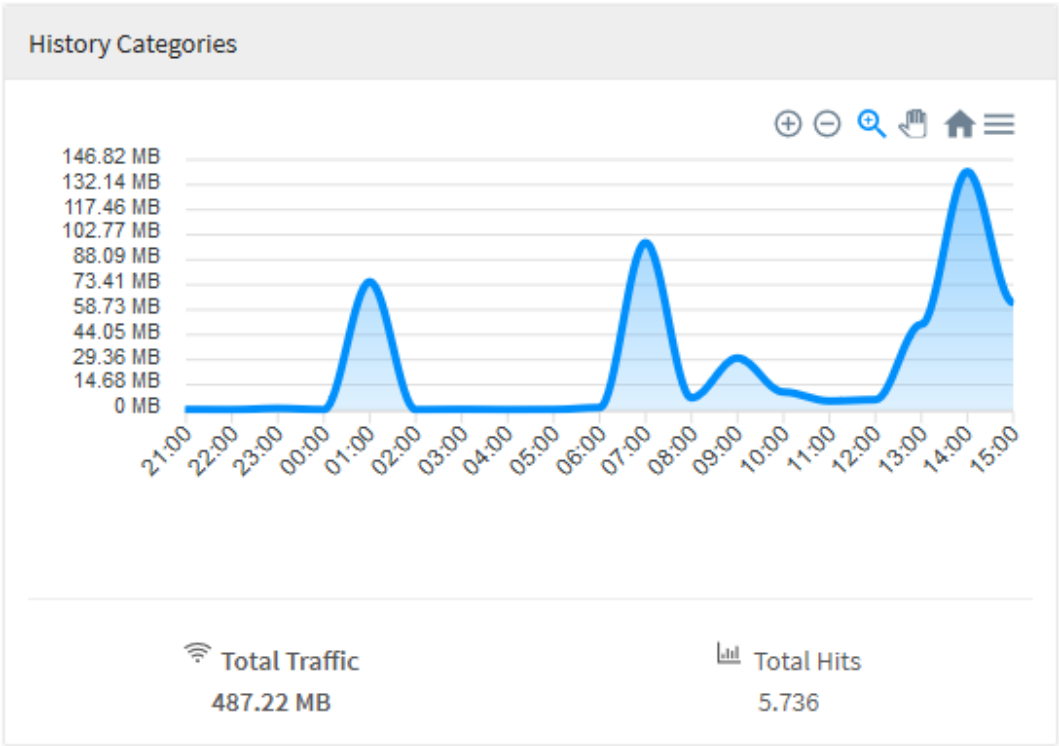


Web Filter – Denied Sites - Period Summary

# Web Filter - History Categories - Total Traffic and Total Hits

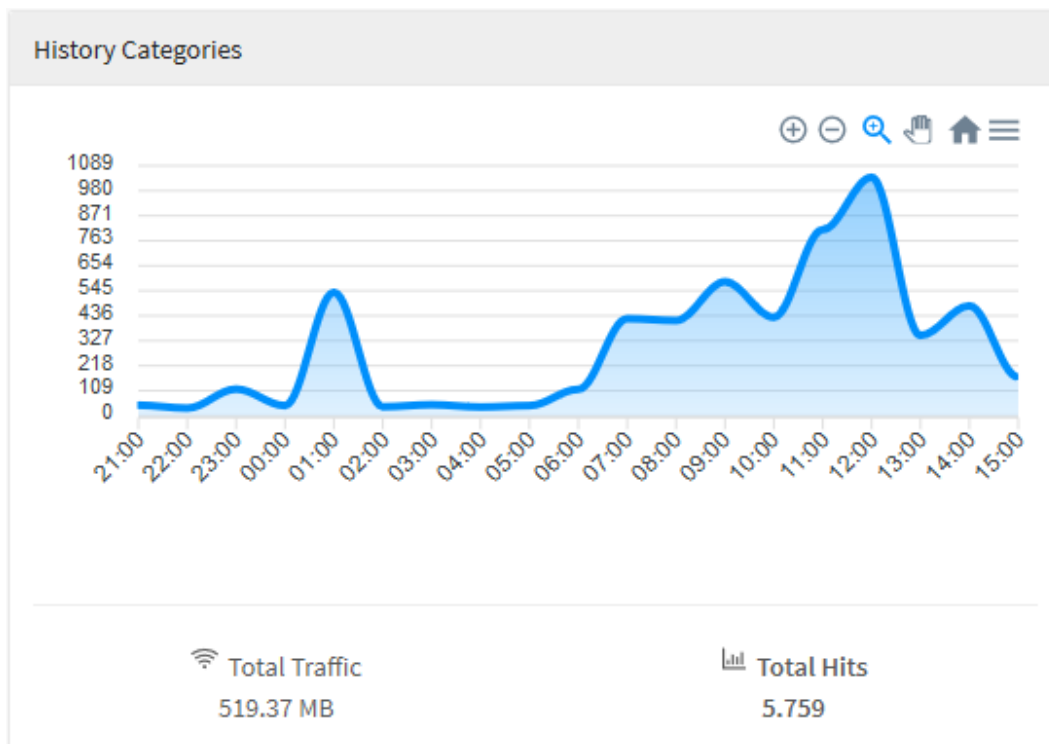
In "History Categories", we have a graph that displays information specifically related to network categories, its function is to demonstrate when some category was applied in one of the accesses. In this area we have "Total Traffic" where the total network traffic in Gigabytes per day and "Total Hits" is displayed, which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this [page](#).



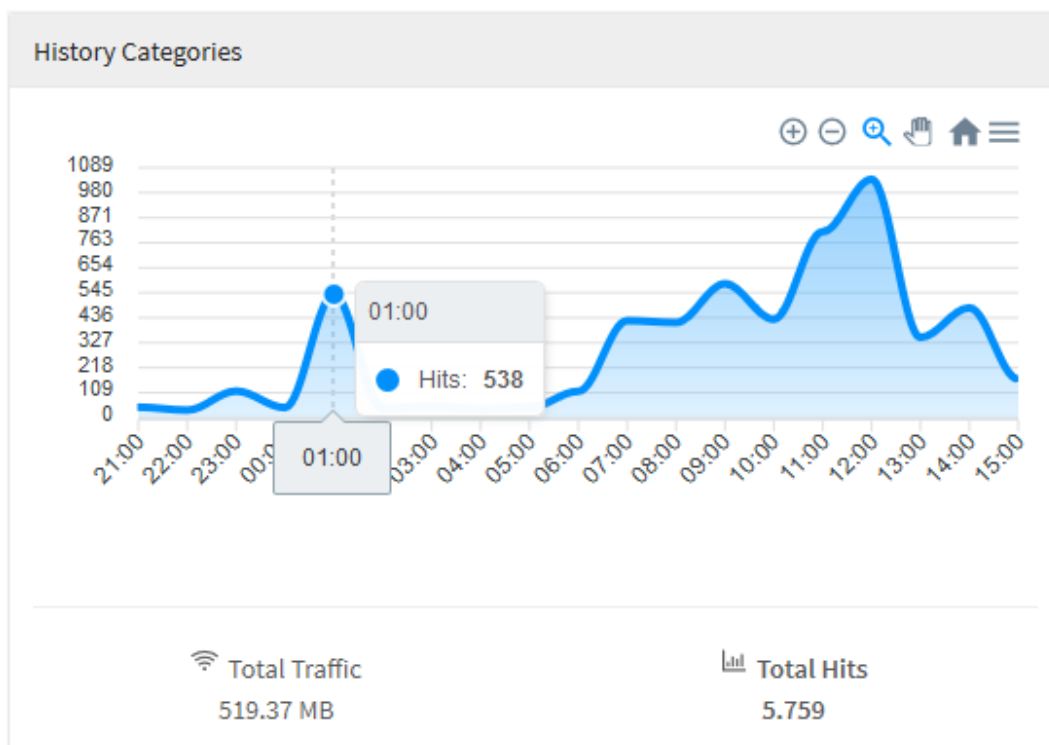
Web Filter – History Categories – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Categories – Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

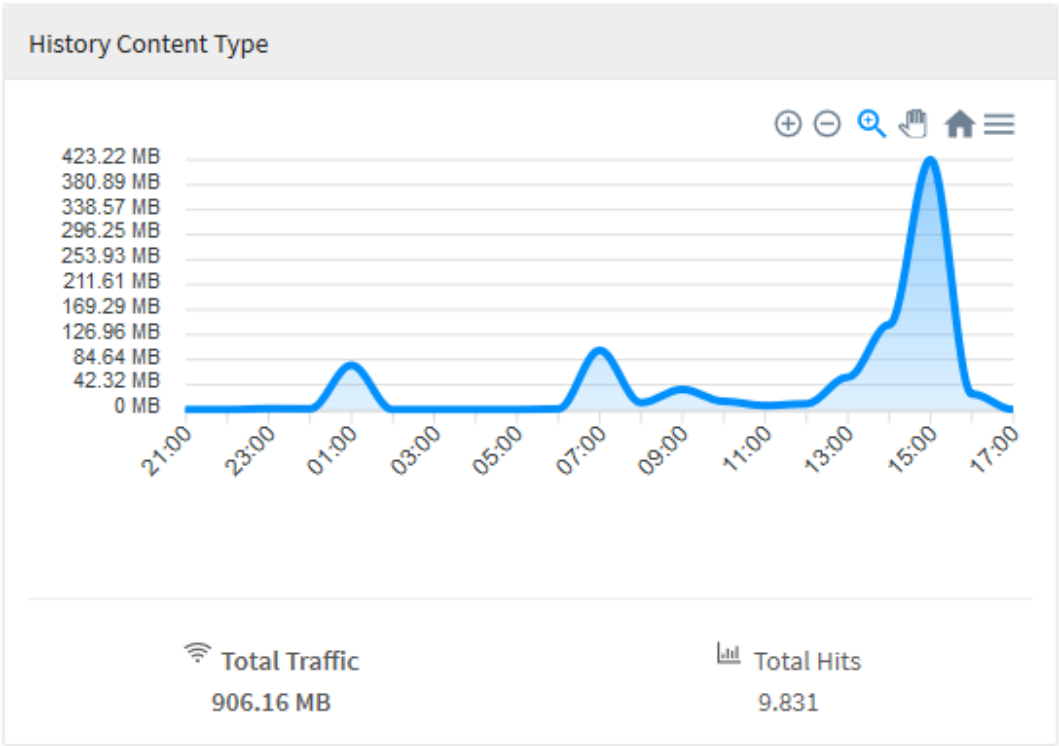


Web Filter – History Categories – Period summary

# Web Filter - History Content Types - Total Traffic and Total Hits

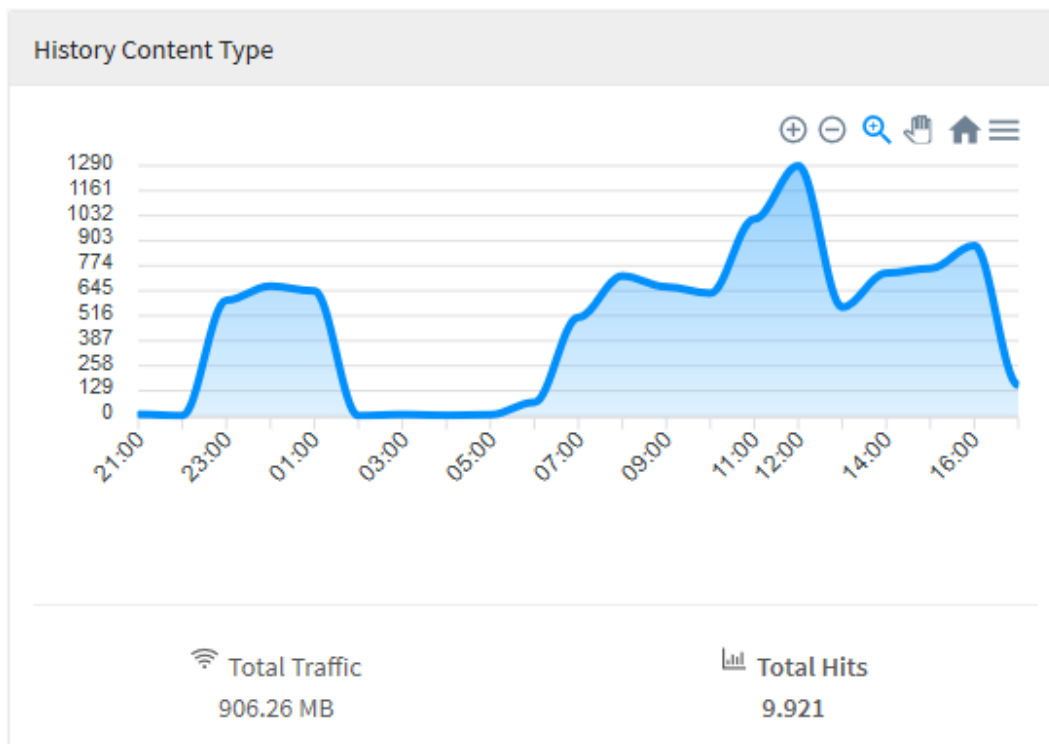
In "Content Type", we have a graphic whose function is to demonstrate when some type of content was accessed. In this area we have "Total Traffic" where the total network traffic in Gigabytes per day and "Total Hits" is displayed, which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph, check this [page](#).



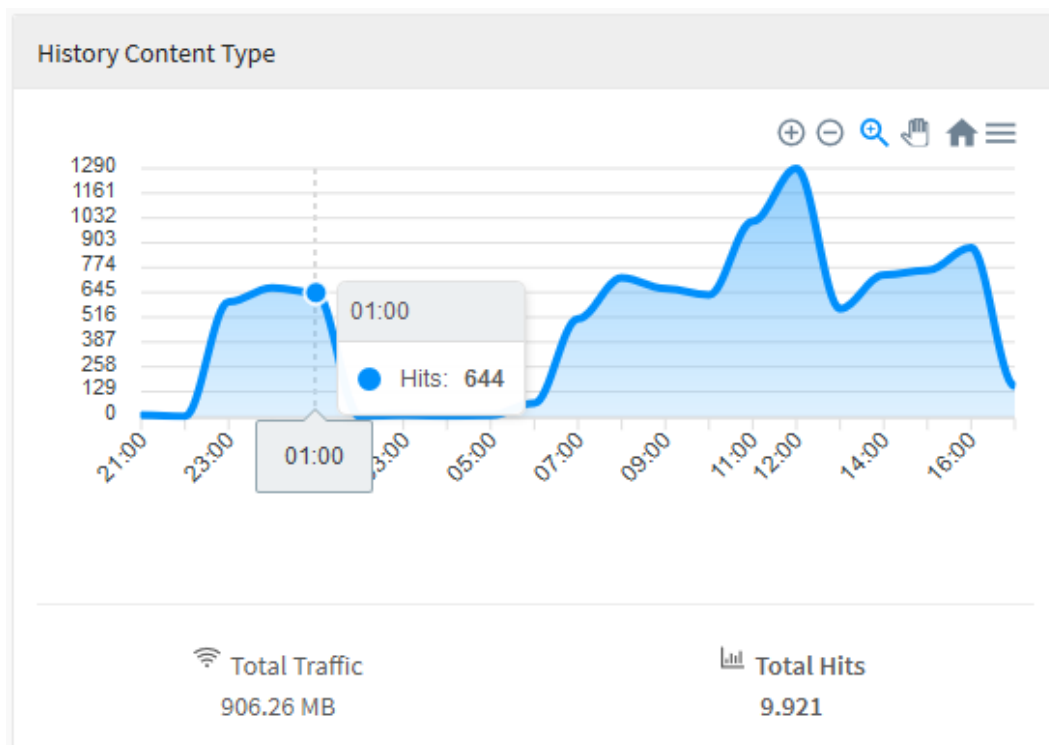
Web Filter – History Content Type – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Content Type – Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

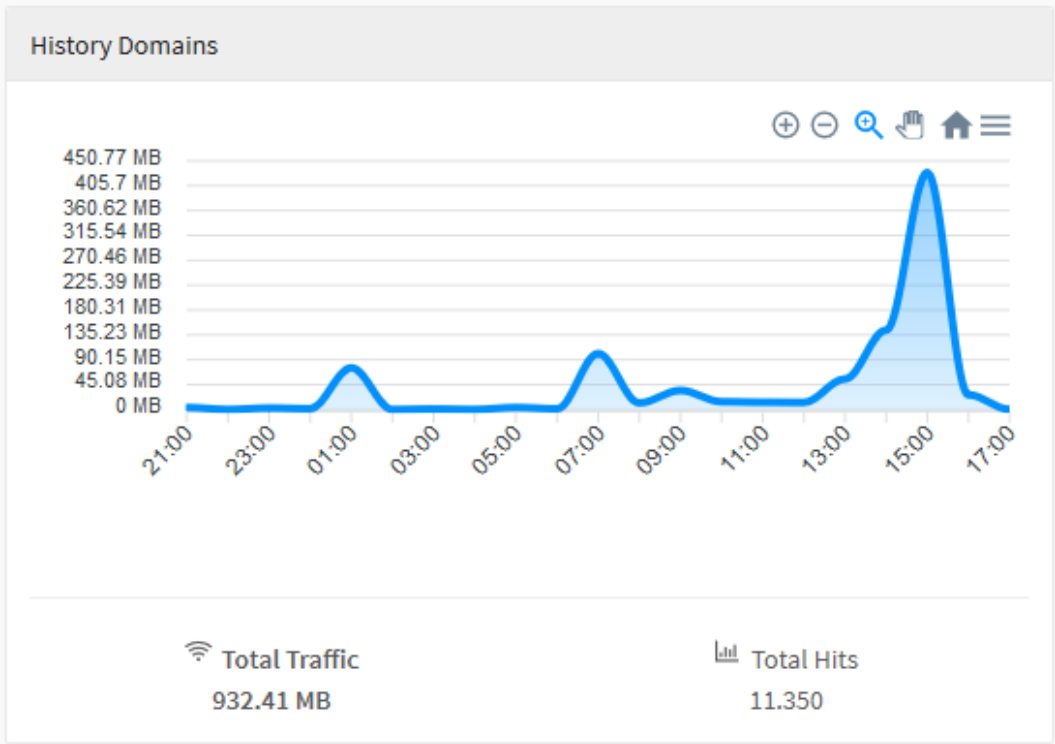


Web Filter – History Content Type - Period Summary

# Web Filter - History Domains - Total Traffic and Total Hits

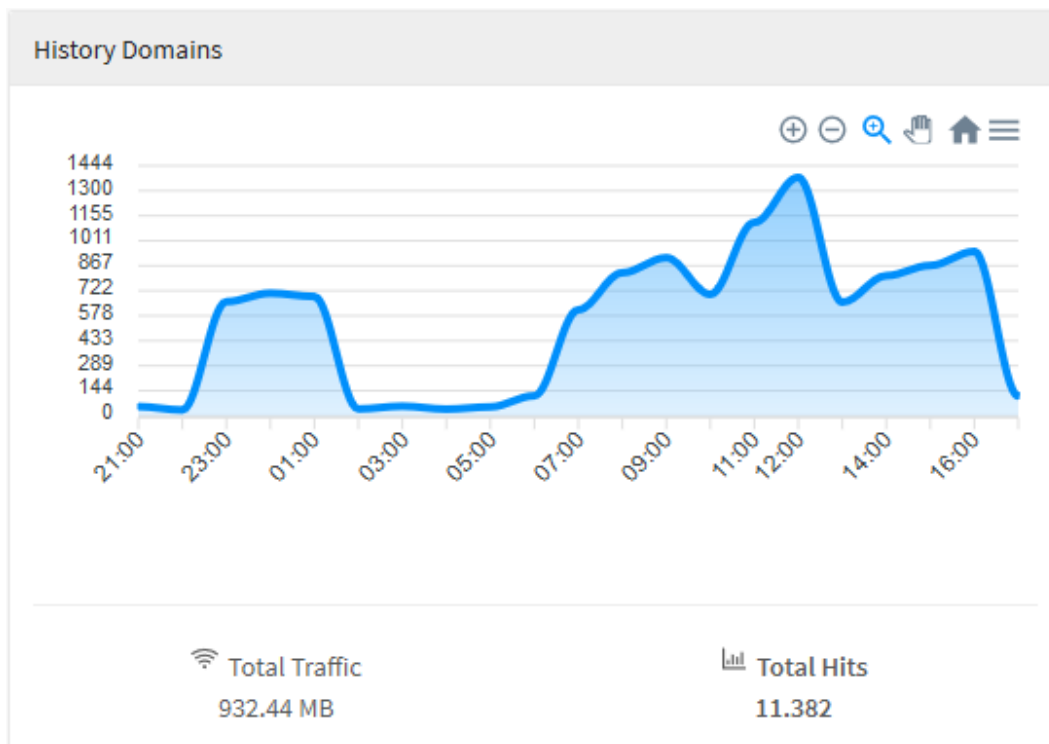
In "History Domains", we have a graph that displays information specifically related to domain access, its function is to demonstrate when a domain has been accessed. In this area we have "Total Traffic" where the total traffic in Gigabytes per day and "Total Hits" is displayed, which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph check this [page](#).



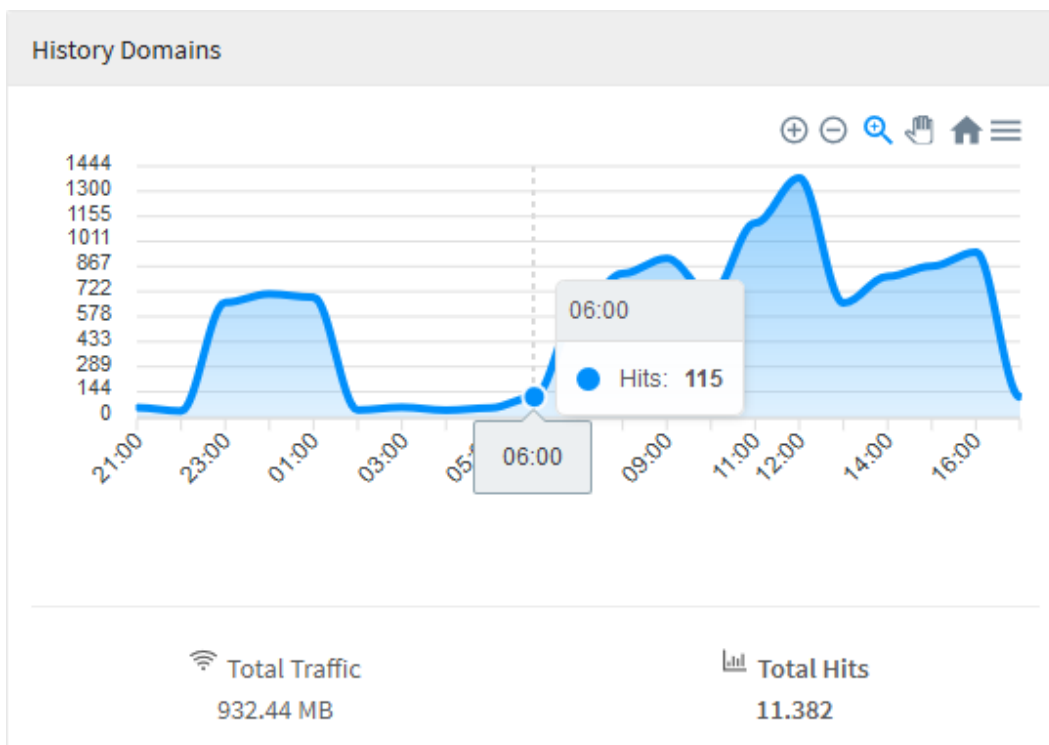
Web Filter - History Domains - Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter - History Domains - Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



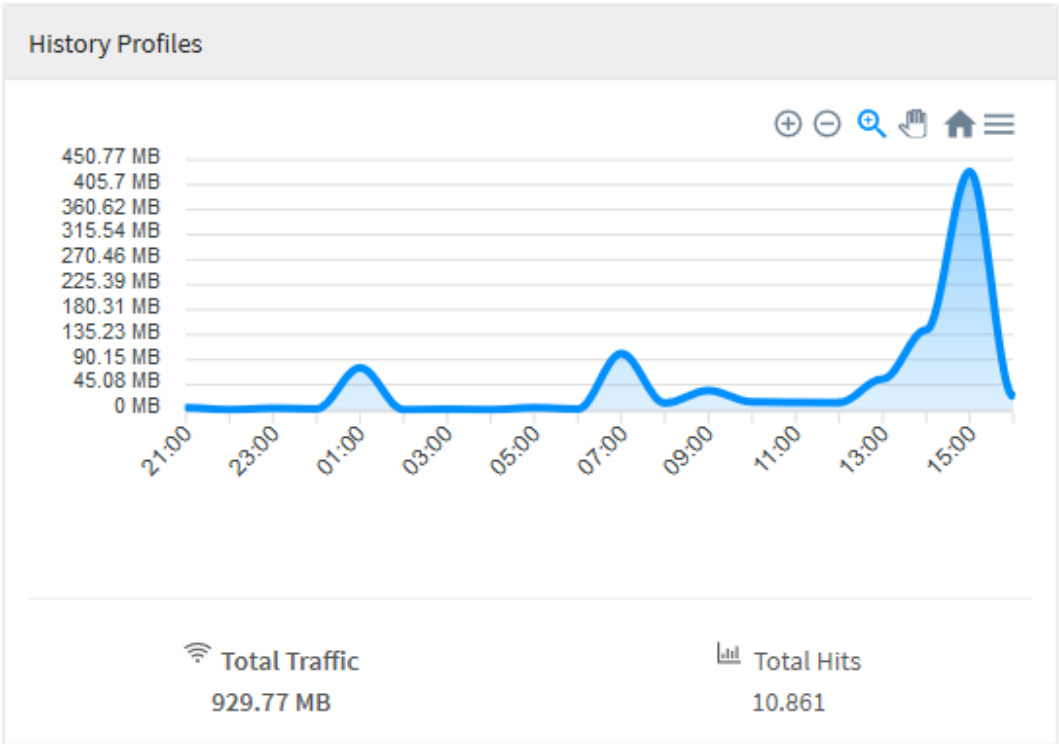
Web Filter - History Domains - Period Summary



# Web Filter - History Profiles - Total Traffic and Total Hits

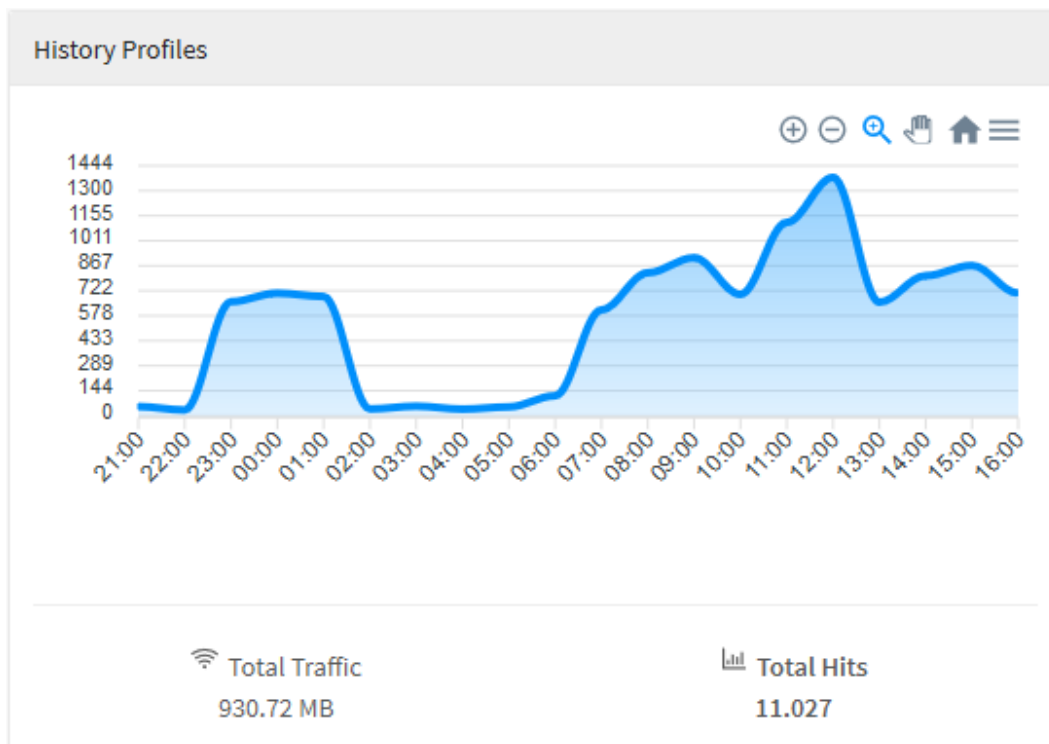
In "History Profiles", we have a graph that displays information specifically related to the [profiles](#) of the network, its function is to demonstrate when some profile was used in an access. In this area we have "Total Traffic" where the total network traffic in Gigabytes per day and "Total Hits" is displayed, which shows the total accesses for each of the days surveyed.

For more information about the navigation menu at the top of this graph check this [page](#).



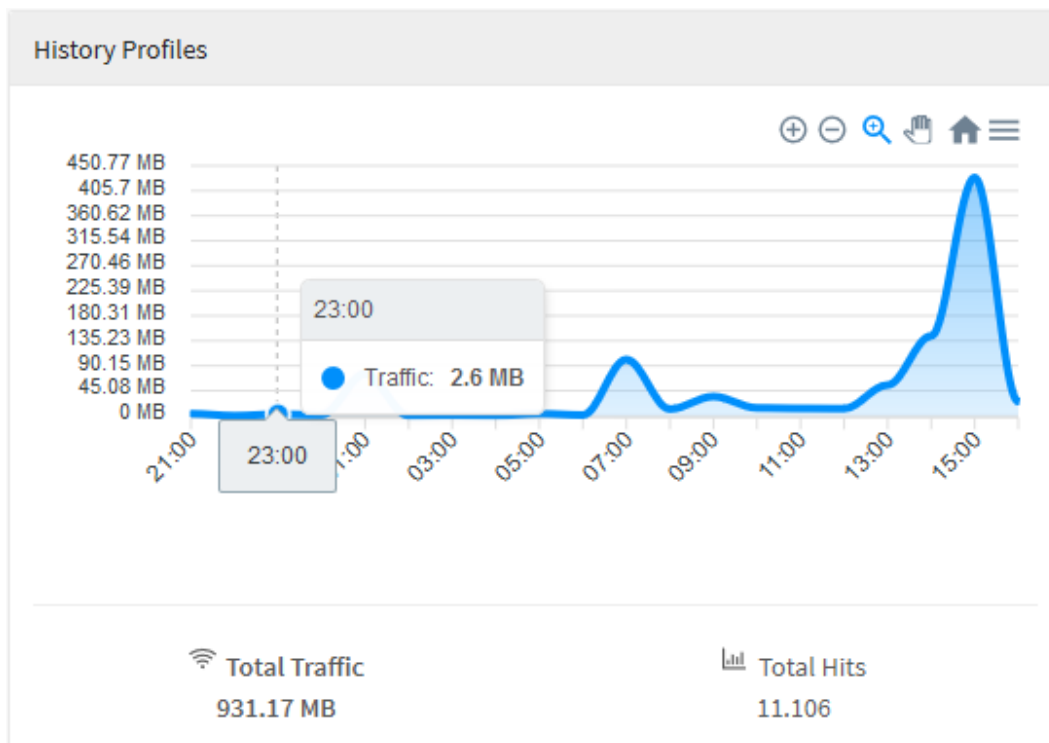
Web Filter – History Profiles – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – History Profiles – Total Hits

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



Web Filter – History Profiles – Resumo do Período

# Web Filter - Top Categories

In the "Top Categories" list, we have a list of the names of the ten categories classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when clicking on one of these users or IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more precise view regarding the selected category.

For more information about the search bar at the top of this graph, check this [page](#).

Top Categories			
#	Name	Hits	Traffic
1	<a href="#">Information Technology</a>	3.089	217.74 MB
2	<a href="#">Proxy Avoidance</a>	11	49.65 MB
3	<a href="#">Government</a>	1.162	6.91 MB
4	<a href="#">Travel</a>	24	6.59 MB
5	<a href="#">Restaurants and Dining</a>	101	2.17 MB
6	<a href="#">Search Engines and Portals</a>	443	529.06 KB
7	<a href="#">Web Hosting</a>	51	350.16 KB
8	<a href="#">Freeware and Software Download</a>	83	210.24 KB
9	<a href="#">Computer Security</a>	25	114.67 KB
10	<a href="#">Internet Communication</a>	3	74.58 KB

Web Filter – Top Categories

## Web Filter - Top Content Type

In the "Top Content Type" list, we have a list of the names of the ten most accessed content types classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when you click on one of these users or IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of these types of content.

For more information about the navigation menu at the top of this graph check this [page](#).

Top Content Type			
#	Name	Hits	Traffic
1	<a href="#">application/vnd.ms-cab-compressed</a>	823	109.73 MB
2	<a href="#">application/octet-stream</a>	391	106.39 MB
3	<a href="#">audio/mpeg</a>	4	49.63 MB
4	<a href="#">image/png</a>	1.658	27.34 MB
5	<a href="#">image/jpeg</a>	140	4.42 MB
6	<a href="#">text/css</a>	732	3.52 MB
7	<a href="#">application/json</a>	822	1.96 MB
8	<a href="#">text/xml</a>	451	1.87 MB
9	<a href="#">text/javascript</a>	337	1.53 MB
10	<a href="#">text/html</a>	246	1.34 MB

*Top Content Type*

# Web Filter - Top Domains

In the "Top Domains" list, we have a list of the names of the ten domains classified in order of the highest amount of accesses and their respective traffic in Megabytes. Finally, when you click on one of these addresses, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected domain.

For more information about the search bar at the top of this graph check this [page](#).

Top Domains			
#	Name	Hits	Traffic
1	<a href="http://au.download.windowsupdate.com">http://au.download.windowsupdate.com</a>	755	195.12 MB
2	<a href="http://e-cdn-proxy-e.deezer.com">http://e-cdn-proxy-e.deezer.com</a>	8	87.59 MB
3	<a href="http://e-cdn-proxy-8.deezer.com">http://e-cdn-proxy-8.deezer.com</a>	6	74.95 MB
4	<a href="http://e-cdn-proxy-9.deezer.com">http://e-cdn-proxy-9.deezer.com</a>	9	73.39 MB
5	<a href="http://e-cdn-proxy-1.deezer.com">http://e-cdn-proxy-1.deezer.com</a>	5	59.74 MB
6	<a href="http://e-cdn-proxy-7.deezer.com">http://e-cdn-proxy-7.deezer.com</a>	5	46.12 MB
7	<a href="http://e-cdn-proxy-3.deezer.com">http://e-cdn-proxy-3.deezer.com</a>	4	41.29 MB
8	<a href="http://e-cdn-proxy-a.deezer.com">http://e-cdn-proxy-a.deezer.com</a>	4	41.05 MB
9	<a href="http://rss.utech.com.br">http://rss.utech.com.br</a>	2.742	38.83 MB
10	<a href="http://e-cdn-proxy-f.deezer.com">http://e-cdn-proxy-f.deezer.com</a>	3	33.24 MB

Web Filter – Top Domains

# Web Filter - Top Domains by Time

In the “Top Domains by Time”, list, one sees the top ten accessed domains, classified by order of the highest amount of traffic time in a domain.

Top Domains by time		
#	Domain	Time
1	https://edge.microsoft.com	58s
2	https://umwatson.events.data.microsoft.com	36s
3	https://www.bing.com	18s
4	http://ctldl.windowsupdate.com	14s
5	http://x1.c.lencr.org	10s
6	https://login.live.com	8s
7	https://slscr.update.microsoft.com	8s
8	https://msedge.api.cdp.microsoft.com	6s
9	https://config.edge.skype.com	5s
10	https://update.googleapis.com	4s

Top Domains by Time

Finally, when clicking in one of these domains ou IPs, one will be redirected to [Events](#) using the selected item as a filter, thus creating, a better detailed report enabling a precise view on these contents.

Events

NGFW - 2.4.0 - 172.23.31.14

logtype="web"

Query Editor

Log Analysis

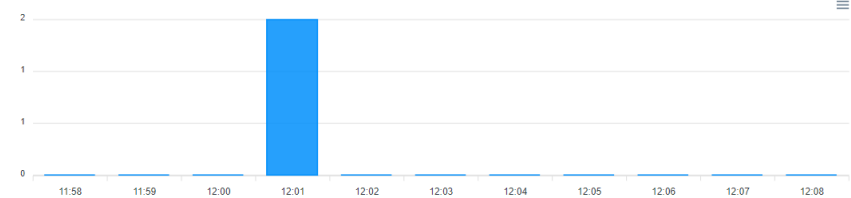
Top Hits

src

179.30.0.10

2 hits

History Hits



Date	User	Source	Destination	Device	Service	Log type	Action
2023-01-31 12:01:54	-	179.30.0.10:55649	192.16.48.200:80	eth1 - default	http	webfilter	allow
2023-01-31 12:01:54	-	179.30.0.10:55649	192.16.48.200:80	eth1 - default	http	webfilter	allow



First

Previous

Page 1

Next

Events - Sessions

Clicking on [  or  ] is possible to verify detailed information in the selected item. Search for "surfing time" information to verify the browsing time.

# Information

⊕ date ⊖ 2023-01-31 12:01:54	⊕ client_mac ⊖ 00:0c:29:29:ba:cd	⊕ proto ⊖ tcp	⊕ host ⊖ utmviola23-14	⊕ web_url ⊖ http://ctldl.windowsupdate.com/msdown load/update/v3/static/trustedr/en/pinrule sstl.cab?3d9830fd6545...	⊕ web_site ⊖ http://ctldl.windowsupdate.com/msdown load/update/v3/static/trustedr/en
⊕ logtype ⊖ web	⊕ dst ⊖ 192.16.48.200	⊕ service ⊖ http	⊕ client_ip ⊖ 179.30.0.10		
⊕ sessid ⊖ 1A0ADF6C286FE0AB30A2683E7B639F38	⊕ dport ⊖ 80	⊕ devout ⊖ default	⊕ web_method ⊖ GET	⊕ web_referer ⊖ -	
⊕ src ⊖ 179.30.0.10	⊕ devin ⊖ eth1	⊕ rule_action ⊖ allow	⊕ web_profile ⊖ Ética de Segurança	⊕ web_agent ⊖ Microsoft-CryptoAPI/10.0	
⊕ sport ⊖ 55649	⊕ zonein ⊖ LAN	⊕ web_mime ⊖ application/octet-stream	⊕ surfing_time ⊖ 1	⊕ bytes ⊖ 0	⊕ web_protocol ⊖ HTTP



Events - Sessions - [ ] Information

## Event View



```

{
  "Event Information": {
    "date": "2023-01-31T12:01:54"
    "logtype": "web"
    "sessid": "1A0ADF6C286FE0AB30A2683E7B639F38"
    "src": "179.30.0.10"
    "sport": "55649"
    "client_mac": "00:0c:29:29:ba:cd"
    "dst": "192.16.48.200"
    "dport": "80"
    "devin": "eth1"
    "zonein": "LAN"
    "proto": "tcp"
    "service": "http"
    "devout": "default"
    "rule_action": "allow"
    "web_mime": "application/octet-stream"
    "host": "utmviola23-14"

    "client_ip": "179.30.0.10"
    "web_category": "Search Engines and Portals"
    "web_method": "GET"
    "web_profile": "Ética de Segurança"
    "surfing_time": 1
    "web_url":
    "http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?3d9830fd6545fd8"
    "web_referer": "-"
    "web_agent": "Microsoft-CryptoAPI/10.0"
    "bytes": "0"
    "web_protocol": "HTTP"
    "web_site": "http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en"
  }
}

```

Cancel



Events - Sessions - [ ] Event View

# Web Filter - Top Profiles

In the "Top Profiles" list, we have a list of the ten most used [profiles](#) classified in order of the highest amount of accesses and their respective usage in Gigabytes

Finally, when you click on one of these profiles, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected profile.

For more information about the search bar at the top of this graph, check this [page](#).

Top Profiles			
#	Name	Hits	Traffic
1	<a href="#">Content Filtering (Wifi)</a>	7.894	688.31 MB
2	<a href="#">ByPass SSL (Wifi)</a>	2.590	241.46 MB
3	<a href="#">Block - filestreamingservice</a>	377	0 Bytes

Web Filter – Top Profiles



## Web Filter - Top Users

As with the other “Top Users” lists, in Web Filter we have a list of ten users classified in order of the highest amount of accesses and their respective usage in Gigabytes. Finally, when you click on one of these users or IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

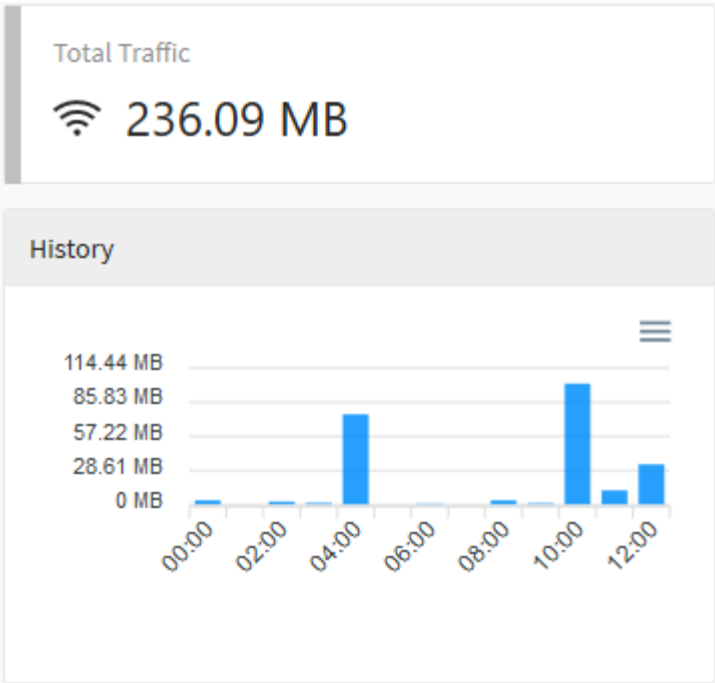
For more information about the search bar at the top of this graph check this [page](#).

Top Users			
#	Name	Hits	Traffic
1	<a href="#">172.32.250.40</a>	762	131.6 MB
2	<a href="#">172.32.250.99</a>	285	98.94 MB
3	<a href="#">doliveira@blockbit.com</a>	1.696	21.28 MB
4	<a href="#">pisantos@blockbit.com</a>	243	20.21 MB
5	<a href="#">172.32.250.46</a>	405	18.68 MB
6	<a href="#">172.32.250.5</a>	553	7.5 MB
7	<a href="#">172.32.250.49</a>	1.461	7.26 MB
8	<a href="#">dsousa@blockbit.com</a>	310	5.43 MB
9	<a href="#">172.32.250.53</a>	67	4.83 MB
10	<a href="#">172.32.250.47</a>	181	4.66 MB

Web Filter – Top Users

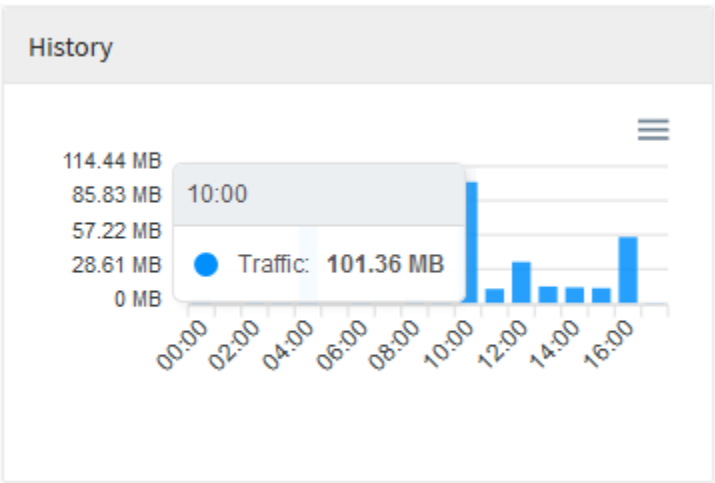
# Web Filter - Total Traffic and History

The "Total Traffic" panel shows the total amount of traffic in Megabytes. Just below, the history is displayed in a bar graph showing the amount of Megabytes trafficked per day.



Web Filter – Total Traffic

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

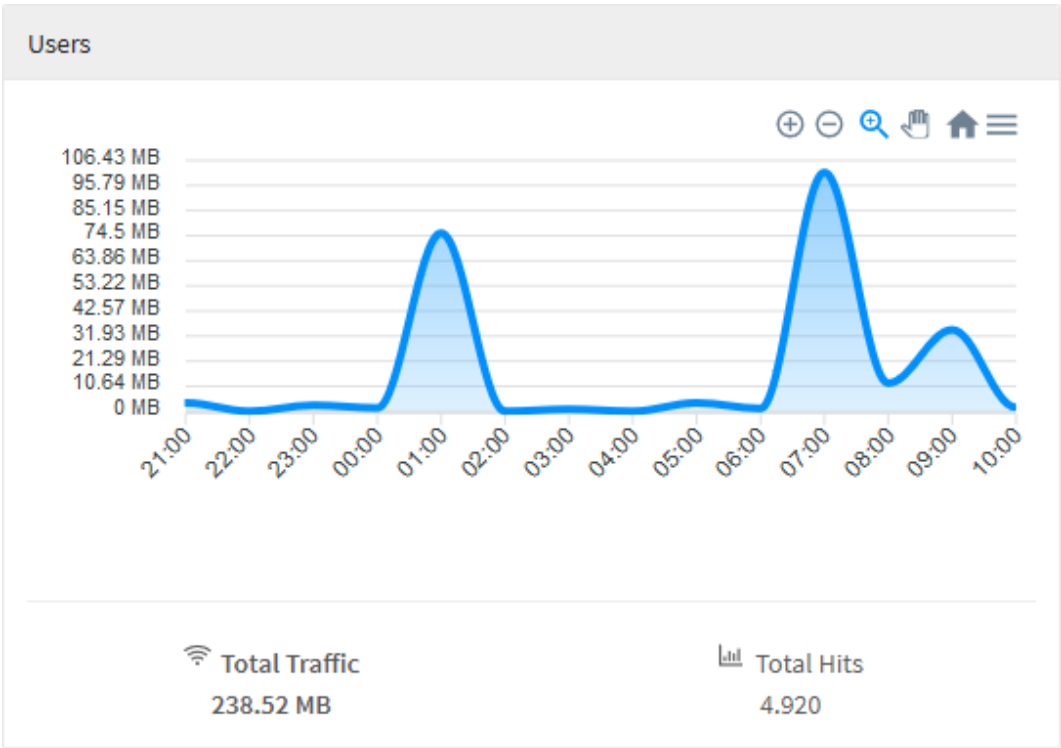


Web Filter – Total Traffic - Period summary

# Web Filter - Users - Total Traffic and Total Hits

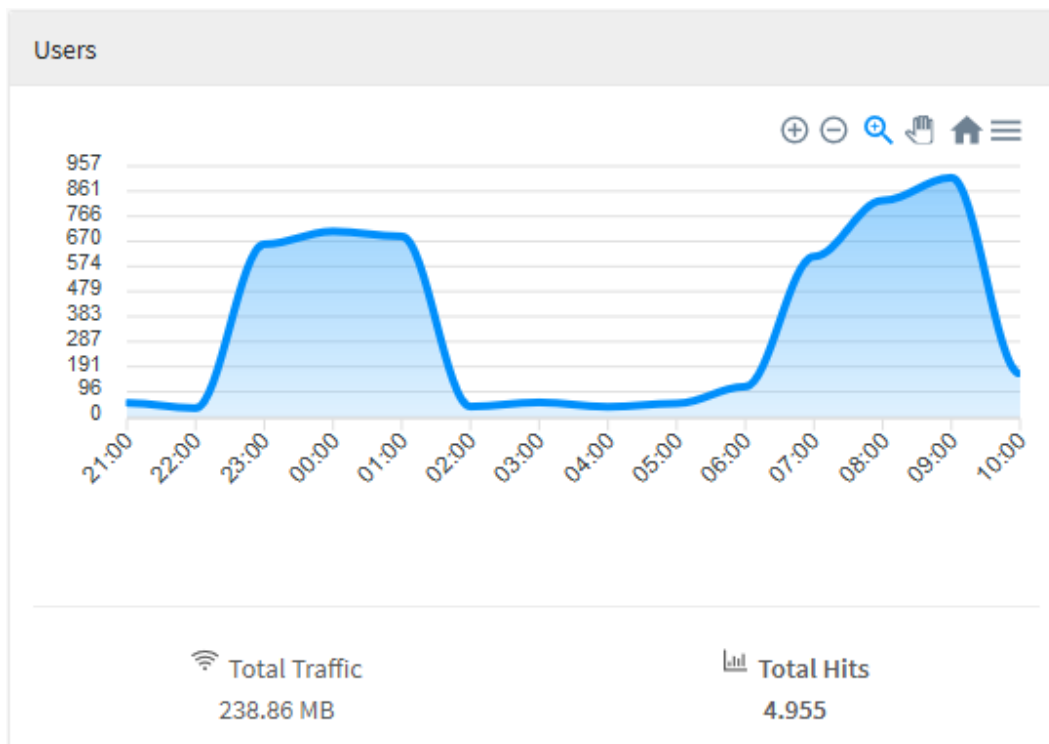
Just below the panels previously described, on the left side of the screen we have the graphic arranged in "Users", which displays information specifically related to the network consumption by users: In it we have "Total Traffic" where the total network traffic is displayed in Megabytes per day and "Total Hits" which shows the total number of hits for each of the days surveyed.

For more information about the navigation menu at the top of this graph check this [page](#).



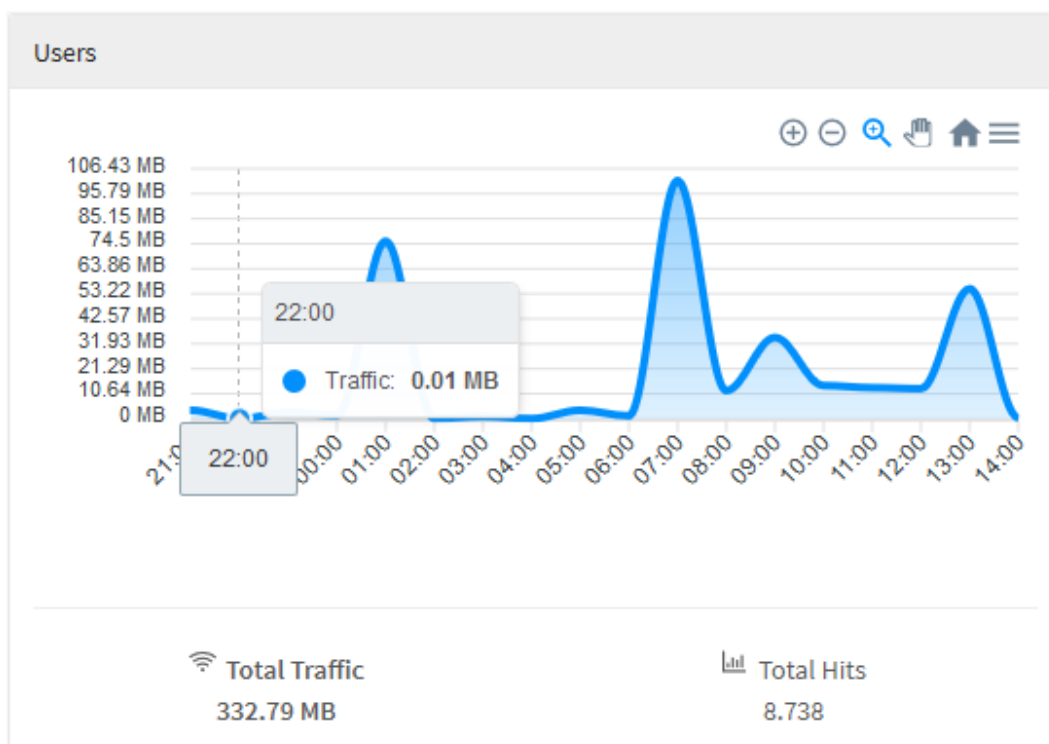
Web Filter – Users – Total Traffic

When clicking on each of these legends, the graph will be automatically modified to illustrate the relevant information, as shown below:



Web Filter – Traffic – Total Hits

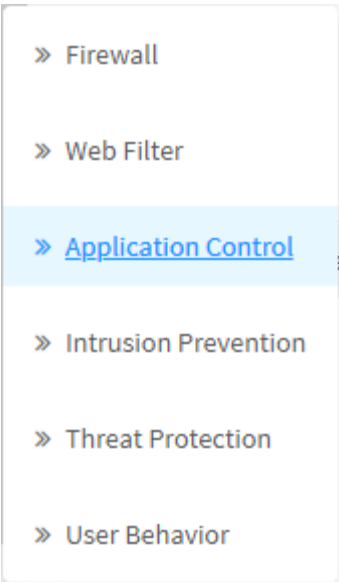
When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



Web Filter – Users – Total Traffic - Period Summary

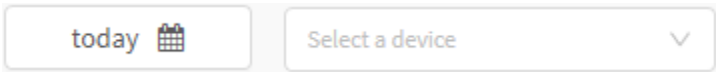
# Application Control

To access the Application Control reports, click on the “Analyzer” icon located on the left side, a dropdown menu will be displayed, select the “Application Control” option.



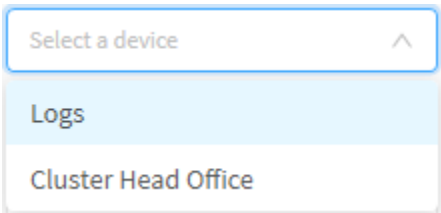
Application Control

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:



Caixa de Seleção

In this checkbox will be listed all devices (or groups of devices) previously registered in [Device Manager](#), to create a report, select the desired device.



Selecting Device

Right on the right side where we just selected the devices, it is possible to see a date selection box, the purpose of which is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today’s date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.


Today

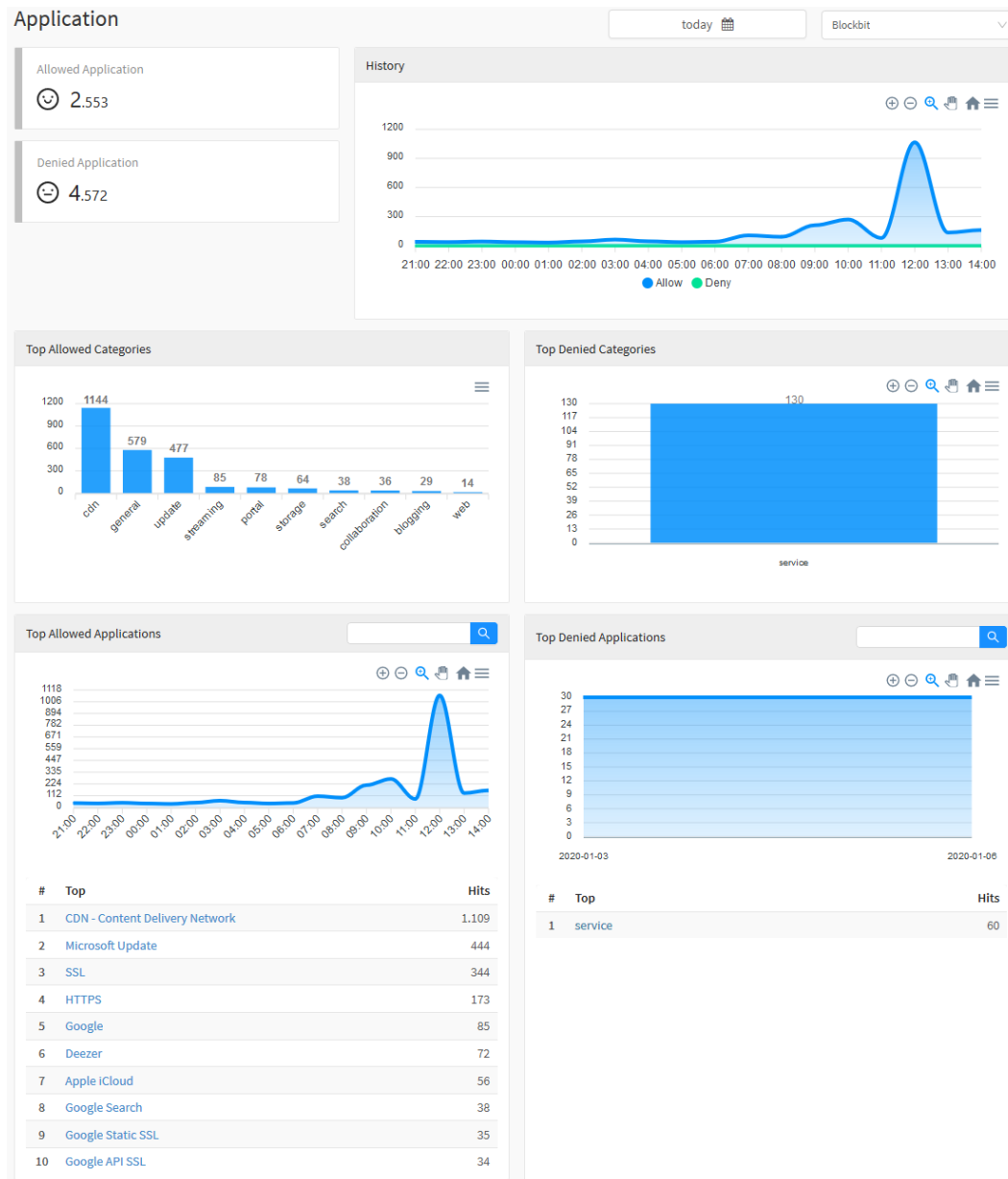
Period:

Today

Cancel
OK







Date Selection

Select the desired date and click [  ] button;




Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- [  ]: It serves to zoom in;
- [  ]: Its function is to remove the zoom;
- [  ]: It serves to make a selection zoom;
- [  ]: It serves to move the graph;
- [  ]: Reset the graph to the starting position;
- [  ]: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

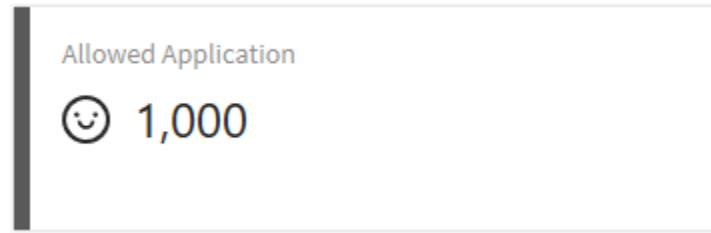
To perform a search, type a term in the search bar and click the search [  ] button.

Next, we will analyze in detail the components of "Application Control":

- [Allowed Application](#);
- [Denied Application](#);
- [History](#);
- [Top Allowed Categories](#);
- [Top Denied Categories](#);
- [Top Allowed Applications](#);
- [Top Denied Applications](#).

# Application Control - Allowed Application

In "Allowed Application" it displays a total of applications that have been authorized to access.

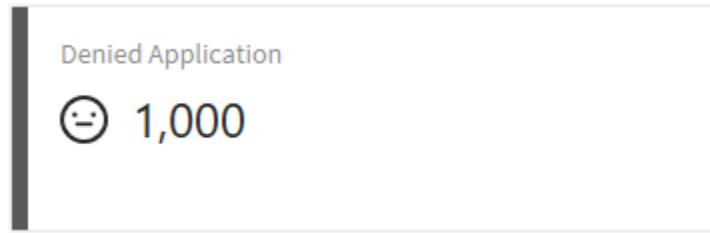


*Application Control – Allowed Application*



# Application Control - Denied Application

In "Application Denied", there is a sum of applications that have been denied access.

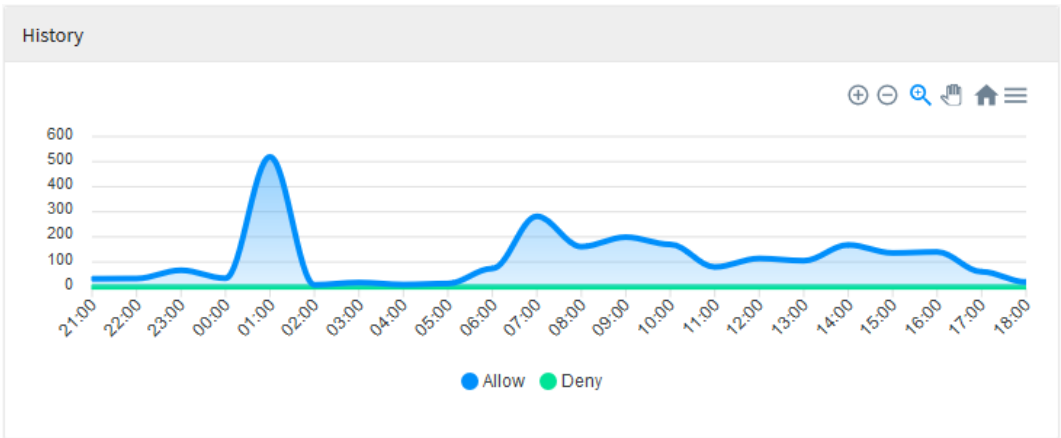


*Application Control – Denied Application*

# Application Control - History

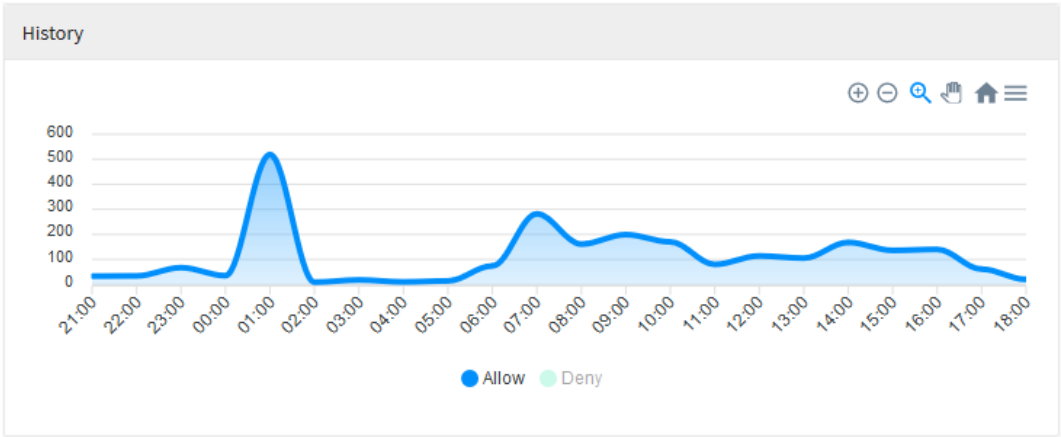
On the right side it is possible to view the "History" graph that displays a history of all applications that have been allowed and denied access, having as reference to their axes the amount of accesses in relation to the previously researched dates. The legend items are interactive and it is possible to change the graph display through them, in order to make the graph display the applications that were allowed and those that were denied by date. In this diagram we have "Allow" where the allowed applications are displayed and "Deny" showing all the applications denied for each of the researched days.

For more information about the navigation menu at the top of this graph check this [page](#).



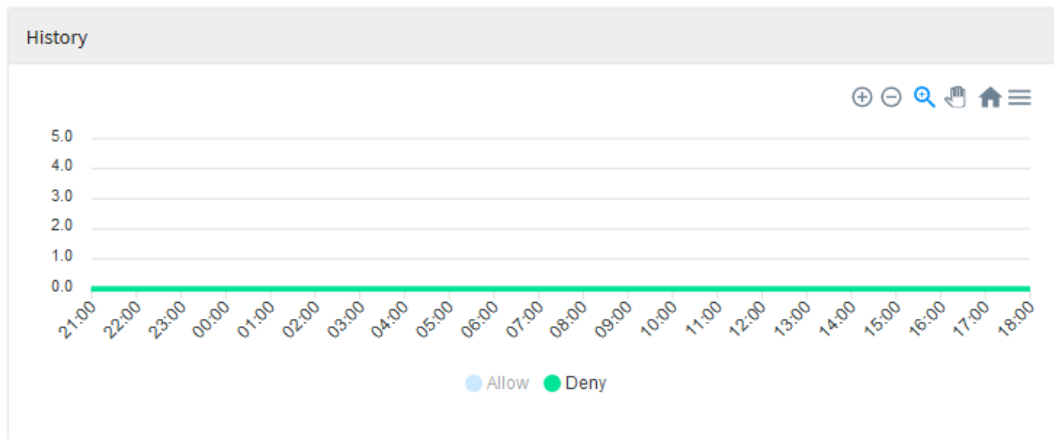
Application Control – History

It is possible to select "Allow", to modify the graph and illustrate the relevant information, as shown below:



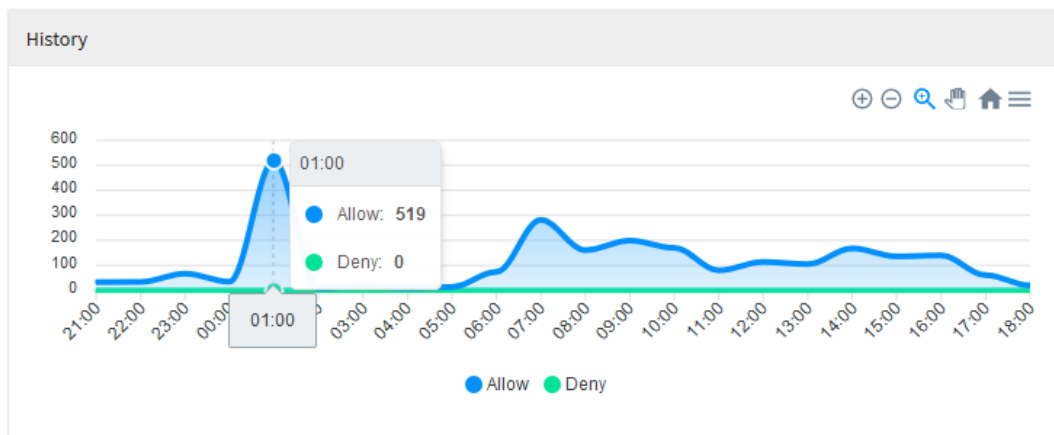
Application Control – History - Allow

You can also click on the "Deny" legend to modify the graph, as shown below:



*Application Control – History - Deny*

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

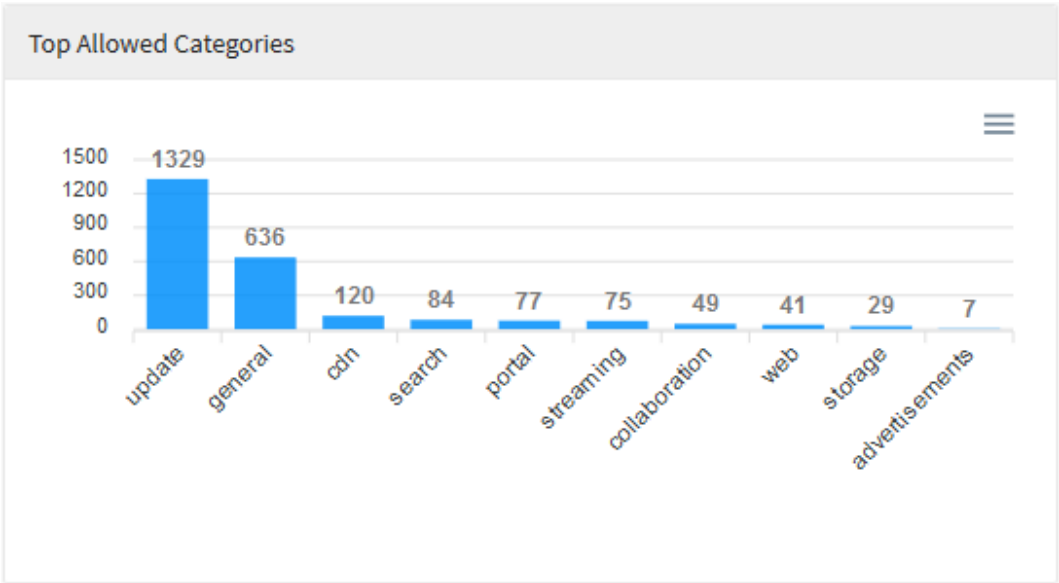


*Application Control – History - Period Summary*

# Application Control - Top Allowed Categories

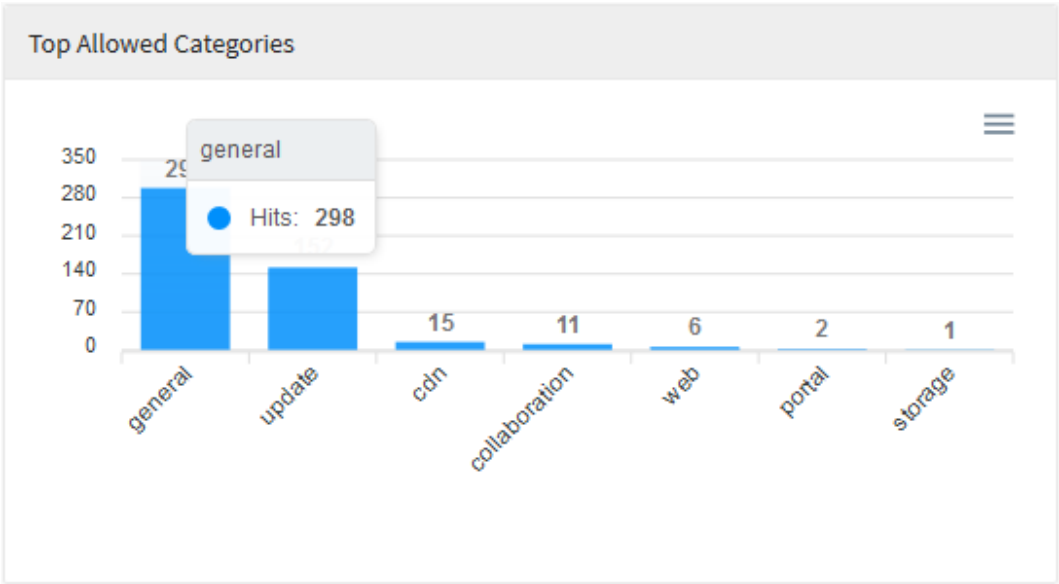
In the diagram “Top Allowed Categories” we have a visual representation of the 10 most allowed categories applied in the users’ accesses, this session serves to represent, in a pragmatic way, the number of pages accessed that apply to each of these categorizations.

For more information about the navigation menu at the top of this graph check this [page](#).



Application Control – Top Allowed Categories

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

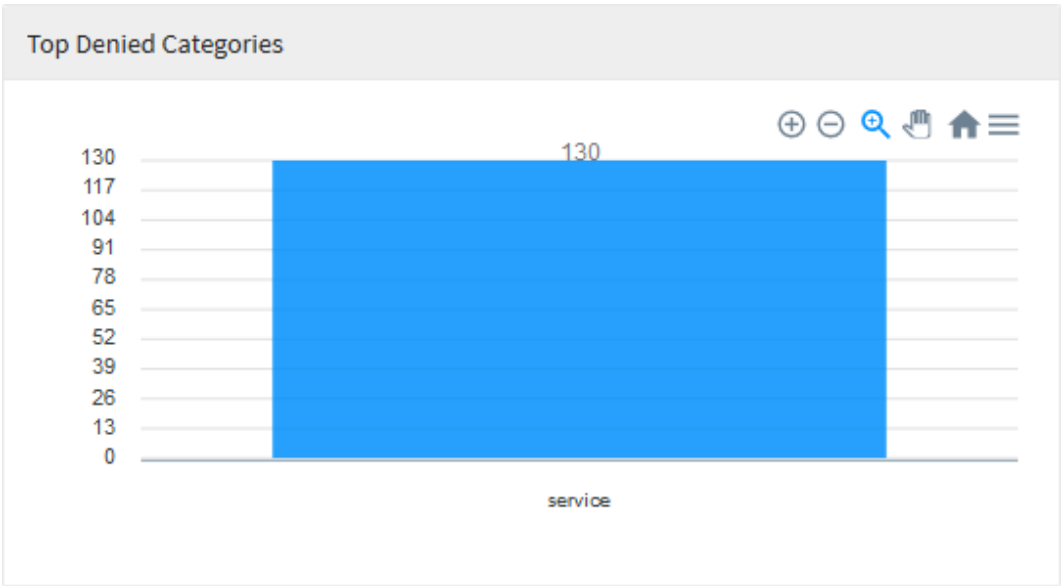


Application Control – Top Allowed Categories - Period Summary

# Application Control - Top Denied Categories

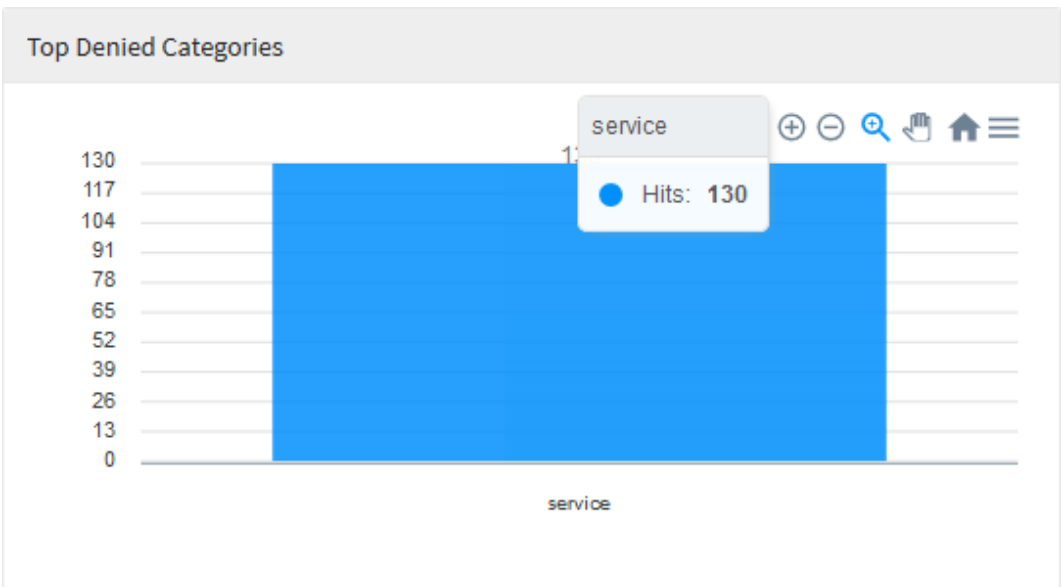
In the diagram "Top Denied Categories" we have a visual representation of the 10 most frequently refused categories used by users, this session serves to represent, in a pragmatic way, the number of pages accessed that fell in each of these categories of refusal.

For more information about the navigation menu at the top of this graph check this [page](#).



Application Control – Top Denied Categories

When hovering the mouse over the graph, a summary of the amount of categories is displayed, as shown in the image below:

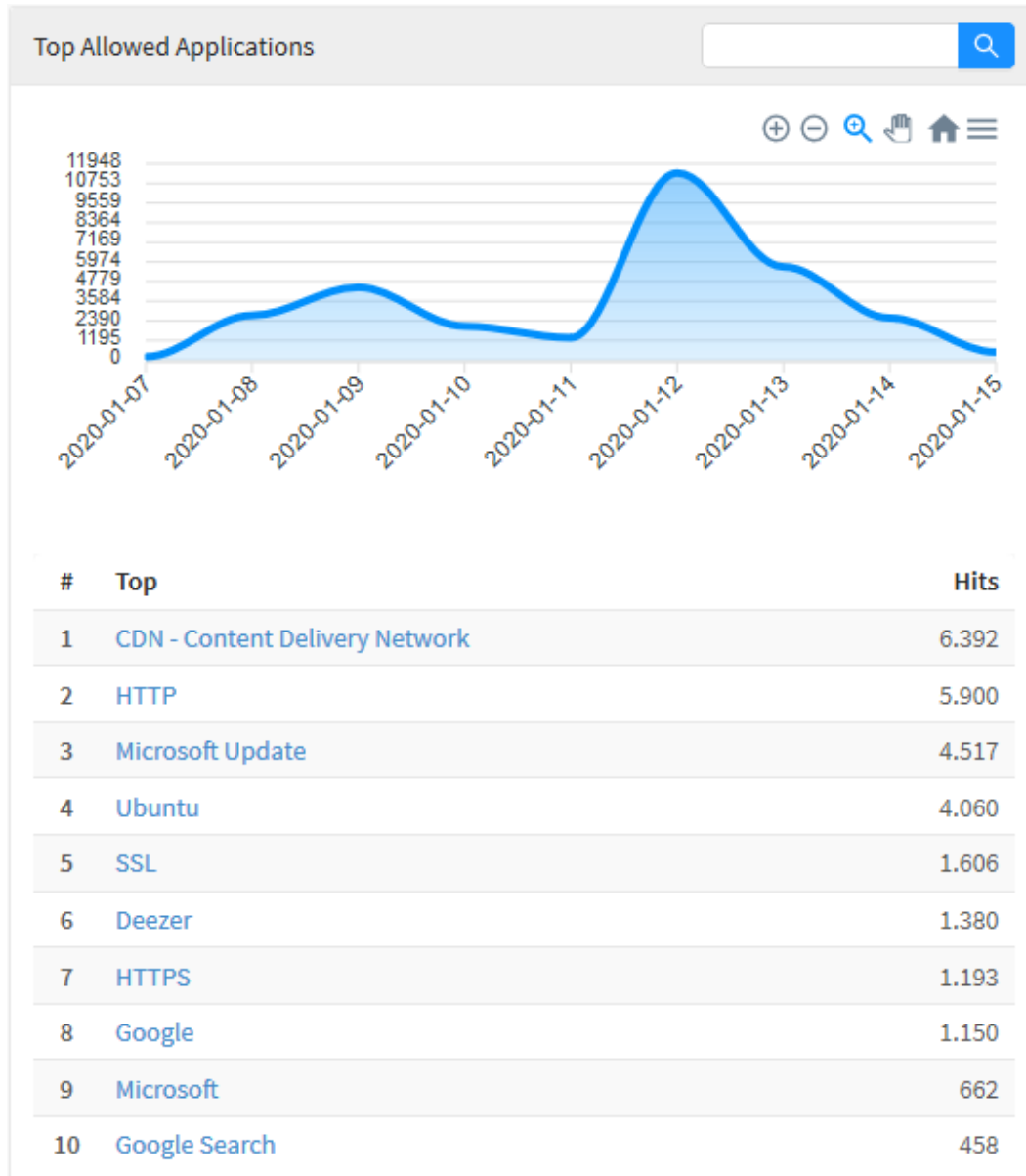


Application Control – Top Denied Categories – Number of declined categories

## Application Control - Top Allowed Applications

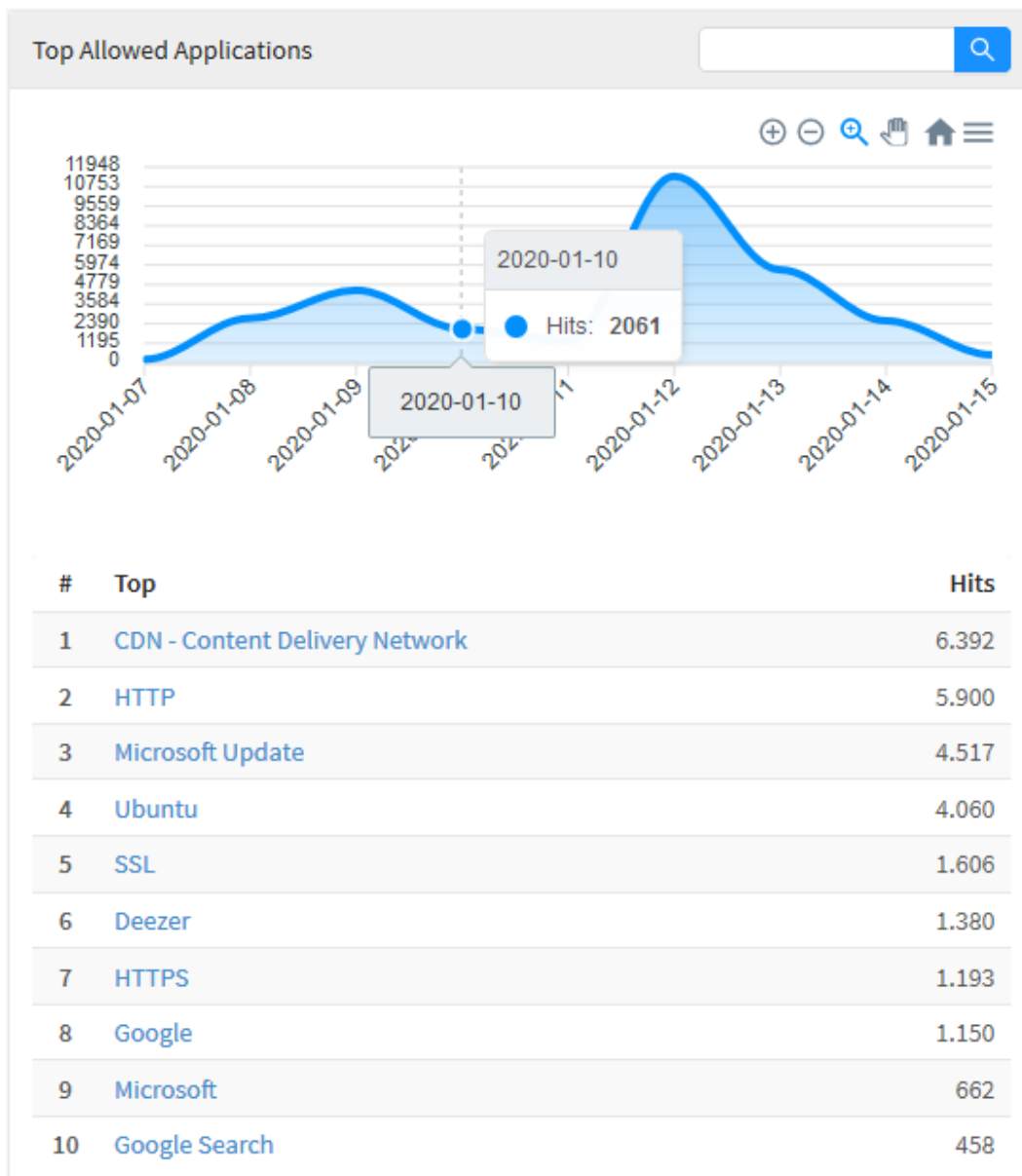
In “Top Allowed Applications” there is a graph representing the ten applications that had their access authorized in relation to the previously specified period of time, below that graph, we have a list of the names of these ten applications classified in order of the largest amount of accesses and their respective categories.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



## Application Control – Top Allowed Applications

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

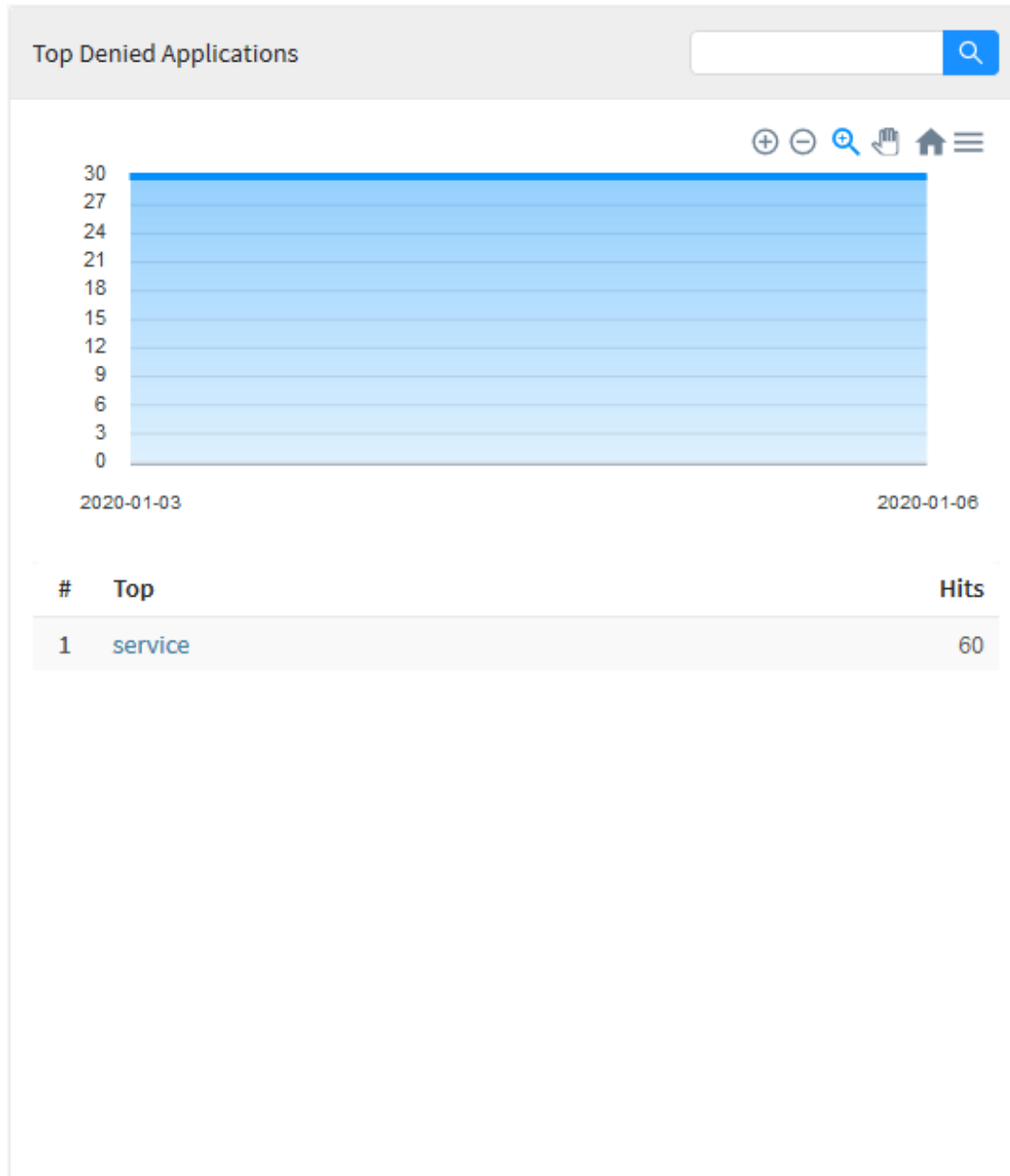


Application Control - Top Allowed Applications - Period Summary

## Application Control - Top Denied Applications

In the panel “Top Denied Applications” we have the exact opposite of the previous session: A graph representing the ten applications that were denied access in relation to the previously specified period of time, below that graph, we have a list of the names of these ten applications classified in order highest amount of accesses and their respective categories.

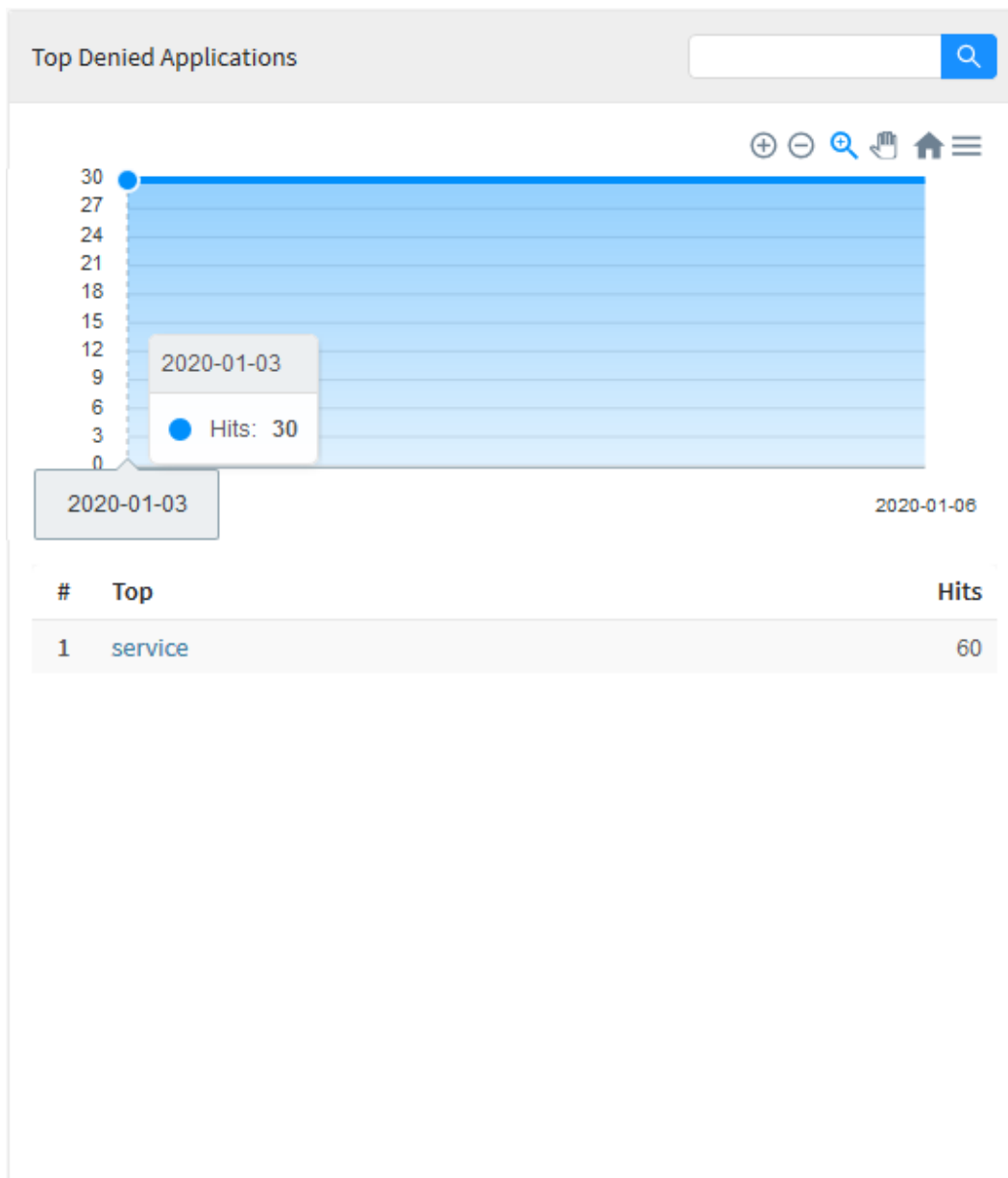
For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



## Application Control – Top Denied Applications

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:

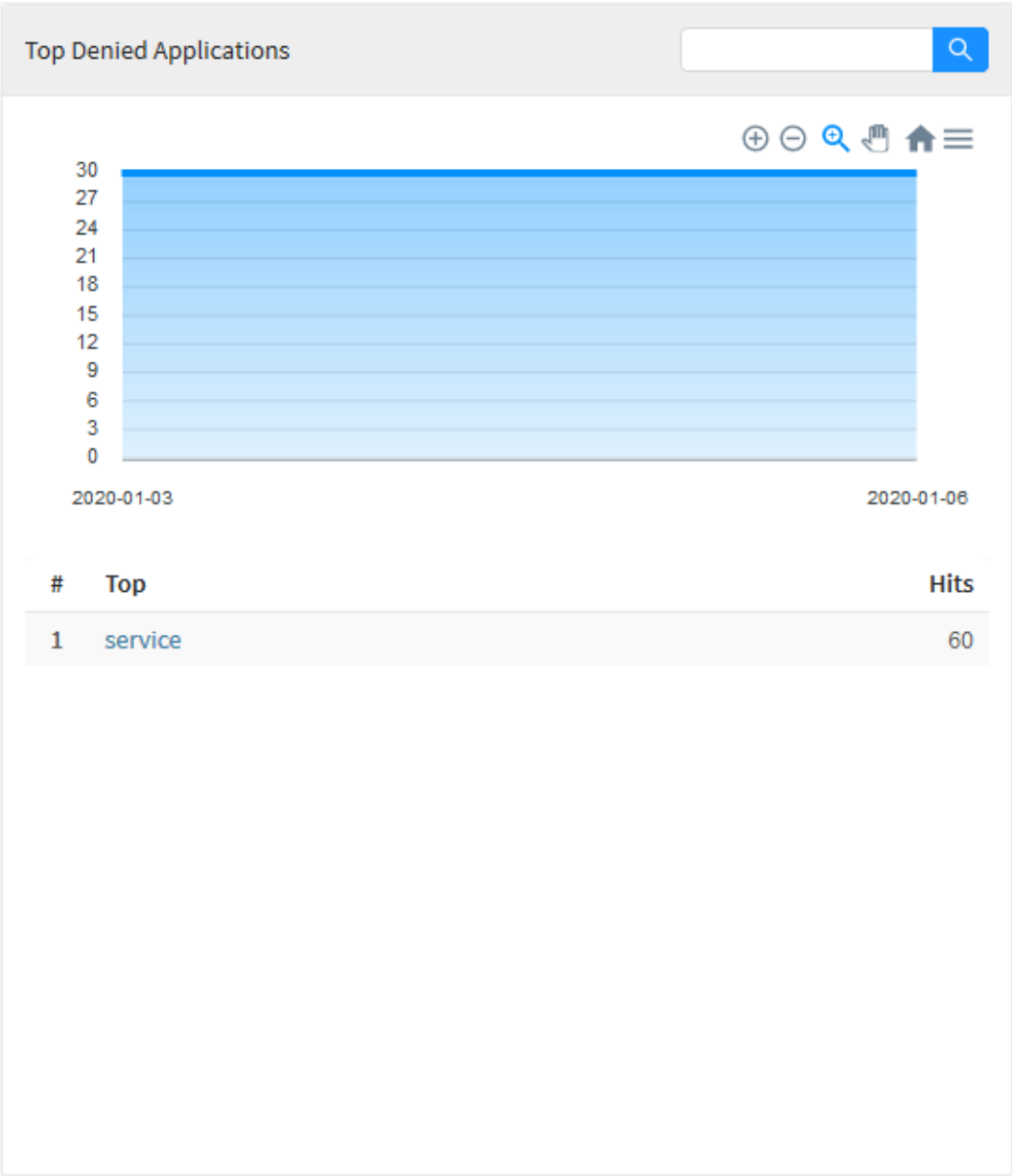




Application Control – Top Denied Applications - Period summary

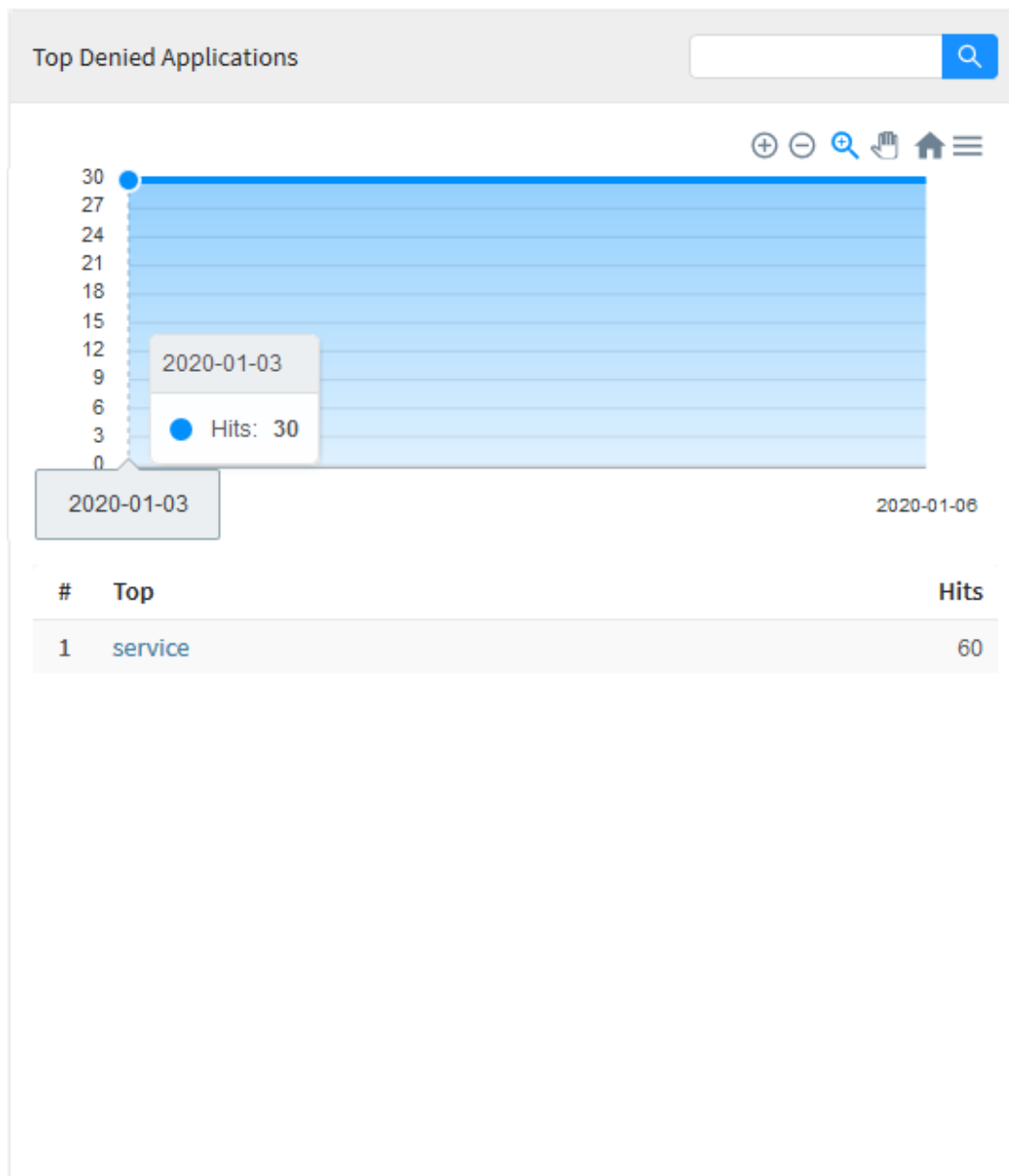
In the panel "Top Denied Applications" we have the exact opposite of the previous session: A graph representing the ten applications that were denied access in relation to the previously specified period of time, below that graph, we have a list of the names of these ten applications classified in order highest amount of accesses and their respective categories.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



Application Control – Top Denied Applications

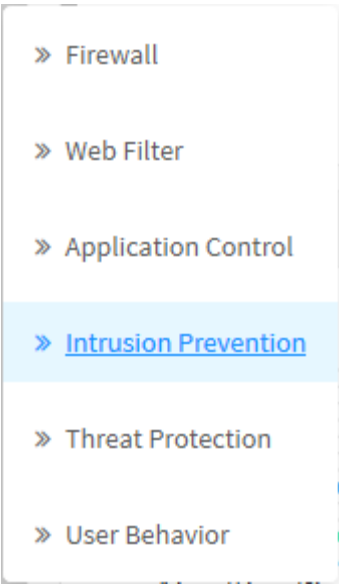
When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



Application Control – Top Denied Applications - Period summary

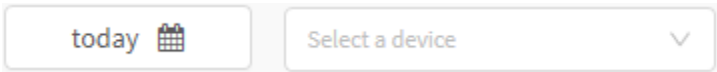
# Intrusion Prevention

To access the Intrusion Prevention reports, click on the “Analysis” icon located on the left side, a dropdown menu will be displayed, select the “Intrusion Prevention” option.



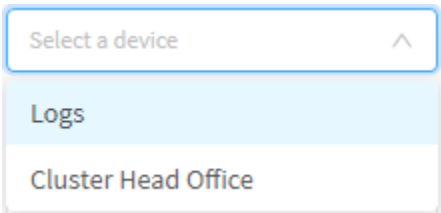
Intrusion Prevention

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:



Selection box

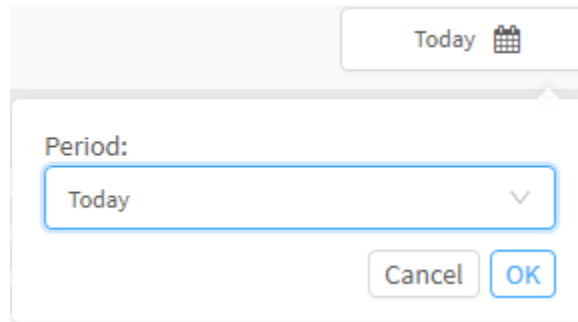
In this checkbox will be listed all devices (or groups of devices) previously registered in [Device Manager](#), to create a report, select the desired device.




Selecting Device


Right on the right side where we just selected the devices, it is possible to see a date selection box, the purpose of which is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.

A dialog box titled "Date Selection" with a light gray header. In the top right corner of the header is a button labeled "Today" next to a calendar icon. The main area of the dialog has a label "Period:" followed by a dropdown menu. The dropdown menu is open, showing "Today" as the selected option with a downward arrow on the right. At the bottom right of the dialog are two buttons: "Cancel" and "OK".


Today 

Period:

Today 

Cancel OK

Date Selection

Select the desired date and click [  ] button;

## Intrusion Prevention

today

Blockbit

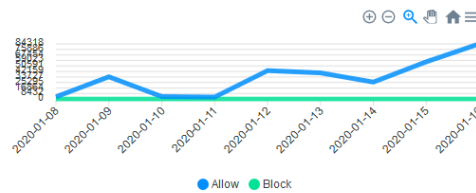
Alerted

✓ 12

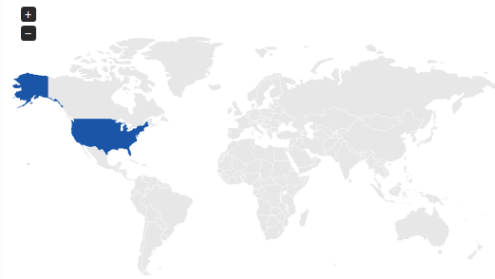
Blocked

7,000

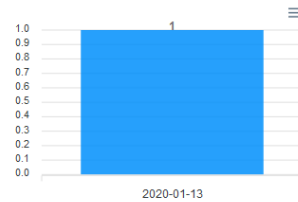
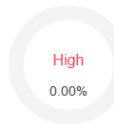
### History



### Geolocation

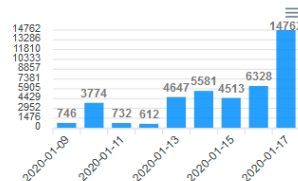
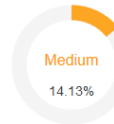


### Impact - High



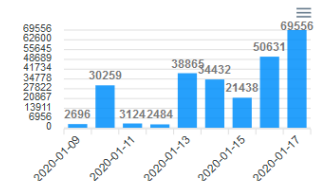
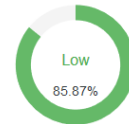
#	Threat	Hits
1	SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt	1

### Impact - Medium



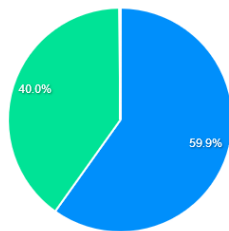
#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	40,993
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	285
3	GPL SNMP request udp	116
4	SERVER-OTHER MRLG fastping echo reply memory corruption attempt	70
5	PROTOCOL-SNMP request udp	65
6	GPL SNMP public access udp	51
7	PROTOCOL-SNMP public access udp	51

### Impact - Low



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	54,896
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	54,874
3	GPL ICMP_INFO PING	41,115
4	PROTOCOL-ICMP PING	40,964
5	PROTOCOL-ICMP ICMPv6 Echo Request	13,811
6	GPL ICMP_INFO Echo Reply	12,550
7	PROTOCOL-ICMP Echo Reply	12,543

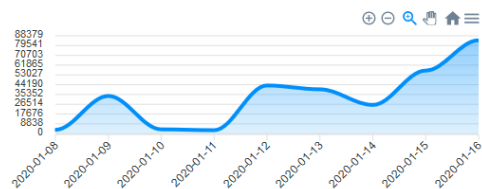
### Layer 3 Intrusion Protection



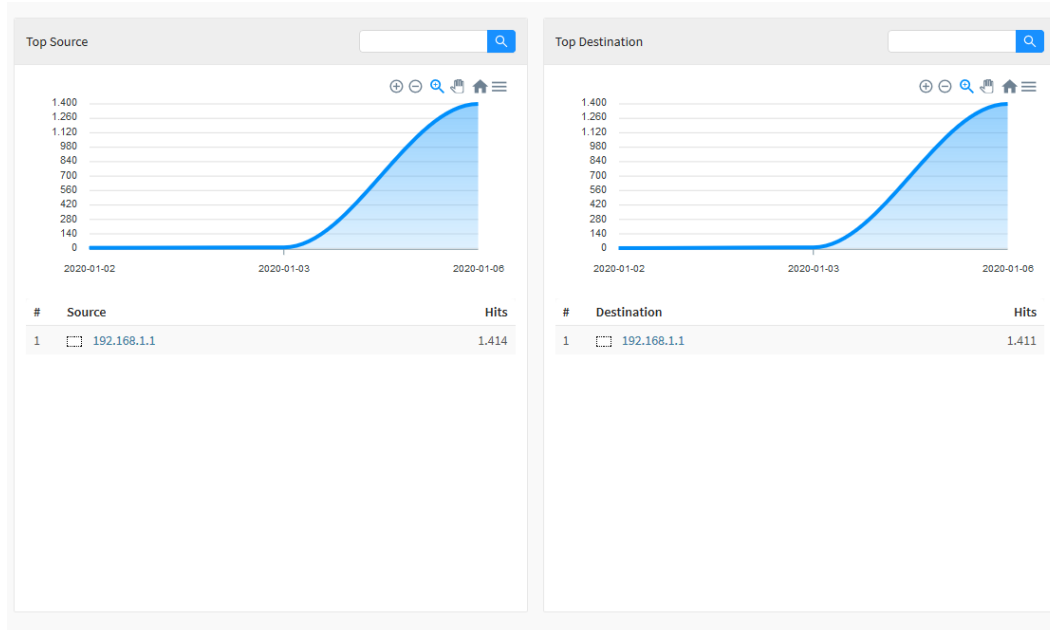
- PROTOCOL-ICMP
- GPL
- PROTOCOL-DNS
- PROTOCOL-SNMP
- SERVER-OTHER
- DNS
- WEB\_SERVER
- INDICATOR-COMPROMISE
- SERVER-WEBAPP

#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	59,453
2	172.32.250.20	GPL	57,497
3	172.32.250.24	PROTOCOL-DNS	281
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.6	SERVER-OTHER	61
6	172.32.250.24	DNS	23
7	192.16.58.8	WEB_SERVER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

### Intrusion Classification



#	Malicious IP	Hits
1	Misc activity	253,461
2	Information Leak	40,993
3	Potentially Bad Traffic	311
4	Attempted Information Leak	310
5	Misc Attack	70
6	Not Suspicious Traffic	24
7	Access to a Potentially Vulnerable Web Application	11
8	Attempted Administrator Privilege Gain	1



*Analyzer - Intrusion Prevention*

Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- [ + ]: It serves to zoom in;
- [ - ]: Its function is to remove the zoom;
- [ 🔍 ]: It serves to make a selection zoom;
- [ 🖱️ ]: It serves to move the graph;
- [ 🏠 ]: Reset the graph to the starting position;
- [ ≡ ]: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the [ 🔍 ] button.

Next, we will analyze in detail the components of "Intrusion Prevention":

- [Alerted, Blocked and History](#);
- [Alerts by Geolocation](#);
- [Impact - High](#);
- [Impact - Medium](#);
- [Impact - Low](#);
- [Layer 3 Intrusion Protection](#);
- [Intrusion Classification](#);
- [Top Source](#);
- [Top Destination](#).

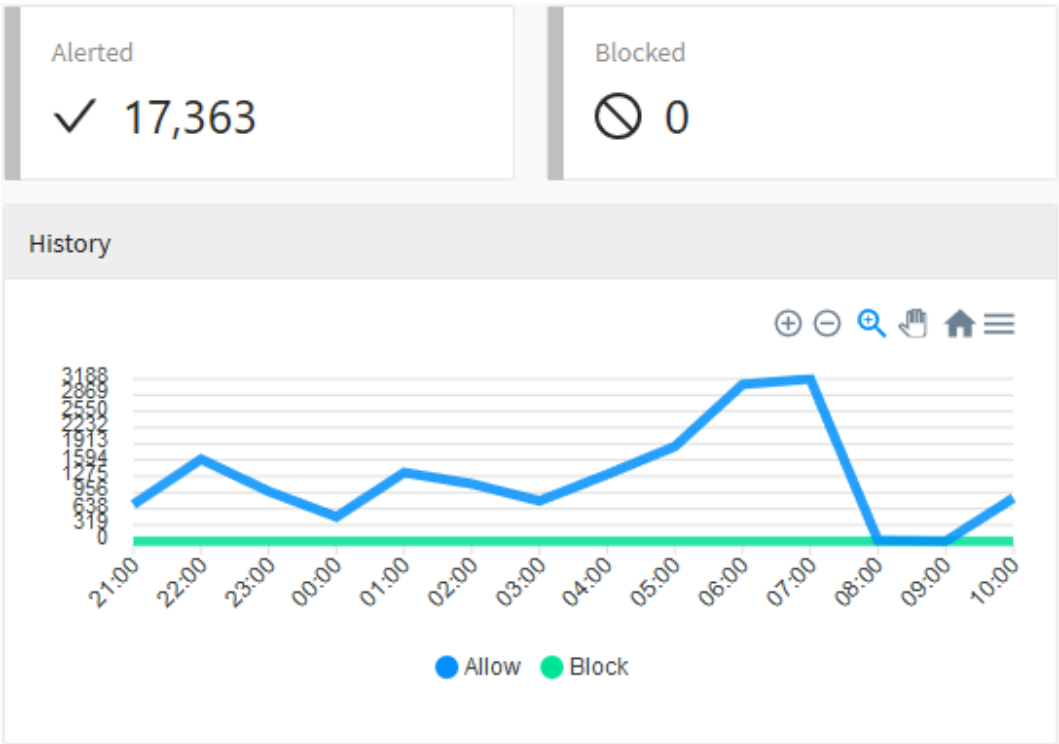
# Intrusion Prevention - Alerted, Blocked and History

The "Alerted" panel displays a total of intrusion alerts.

In "Blocked", a number is displayed totaling the blocked intrusion attempts.

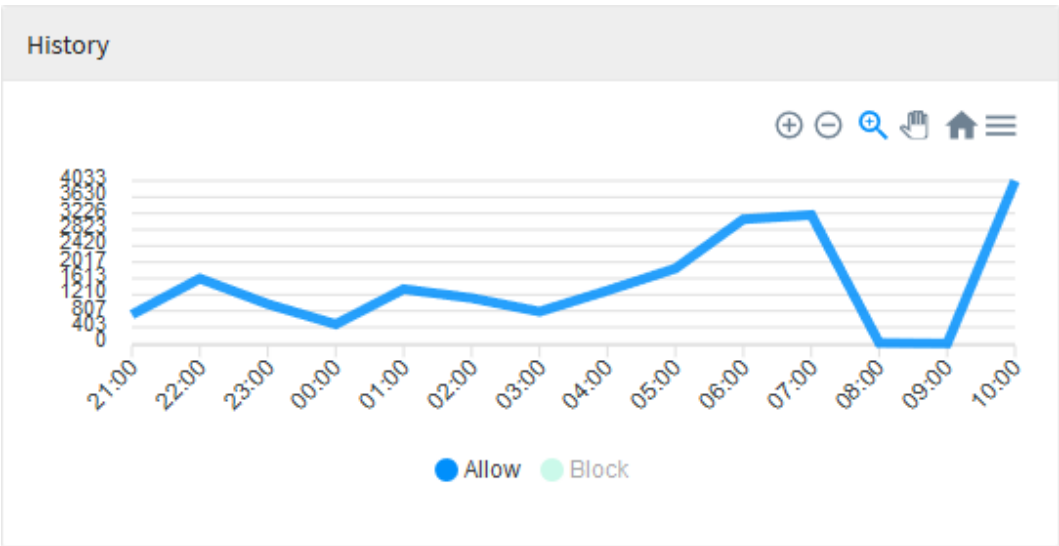
Below, a summary of alerts and blockages is shown in a line graph showing the number of intrusion-related events within the previously selected time period. By selecting one of the captions ("Alerted" or "Blocked") at the top of the graph, it is possible to determine that only one of these will be displayed on the graph.

For more information about the navigation menu at the top of this graph check this [page](#).



Alerted, Blocked and History

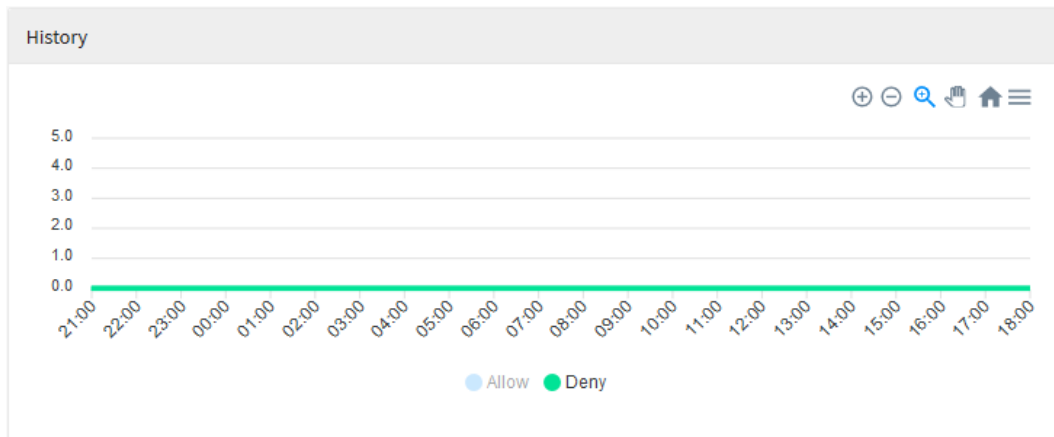
It is possible to select "Allow", to modify the graph and illustrate the relevant information, as shown below:





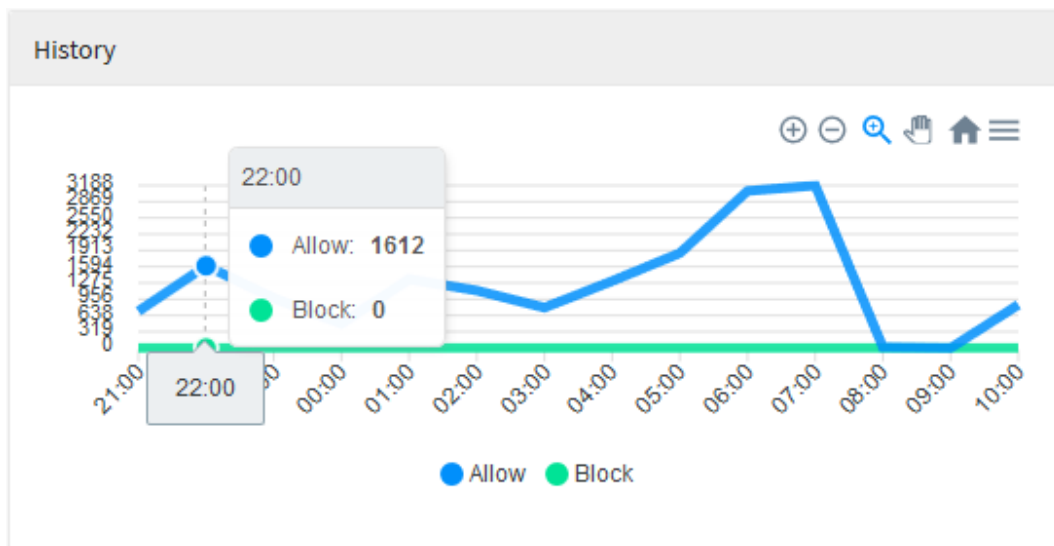
### Alerted, Blocked and History - Allow

You can also click on the "Deny" legend to modify the graph, as shown below:



### Alerted, Blocked and History - Deny

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



### Alerted, Blocked and History - Period Summary

# Intrusion Prevention - Alerts by Geolocation

In "Alerts by Geolocation" the origin of the intrusions by geolocation is displayed, the global map demonstrates through a colored legend the amount of accesses made by users. When hovering the mouse over the countries a total number of alerts is displayed, when doing the same with the legend it is possible to view an average, in addition, the country referring to this value is highlighted on the map.



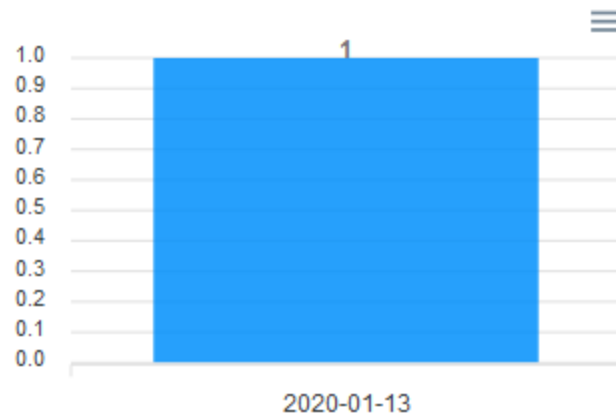
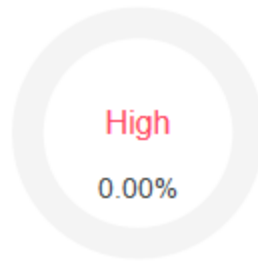
*Alerts by Geolocation*

# Intrusion Prevention - Impact - High

In "Impact - High" we have a donut chart showing the percentage of high impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring high-impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph check this [page](#).

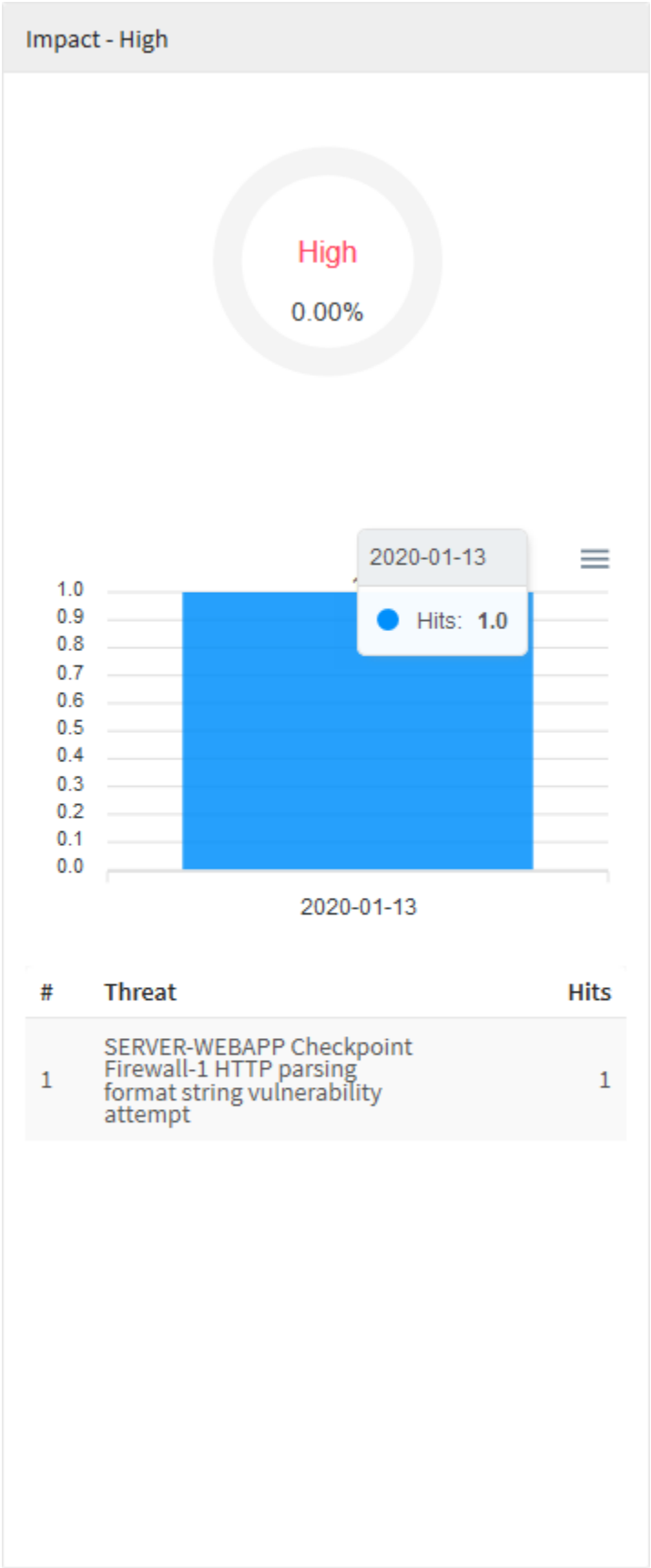
## Impact - High



#	Threat	Hits
1	SERVER-WEBAPP Checkpoint Firewall-1 HTTP parsing format string vulnerability attempt	1

Impact - High

When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



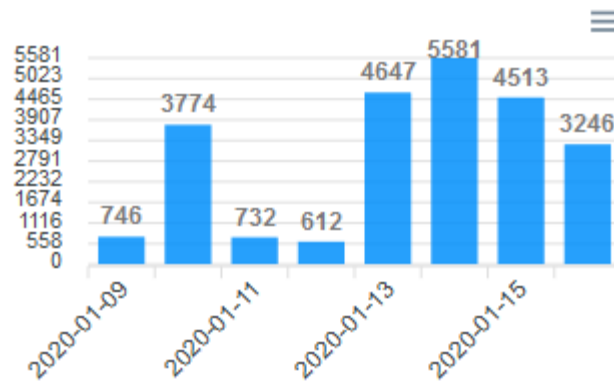
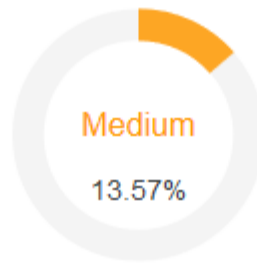


# Intrusion Prevention - Impact - Medium

In "Impact - Medium" we have a donut chart showing the percentage of medium impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring medium impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph check this [page](#).

## Impact - Medium

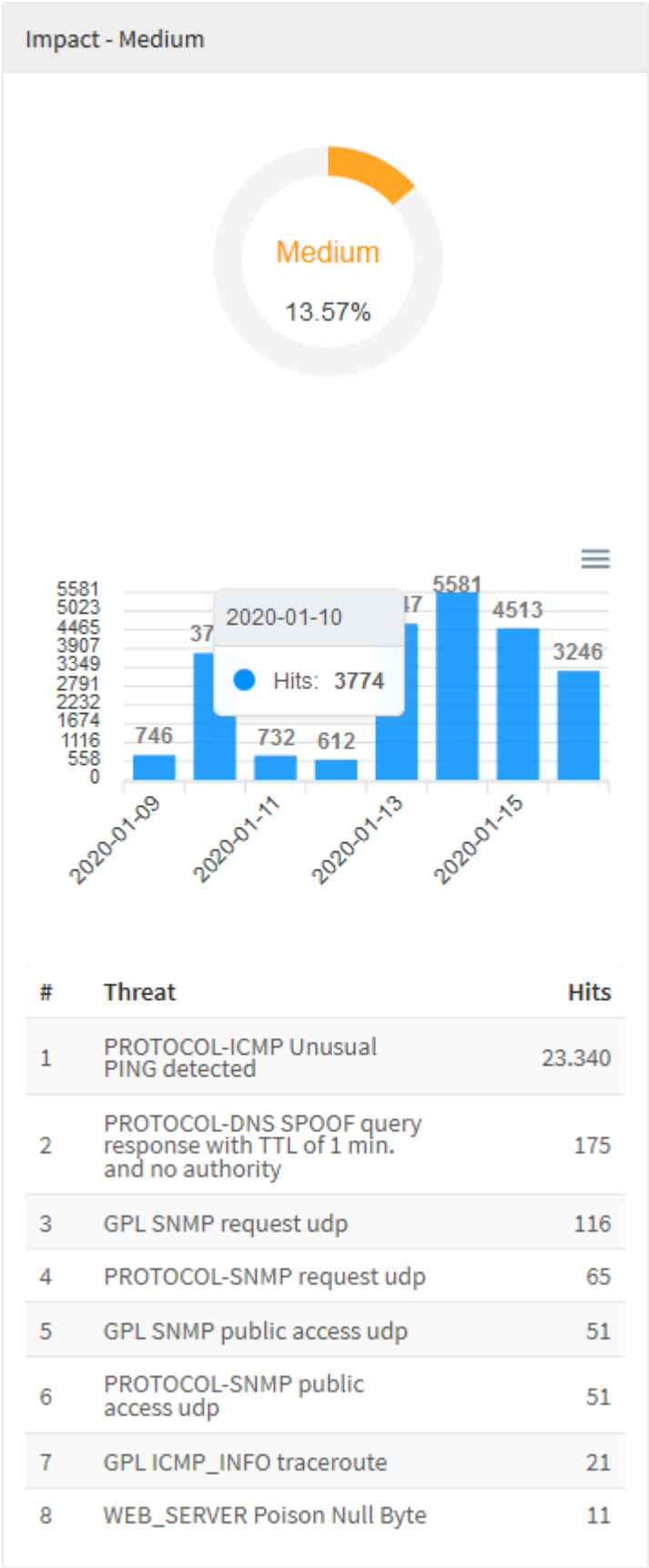


#	Threat	Hits
1	PROTOCOL-ICMP Unusual PING detected	23.340
2	PROTOCOL-DNS SPOOF query response with TTL of 1 min. and no authority	175
3	GPL SNMP request udp	116
4	PROTOCOL-SNMP request udp	65
5	GPL SNMP public access udp	51
6	PROTOCOL-SNMP public access udp	51
7	GPL ICMP_INFO traceroute	21
8	WEB_SERVER Poison Null Byte	11

Impact - Medium



When hovering the mouse over the graph, a summary of the period is displayed, as shown in the image below:



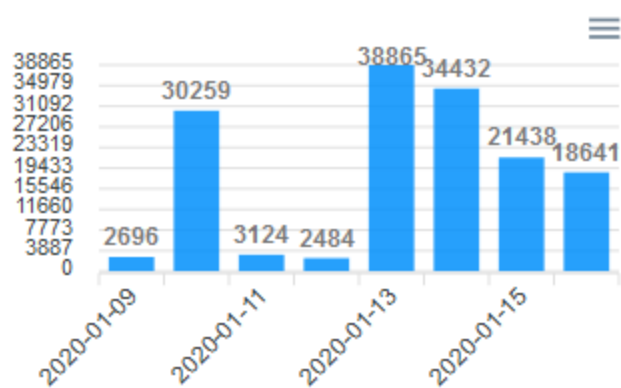
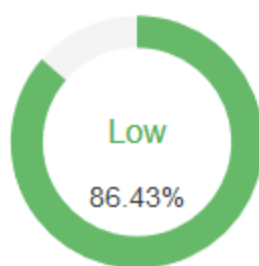


# Intrusion Prevention - Impact - Low

In "Impact - Low" we have a donut chart showing the percentage of low impact intrusion threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring low-impact threats, displaying their name and listing them by number of recurrences.

For more information about the navigation menu at the top of this graph check this [page](#).

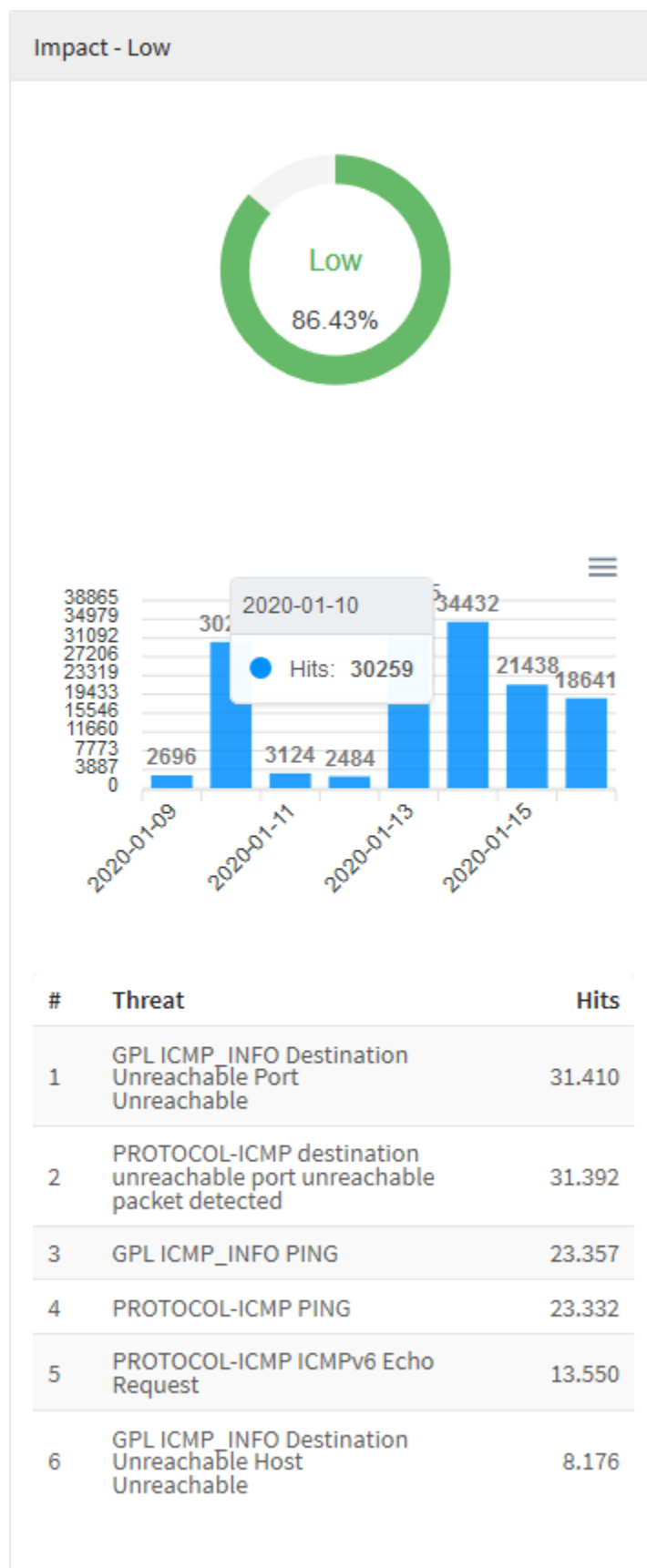
## Impact - Low



#	Threat	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	31.410
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	31.392
3	GPL ICMP_INFO PING	23.357
4	PROTOCOL-ICMP PING	23.332
5	PROTOCOL-ICMP ICMPv6 Echo Request	13.550
6	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.176

Impact - Low

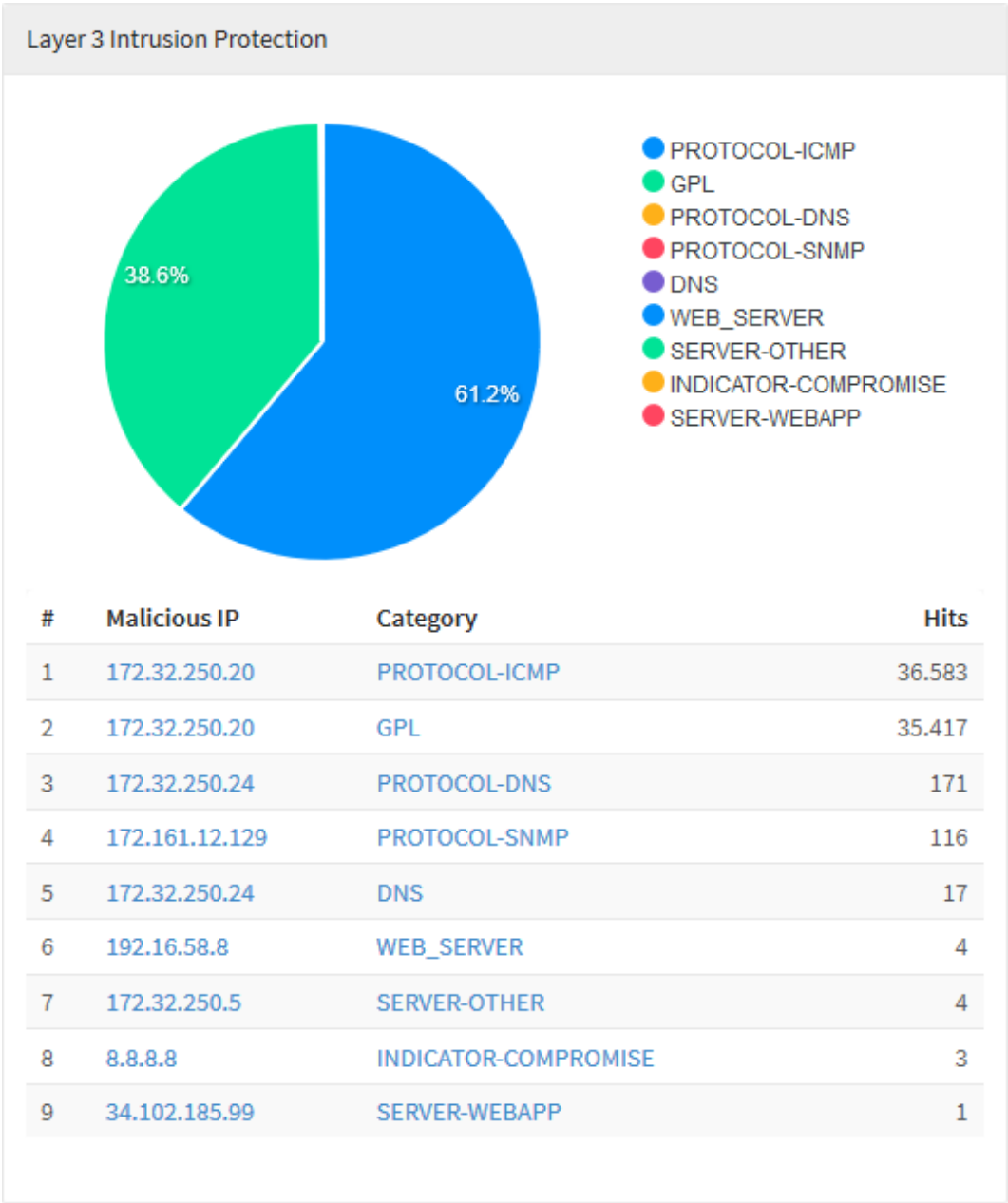
When you mouse over the graph, a summary of the period is displayed, as shown in the image below:





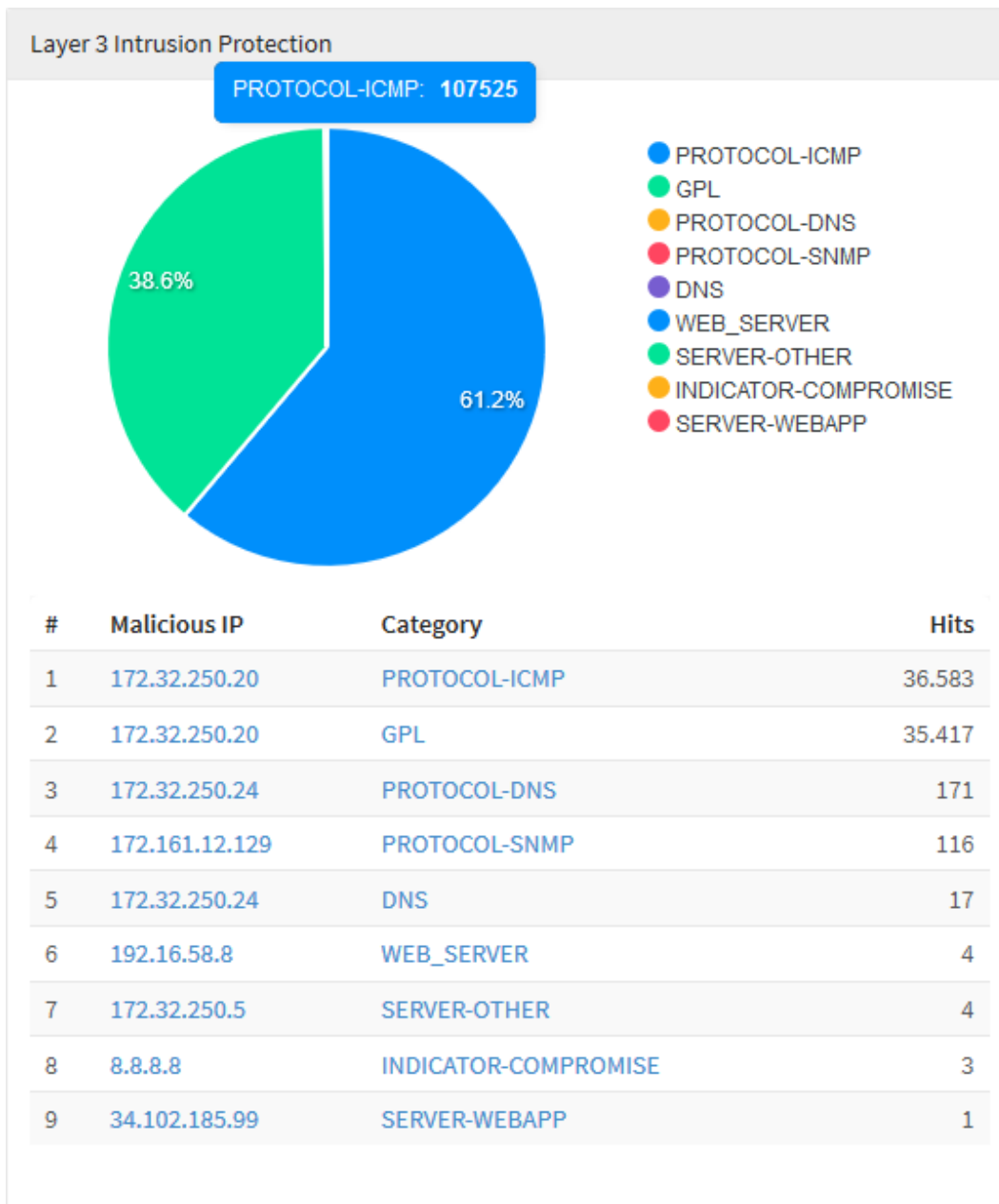
# Intrusion Prevention - Layer 3 Intrusion Protection

In "Layer 3 Intrusion Protection" we have a graph showing the ten categories of most detected intrusion alerts in layer 3 of the IPS (Intrusion Prevention System). When you click on one of the IPs or one of the categories, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected item. Just below the graph, we have a list of the ten IPs and the most accessed categories in order by the number of accesses.



Layer 3 Intrusion Prevention

When you hover your mouse over the graph, it will display a number with the amount of intrusion alerts, as shown in the image below:

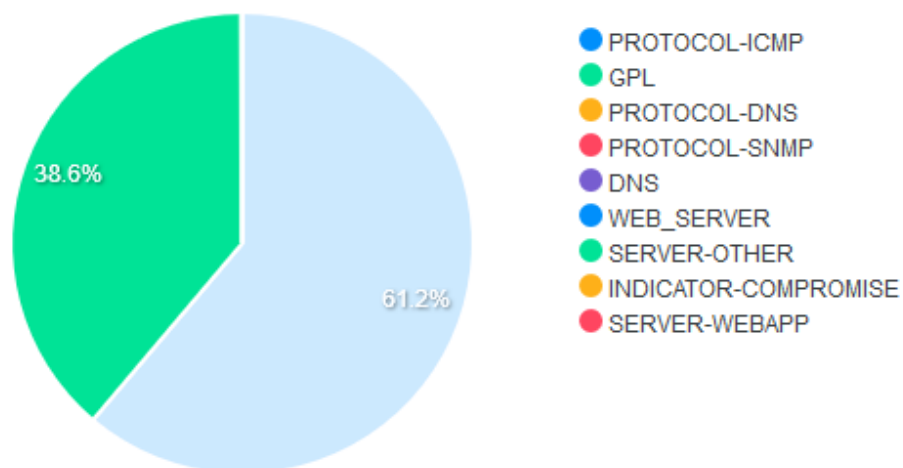


Layer 3 Intrusion Prevention - Amount of intrusion alerts

When hovering the mouse over the information, the graphic will be highlighted, as shown below:



## Layer 3 Intrusion Protection



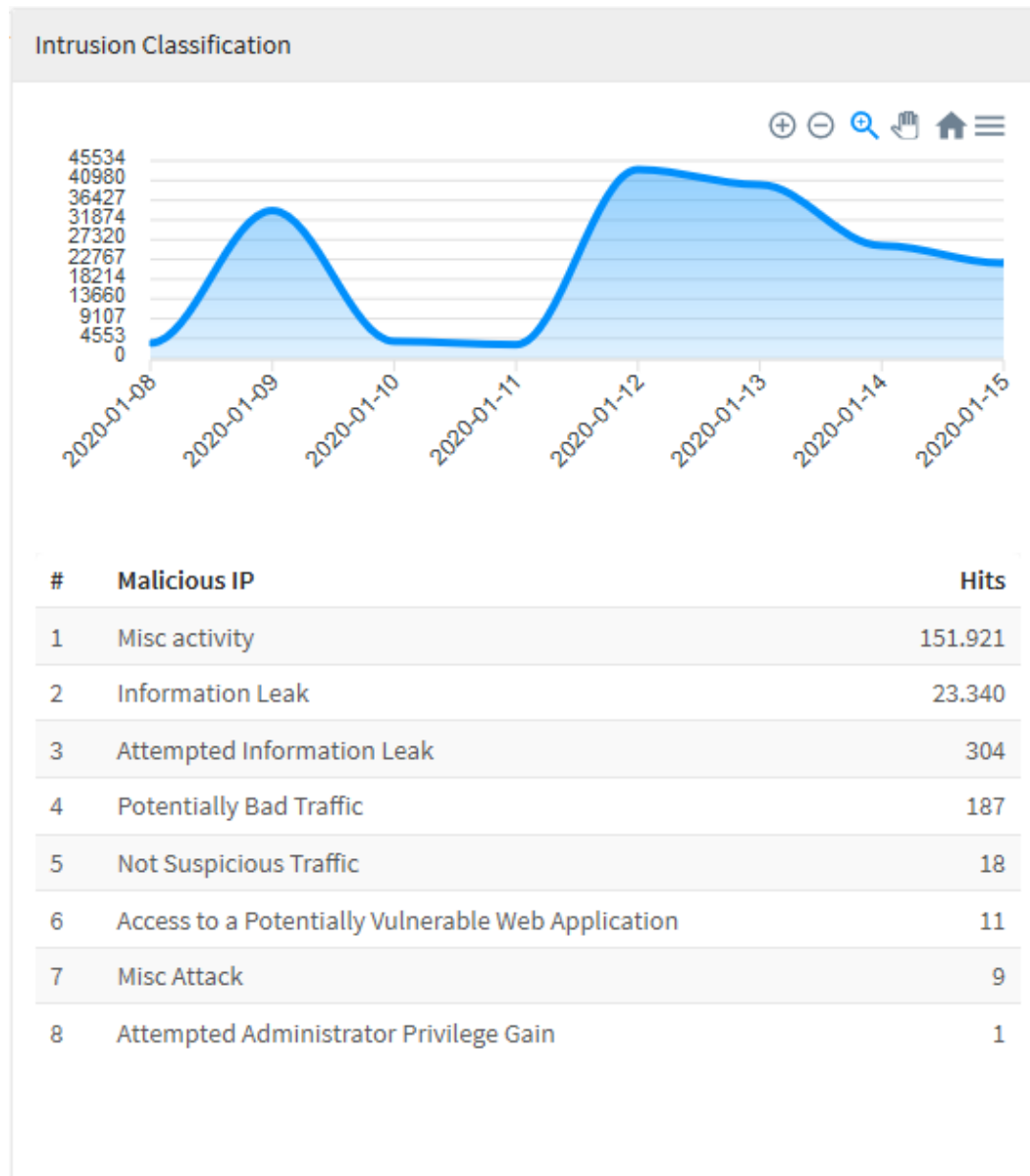
#	Malicious IP	Category	Hits
1	172.32.250.20	PROTOCOL-ICMP	36.583
2	172.32.250.20	GPL	35.417
3	172.32.250.24	PROTOCOL-DNS	171
4	172.161.12.129	PROTOCOL-SNMP	116
5	172.32.250.24	DNS	17
6	192.16.58.8	WEB_SERVER	4
7	172.32.250.5	SERVER-OTHER	4
8	8.8.8.8	INDICATOR-COMPROMISE	3
9	34.102.185.99	SERVER-WEBAPP	1

Layer 3 Intrusion Prevention - Highlighted graph

## Intrusion Prevention - Intrusion Classification

In "Intrusion Classification" we have a graph representing the ten most recurrent intrusion alert classes in relation to the previously specified time period. Below the graph, we have a list of the names of the ten classifications in order of the highest amount of accesses.

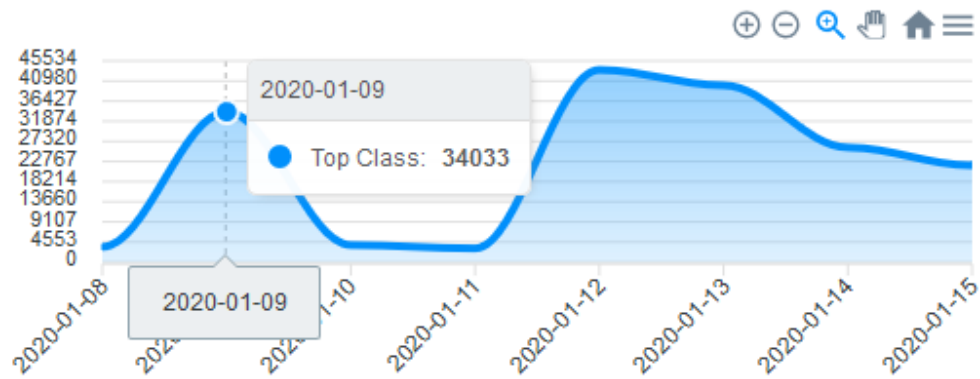
For more information about the navigation menu at the top of this graph check this [page](#).



### Intrusion Classification

By hovering the mouse over the graph, it will highlight the date and number of accesses of the highest class on this specific day.

## Intrusion Classification



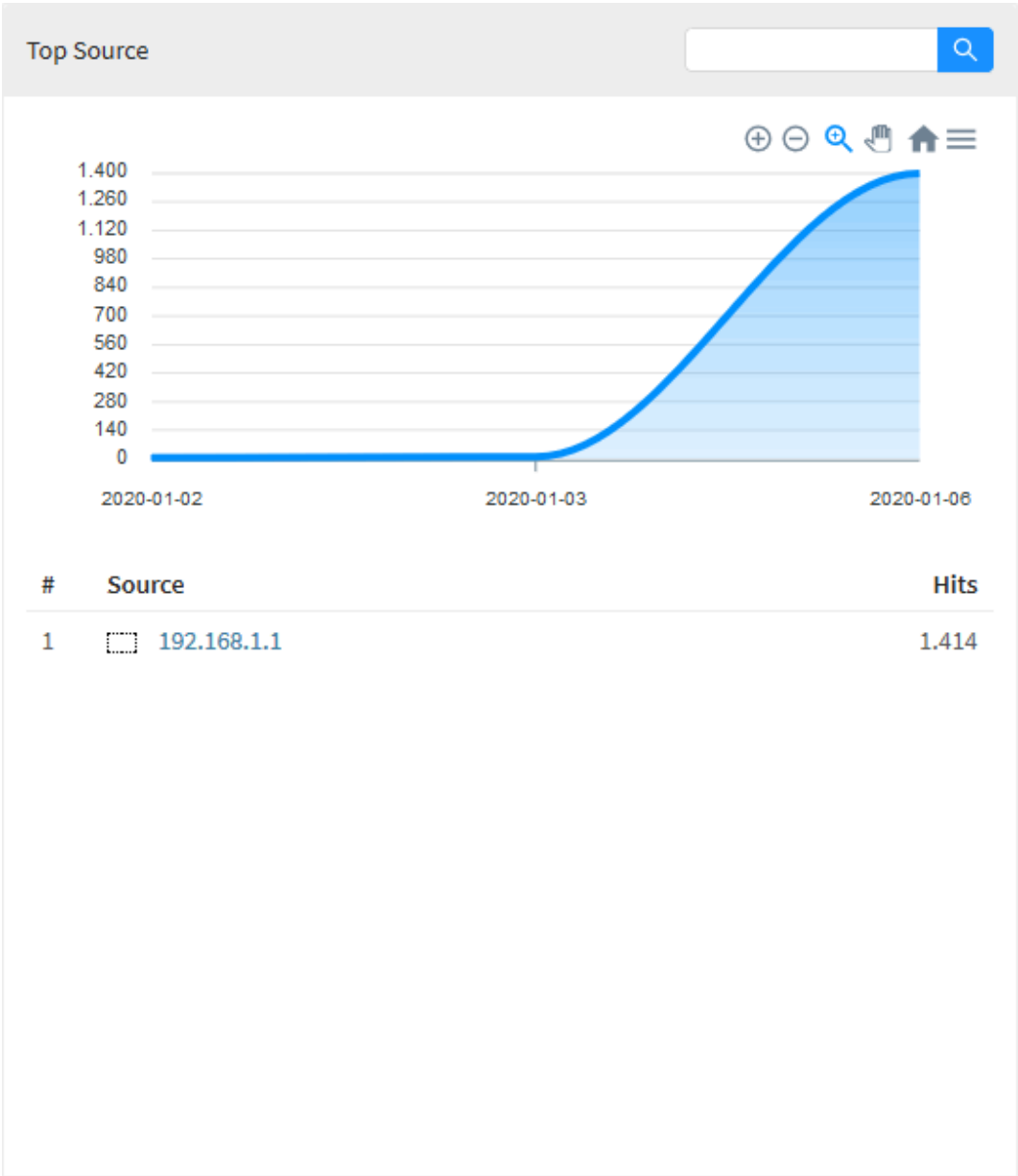
#	Malicious IP	Hits
1	Misc activity	151.921
2	Information Leak	23.340
3	Attempted Information Leak	304
4	Potentially Bad Traffic	187
5	Not Suspicious Traffic	18
6	Access to a Potentially Vulnerable Web Application	11
7	Misc Attack	9
8	Attempted Administrator Privilege Gain	1

*Intrusion Classification - Class summary*

# Intrusion Prevention - Top Source

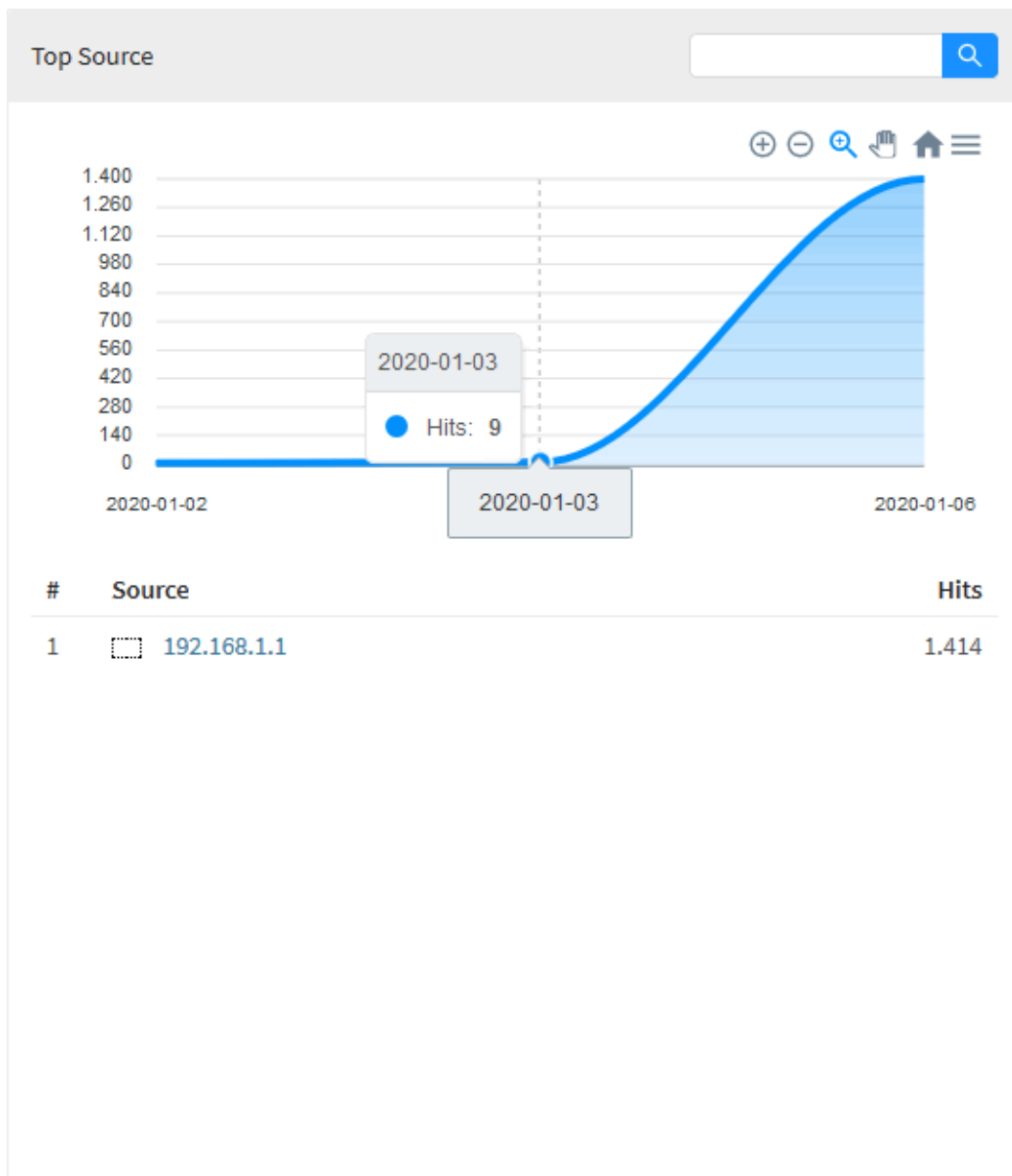
In "Top Source" a line graph is displayed representing the ten most recurrent intrusion alert sources in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten sources previously mentioned, which are classified in order of the highest amount of accesses. When you click on one of the IPs or one of the categories, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected category

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



Top Source

When hovering the mouse over the graph, it will highlight the date and the number of accesses of the highest class of this specific day:



Top Source - Summary

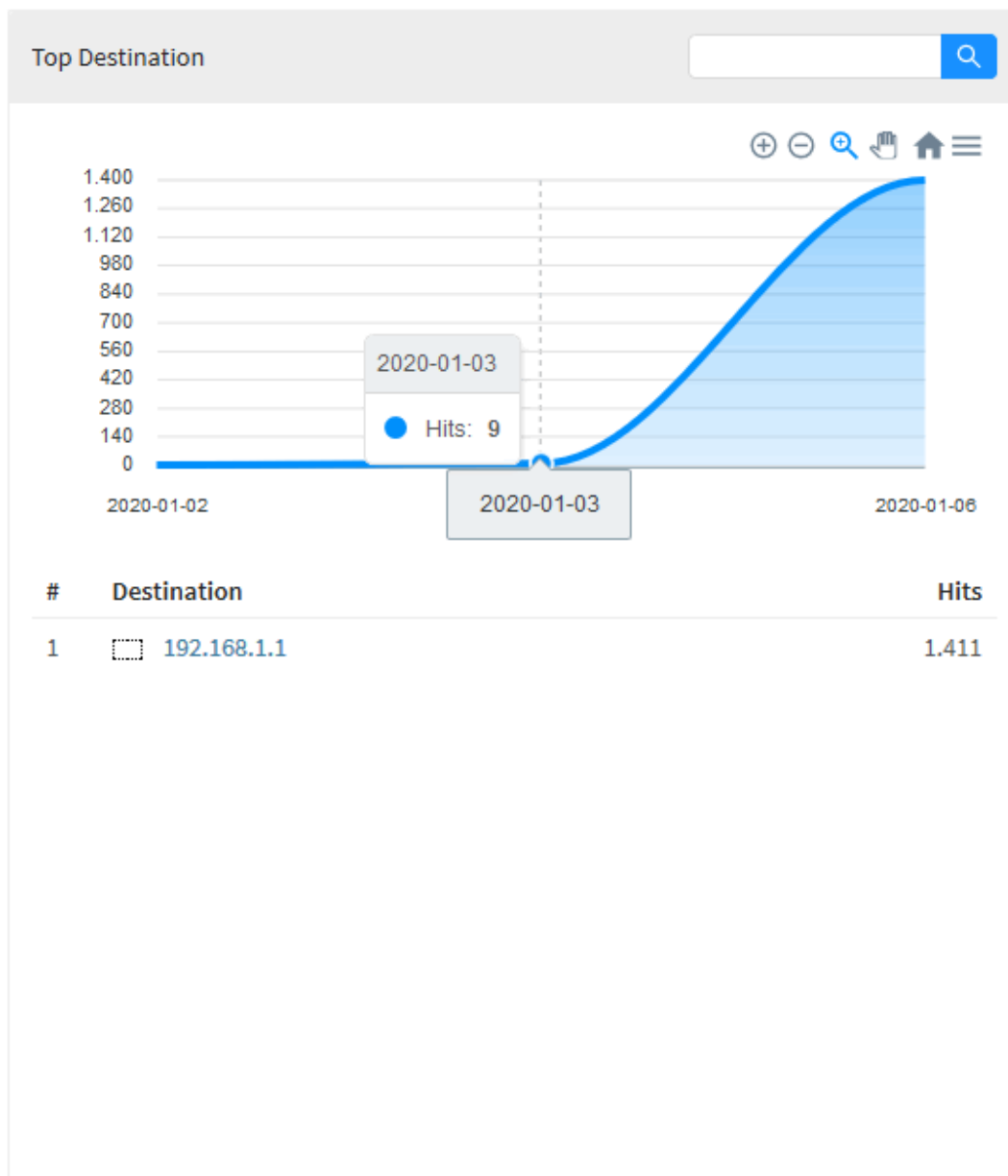
In “Top Destination” there is a line graph showing the ten most recurrent intrusion alert destinations in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of access to these sources generally. Below is a list showing the IPs of the ten destinations with the highest amount of access. Ao clicar em um dos IPs ou uma das categorias, você será redirecionado para [Events](#) usando o item que foi clicado como filtro, criando assim, um relatório mais específico de modo a ter uma visão mais precisa a respeito do item selecionado.

Top Destination

The chart displays the number of hits for the top destination, 192.168.1.1, over a five-day period from 2020-01-02 to 2020-01-06. The y-axis represents the number of hits, ranging from 0 to 1,400 in increments of 140. The x-axis shows the dates. The data shows a period of zero hits from 2020-01-02 to 2020-01-03, followed by a rapid increase, reaching a peak of 1,411 hits on 2020-01-06.

#	Destination	Hits
1	192.168.1.1	1,411

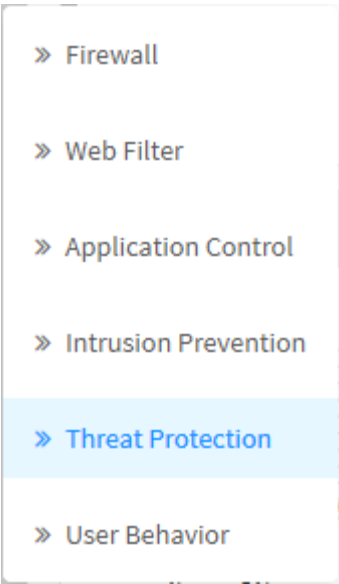
When hovering the mouse over the graph, it will highlight the date and the number of accesses of the highest class of this specific day:



Top Destination - Access Summary

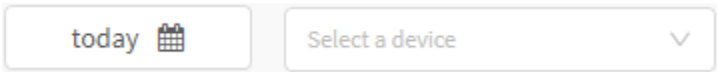
# Threat Protection

To access the Threat Protection reports, click on the “Analysis” icon located on the left side, a dropdown menu will be displayed, select the “Threat Protection” option.



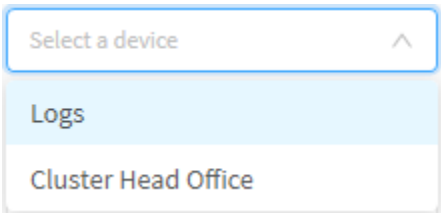
Threat Protection

To generate a report, locate the checkbox that is positioned at the top right of the screen, as shown below:



Selection box

In this checkbox will be listed all devices (or groups of devices) previously registered in [Device Manager](#), to create a report, select the desired device.




Selecting Device


Right on the right side where we just selected the devices, it is possible to see a date selection box, the purpose of which is basically to allow even more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date (“Start date”) to an end date (“End date”);
- **Today:** Displays results specifically for today’s date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.



Today 


Period:

Today 

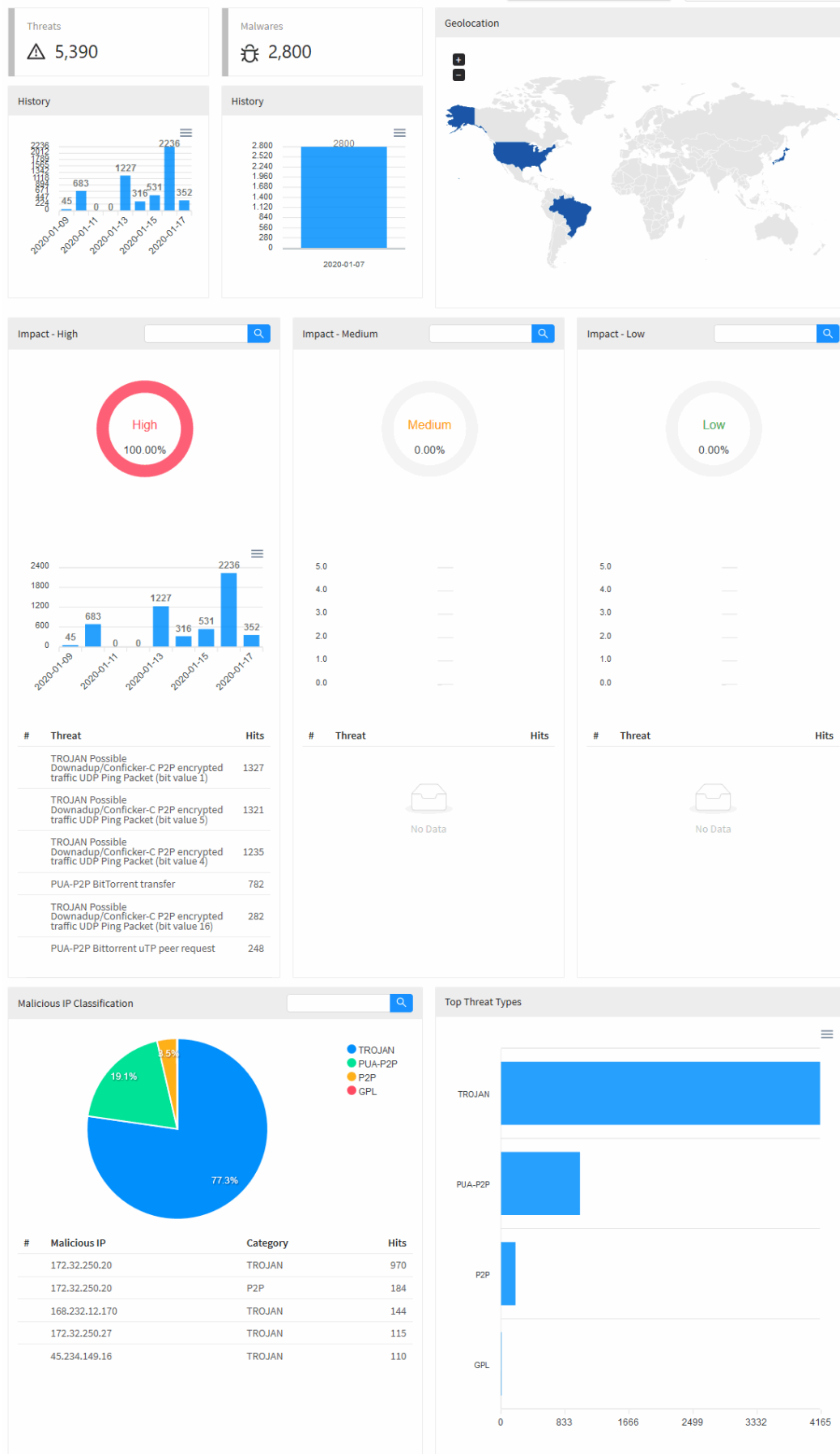
Cancel

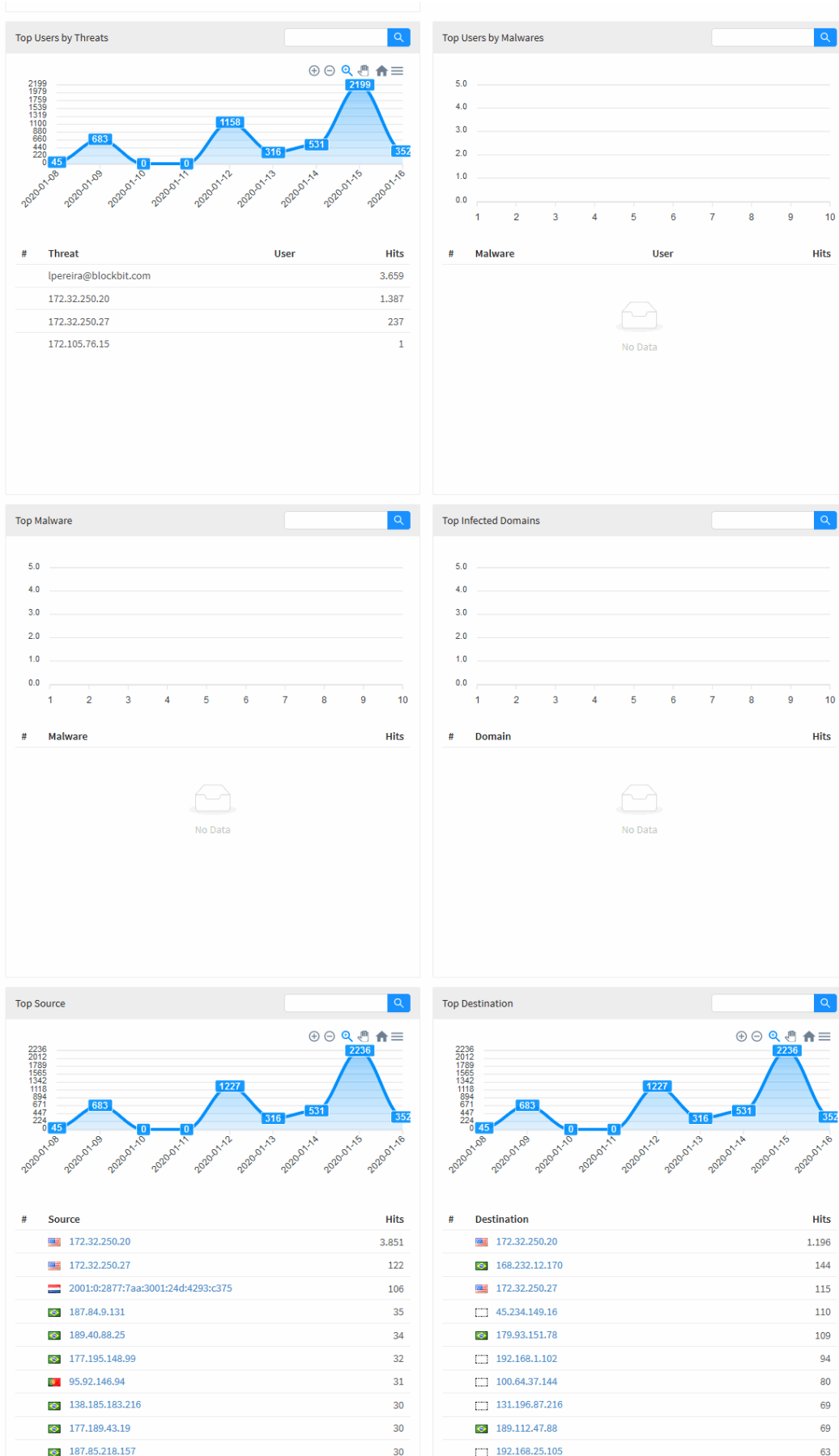
OK

Date Selection

Select the desired date and click [  ] button;







## Threats






Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- : Its function is to zoom;
- : Its function is to remove the zoom;
- : It serves to make a selection zoom;
- : Serves to move the graph;
- : Reset the graph to the starting position;
- : Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

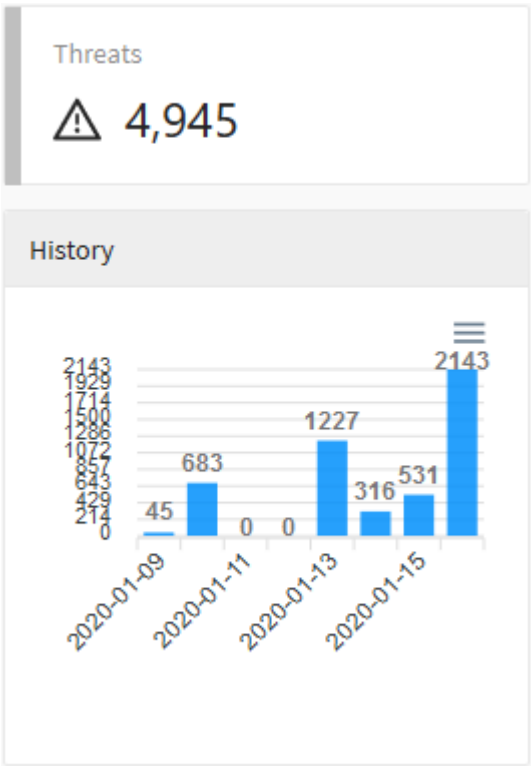
To perform a search, type a term in the search bar and click the search  button.

Next, we will analyze in detail the components of "Threat Protection":

- [Threats and History](#);
- [Malwares and History](#);
- [Geolocation](#);
- [Impact - High](#);
- [Impact - Medium](#);
- [Impact - Low](#);
- [Malicious IP Classification](#);
- [Top Threat Types](#);
- [Top Users by Threats](#);
- [Top Users by Malware](#);
- [Top Malware](#);
- [Top Infected Domains](#);
- [Top Source](#);
- [Top Destination](#).

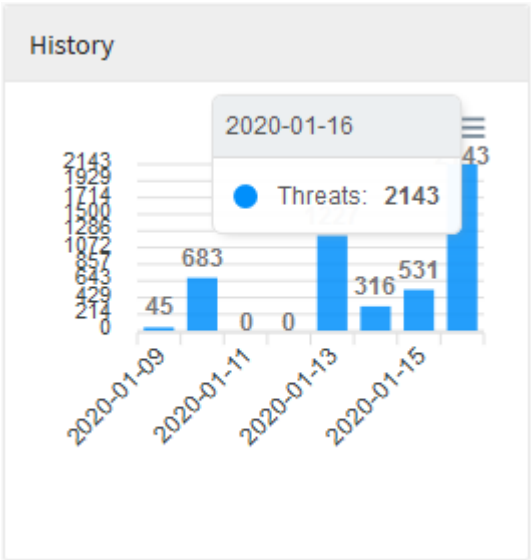
# Threat Protection - Threats and History

The "Threats" panel displays a total of detected threats. Below, the history is displayed in a line graph showing the number of threats detected per day. For more information about the navigation menu at the top of this graph check this [page](#).



Threat Protection - Threats and History

When you hover your mouse over the graph, a summary of the threats for the period is displayed, as shown in the image below:

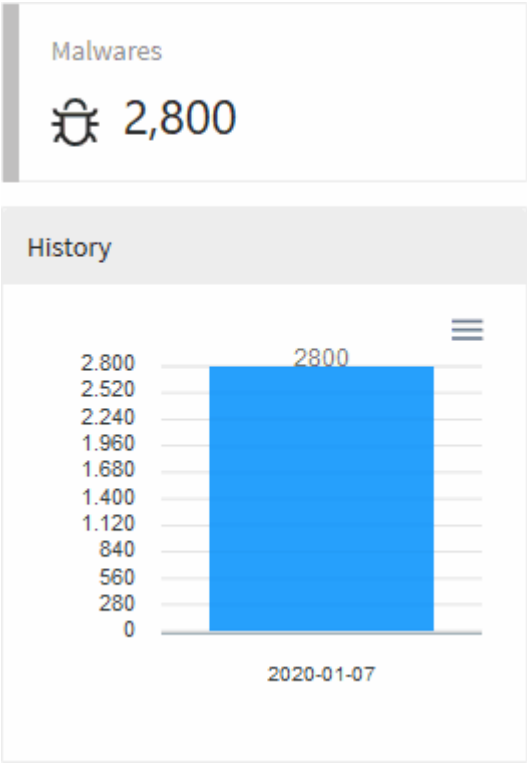


Threat Protection - History - Threat Summary

# Threat Protection - Malwares and History

In "Malwares", a number is displayed totaling the amount of malware detected. Below, the history is displayed in a bar graph showing the amount of threats detected per day.

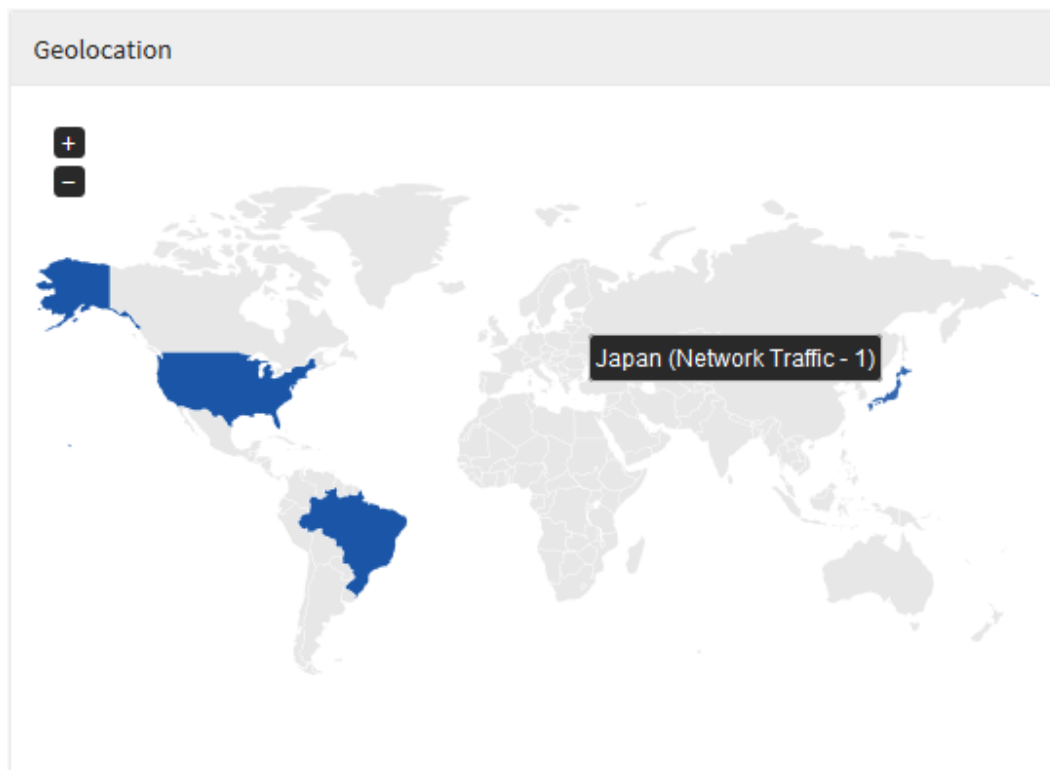
For more information about the navigation menu at the top of this graph, check this [page](#).



Threat Protection - Malware and History

# Threat Protection - Geolocation

In "Geolocation" the source of the threats by geolocation is displayed, the global map shows the level of risk through a colored legend. When hovering the mouse over the countries a total number of threats is displayed, when doing the same with the legend it is possible to view an average, in addition, the country for that value is highlighted on the map.



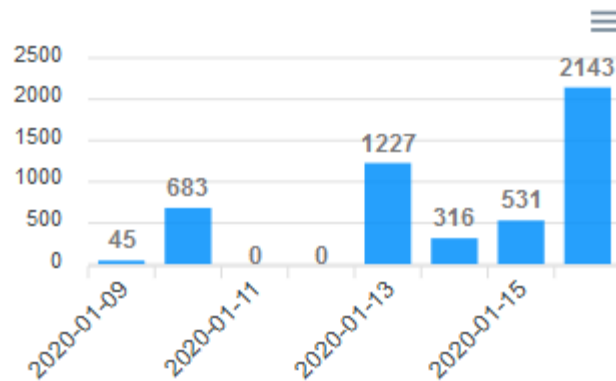
Threat Protection – Geolocation

# Threat Protection - Impact - High

In "Impact - High" we have a donut chart showing the percentage of high impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring high-impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this [page](#).



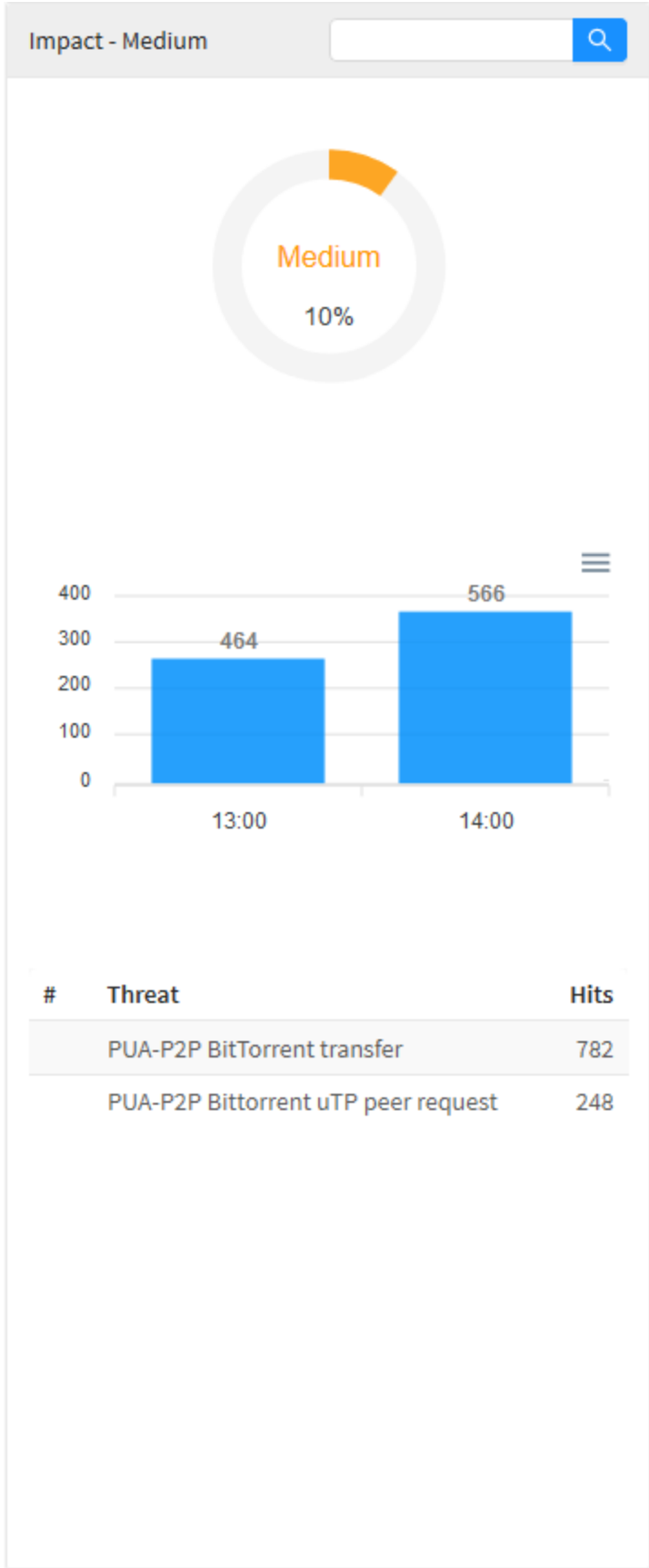


#	Threat	Hits
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	1191
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	1150
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	1109
	PUA-P2P BitTorrent transfer	782
	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 16)	270
	PUA-P2P Bittorrent uTP peer request	248

## Threat Protection – Impact - Medium

In “Impact - Medium” we have a donut chart showing the percentage of medium impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic of the day. In addition, a list is displayed with the 10 most recurring medium impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this [page](#).

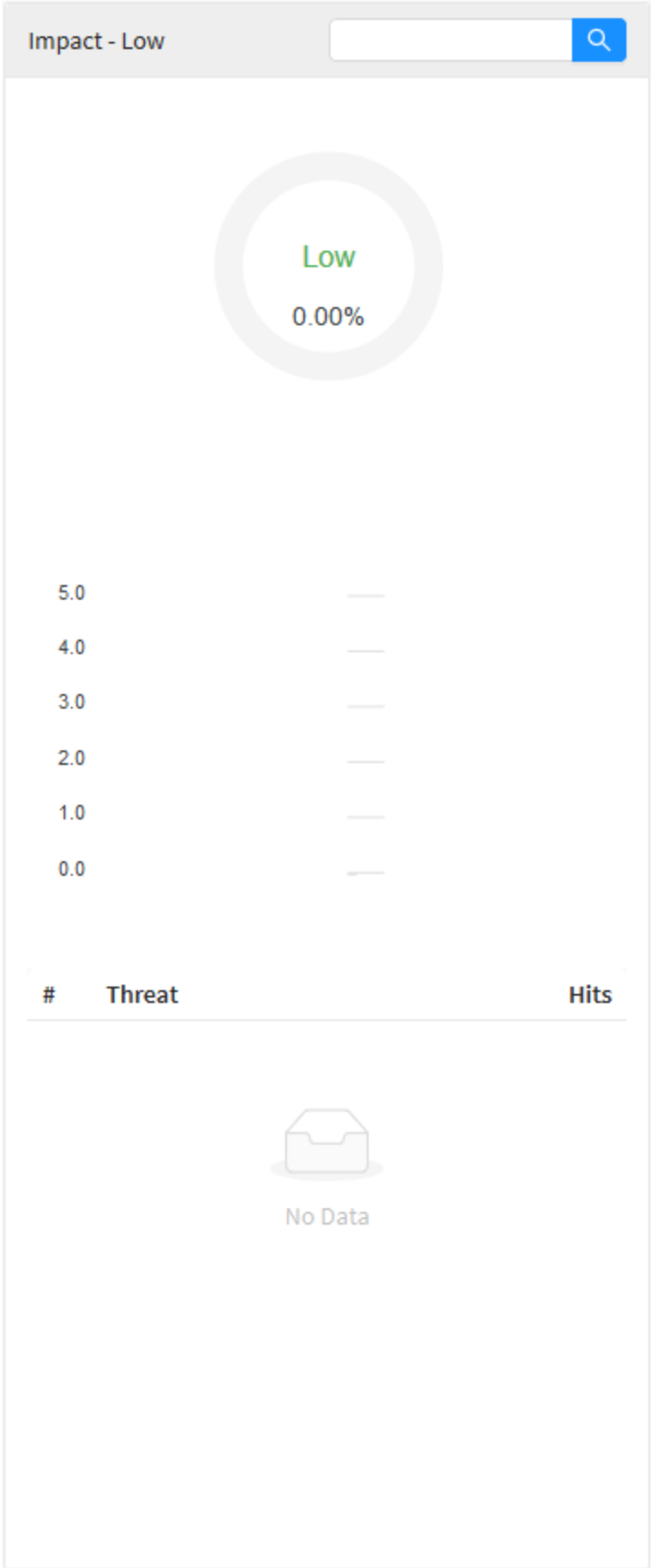


Threat Protection – Impact Medium

## Threat Protection – Impact - Low

In “Impact - Low” we have a donut chart showing the percentage of low impact threats, followed by a column diagram showing how many of these occurred within the previously selected timeframe compared to the network traffic for the day. In addition, a list is displayed with the 10 most recurring low-impact threats, displaying their name and listing them by number of recurrences.

For more information about the search bar at the top of this graph check this [page](#).

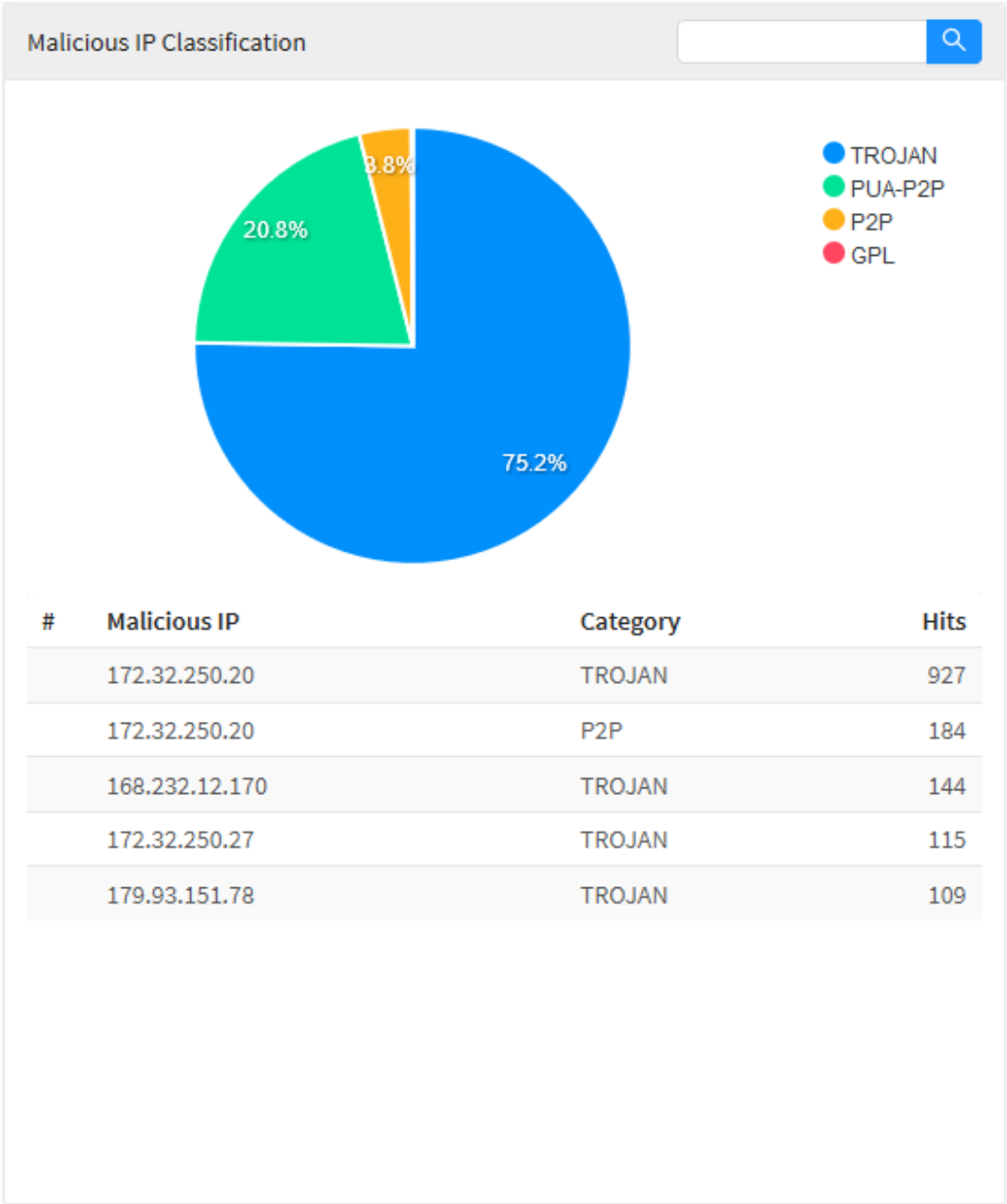


Threat Protection – Impact Low

# Threat Protection – Malicious IP Classification

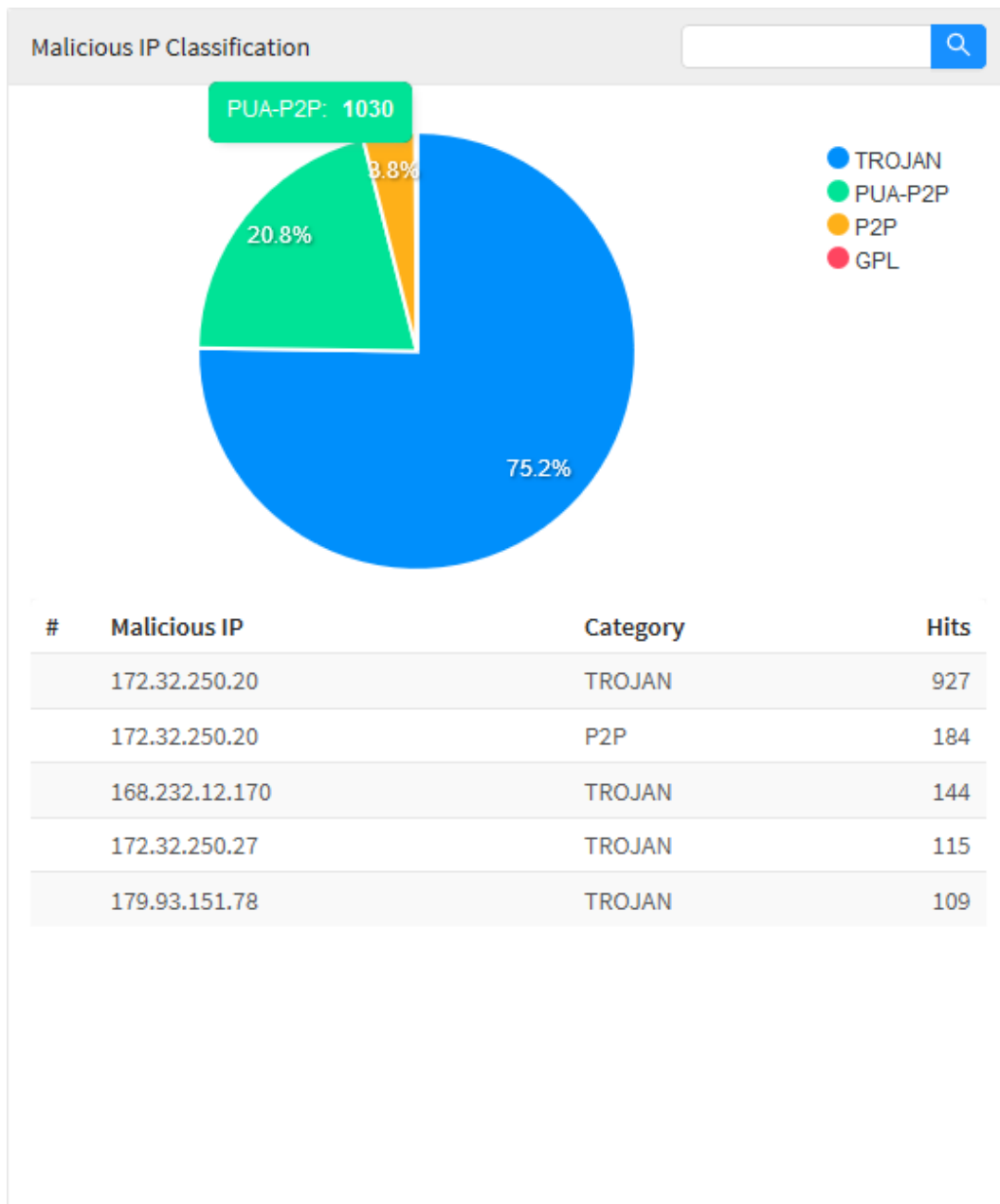
In “Malicious IP Classification” we have a donut chart showing the ten most detected categories of Malicious IP alerts on the network, when you hover over each part of the graph or its corresponding text, it will highlight it and display a number with the amount of accesses to this IP category and its corresponding percentage in relation to the other categories. Just below the graph, we have a list of the ten IPs that most accessed these categories, ordered by number of accesses.

For more information about the navigation menu and the search bar at the top of this graph check this [page](#).



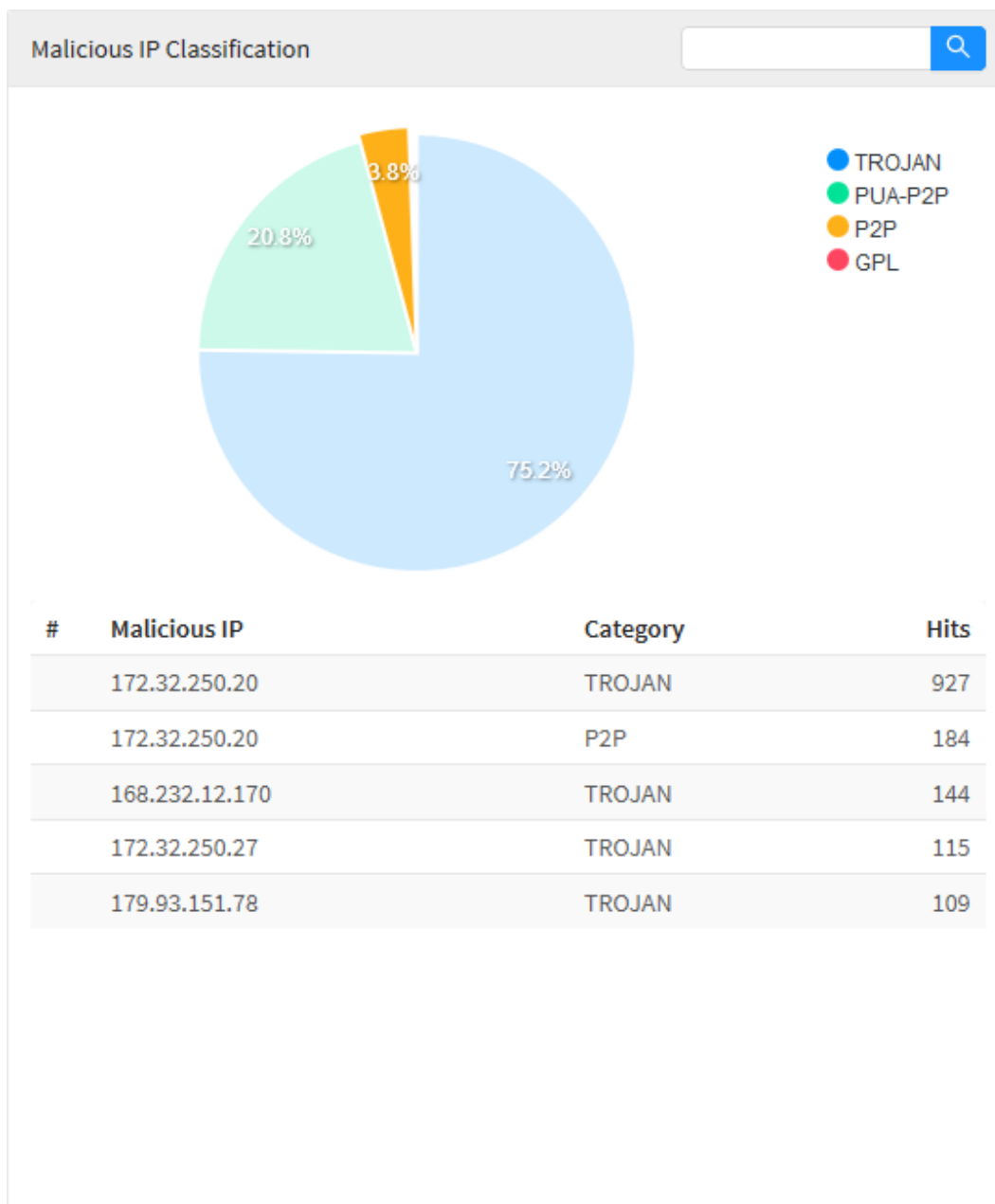
Threat Protection – Malicious IP Classification

When you hover your mouse over the graph, it will display a number with the amount of malicious IPs, as shown in the image below:



Threat Protection – Malicious IP Classification - Summary

When hovering the mouse over the legend, the graphic will be highlighted, as shown below:

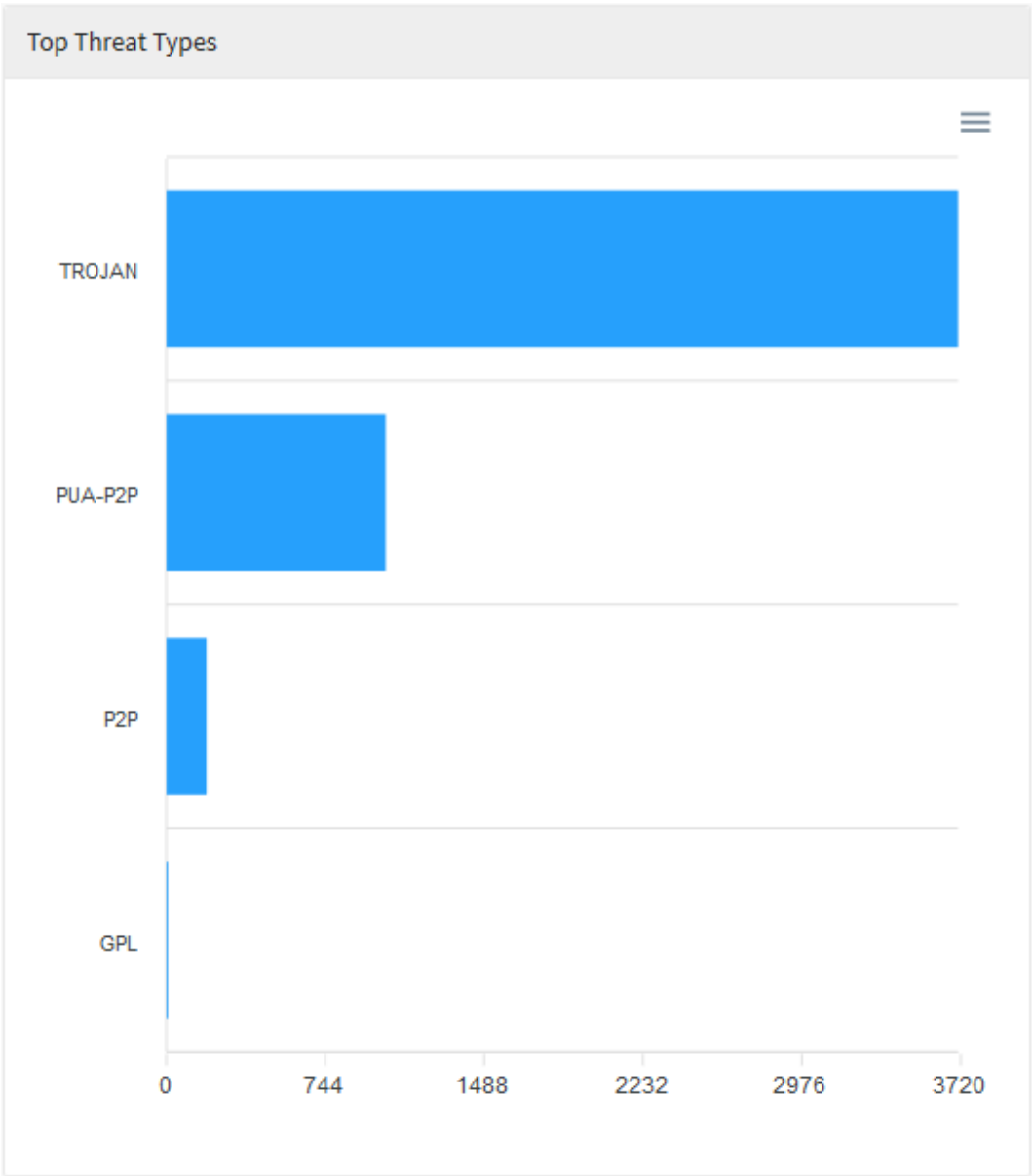


Threat Protection – Malicious IP Classification - Summary



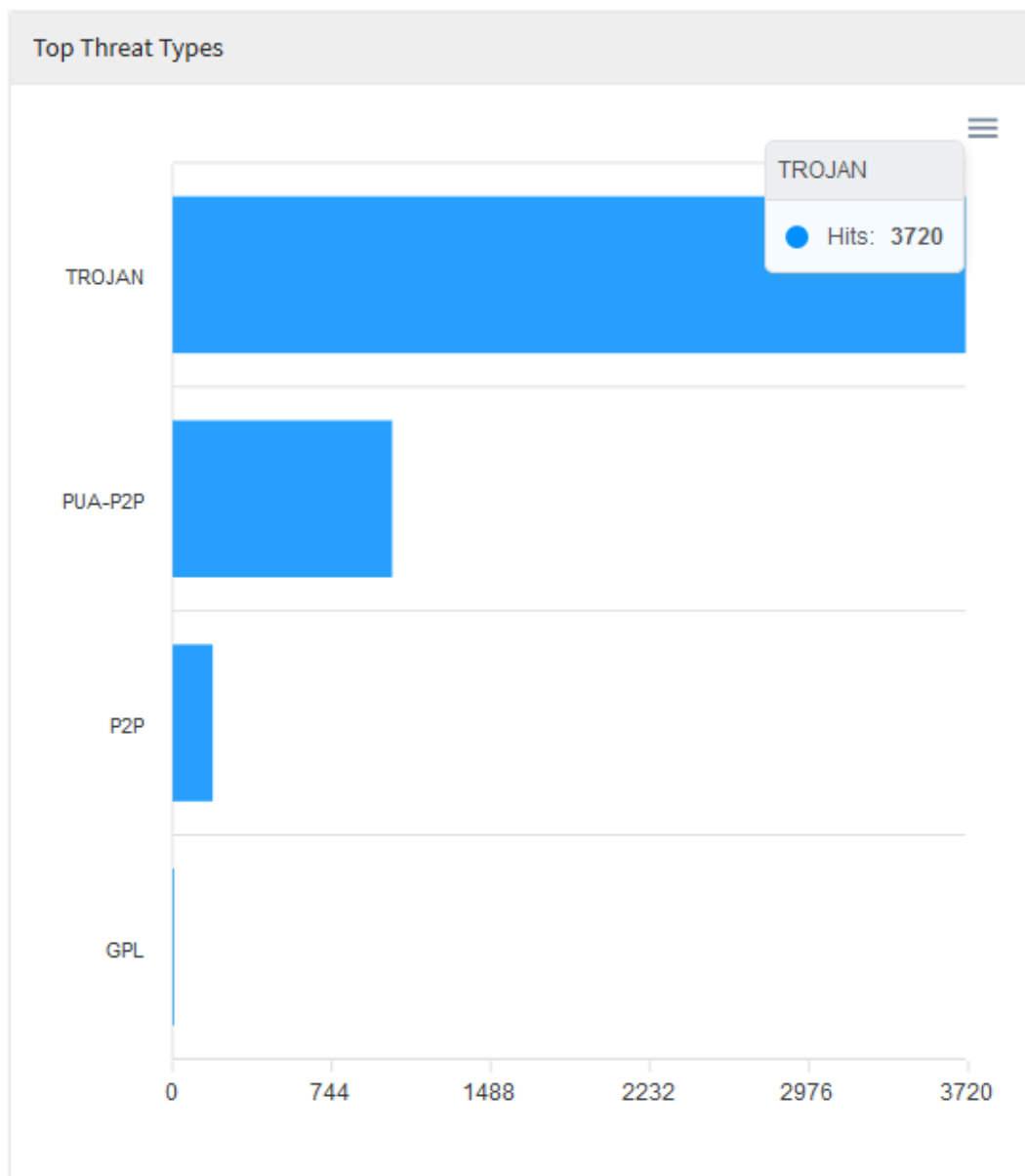
# Threat Protection – Top Threat Types

In "Top Threat Types" a bar graph is displayed representing the most recurrent threat types in relation to the number of times they were detected. For more information about the navigation menu at the top of this graph check this [page](#).



Threat Protection – Top Threat Types

Hovering the mouse over the graph will show the exact amount of detections:



Threat Protection – Top Threat Types - Summary

In "Top Users by Threats" we have a line graph showing the amount of threats per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of threats for the selected day. Just below the graph, we have a list of the ten users who were most affected by these threats, ordered by number of hits.

**Top Users by Threats**

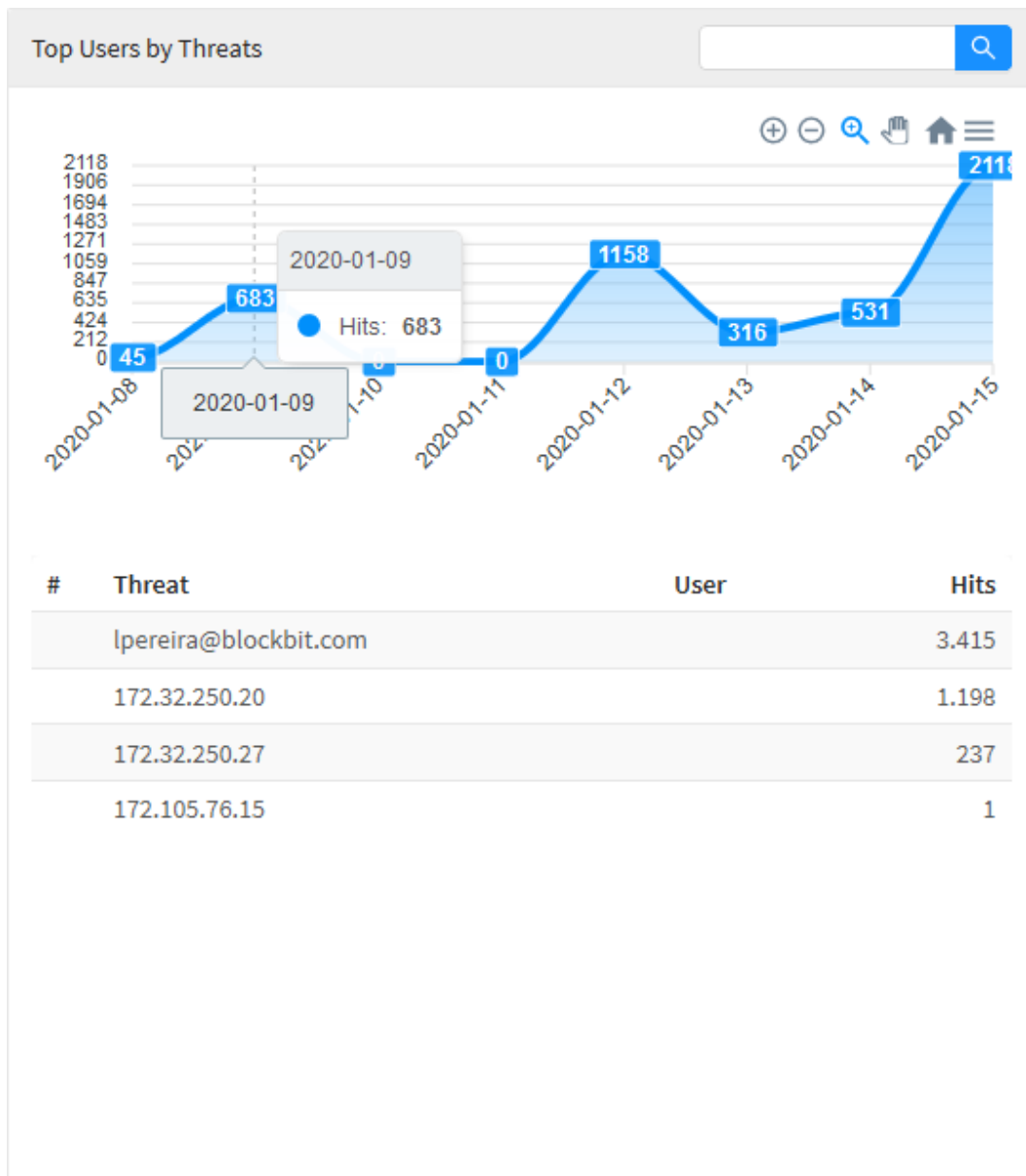
The chart displays the number of threats received by top users over a seven-day period. The Y-axis represents the number of threats, ranging from 0 to 2118. The X-axis shows dates from 2020-01-08 to 2020-01-15. The data points are as follows:

Date	Threats
2020-01-08	45
2020-01-09	683
2020-01-10	0
2020-01-11	0
2020-01-12	1158
2020-01-13	316
2020-01-14	531
2020-01-15	2118

Below the chart, a table lists the top users and the number of hits they received:

#	Threat	User	Hits
1	lpereira@blockbit.com		3.415
2	172.32.250.20		1.198
3	172.32.250.27		237
4	172.105.76.15		1

When hovering the mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:

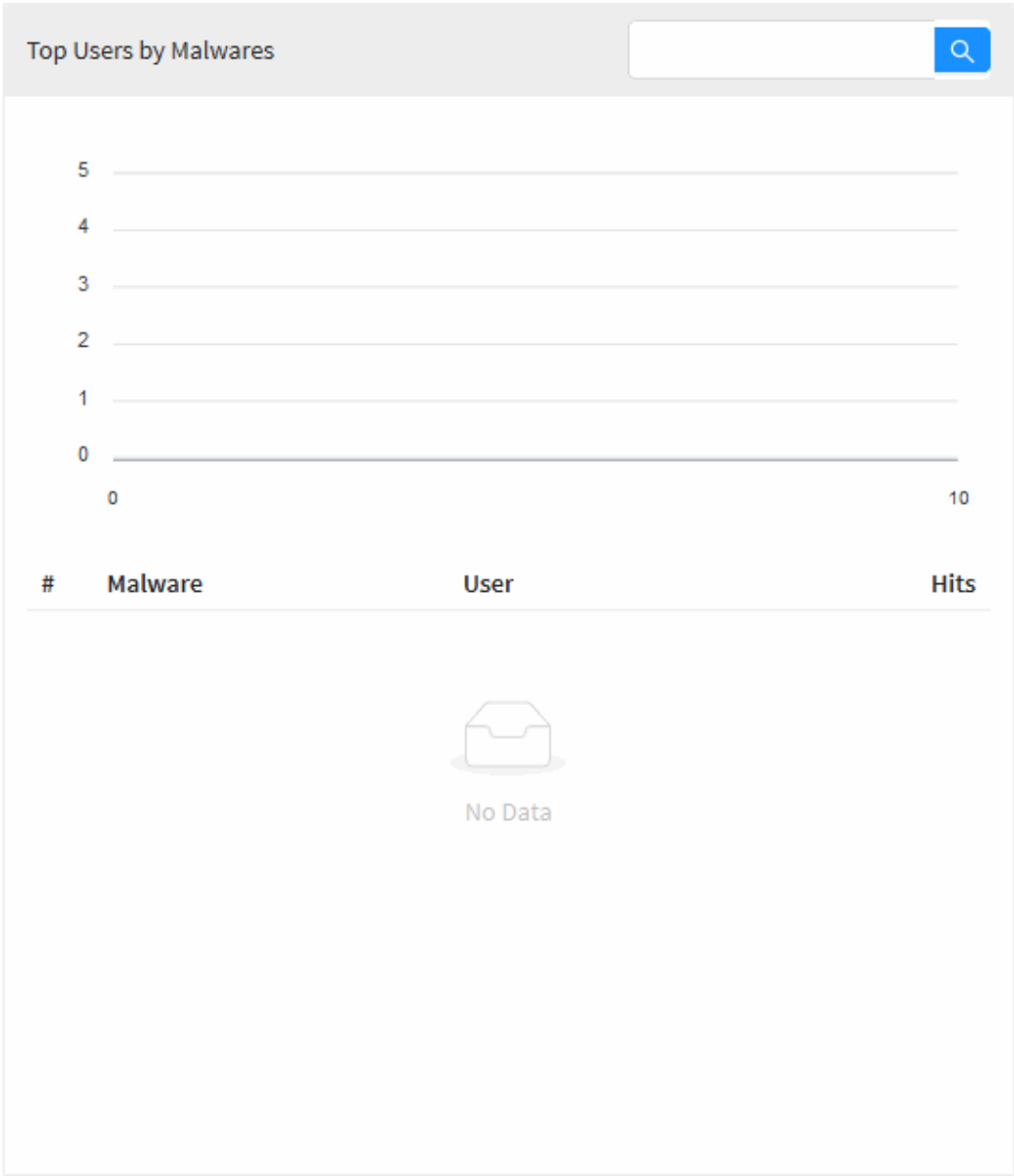


Threat Protection – Top Users by Threats - Summary

# Threat Protection – Top Users by Malware

In “Top Users by Malware” we have a line graph showing the amount of malware alert per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of threats for the selected day. Just below the graph, we have a list of the ten users who were most affected by malware ordered by the amount of detections. Below the graph, we have a list of the ten users who were most affected by these threats, ordered by the number of accesses. Finally, when clicking on one of these users or IPs, you will be redirected to Events using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected user.

For more information about the search bar at the top of this graph check this [page](#).



Threat Protection – Top Users by Malware

# Threat Protection – Top Malware

In "Top Malware" we have a line graph showing the amount of malware detected per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of detections for the selected day. Just below the graph, we have a list of the ten most recurring malware ordered by the amount of detections.

For more information about the search bar at the top of this graph check this [page](#).



Threat Protection – Top Malware

# Threat Protection – Top Infected Domains

In “Top Infected Domains” we have a line graph showing the amount of infected domains detected per day, when hovering over each part of the graph, it will highlight it and display a number with the amount of detections for the selected day. Just below the graph, we have a listing of the ten most recurring domains ordered by the amount of detections.

For more information about the search bar at the top of this graph check this [page](#).



Threat Protection – Top Infected Sites

In "Top Source" a line graph is displayed representing the ten most recurrent threat sources in relation to the previously specified period of time, when hovering over the graph it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten sources previously mentioned, which are classified in order of the highest amount of accesses. When you click on one of the IPs or one of the categories, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected threat source.

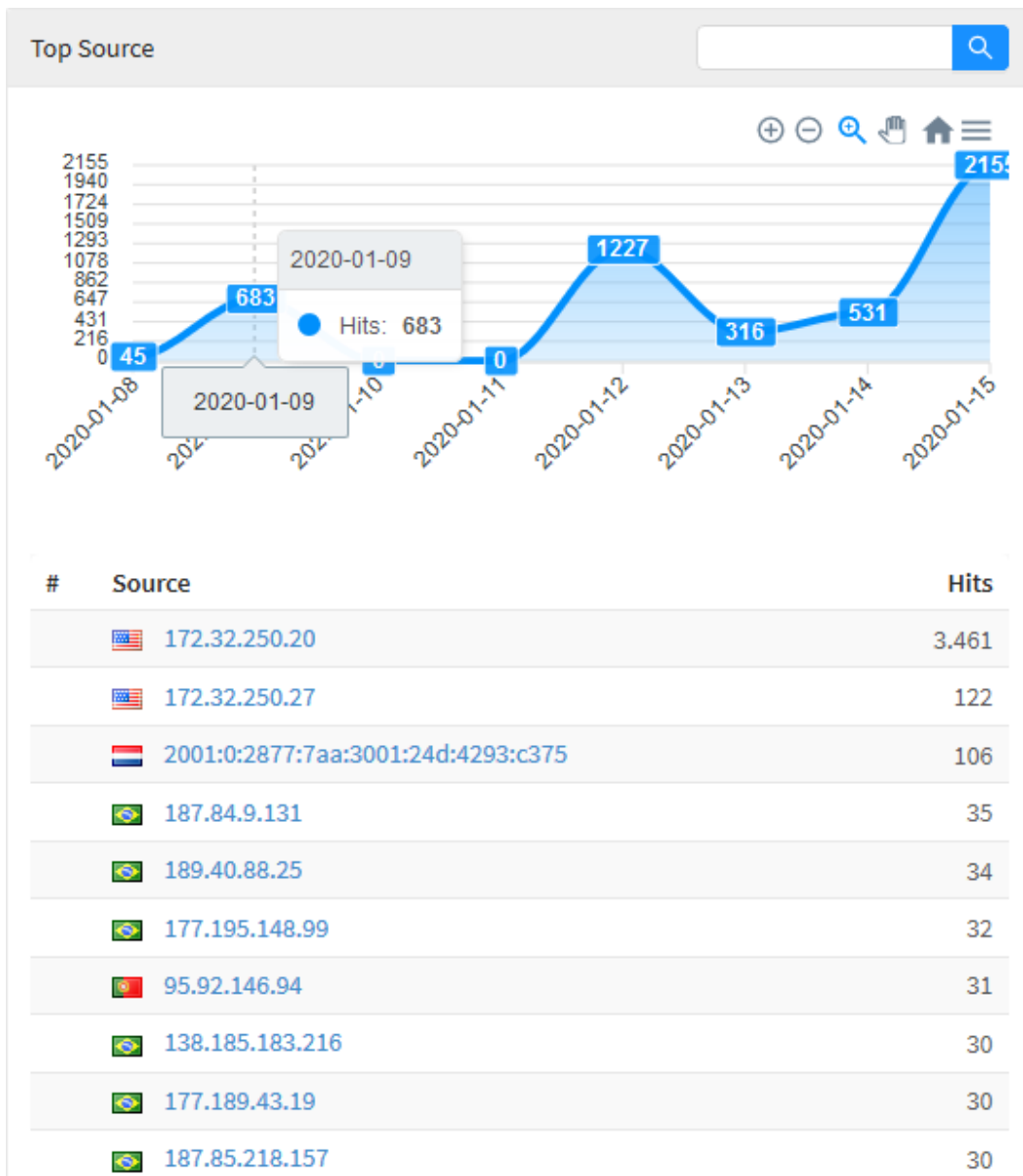
**Top Source**

Date	Hits
2020-01-08	45
2020-01-09	683
2020-01-10	0
2020-01-11	0
2020-01-12	1227
2020-01-13	316
2020-01-14	531
2020-01-15	2155

#	Source	Hits
1	172.32.250.20	3.461
2	172.32.250.27	122
3	2001:0:2877:7aa:3001:24d:4293:c375	106
4	187.84.9.131	35
5	189.40.88.25	34
6	177.195.148.99	32
7	95.92.146.94	31
8	138.185.183.216	30
9	177.189.43.19	30
10	187.85.218.157	30

When hovering the mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:





Threat Protection – Top Source - Summary

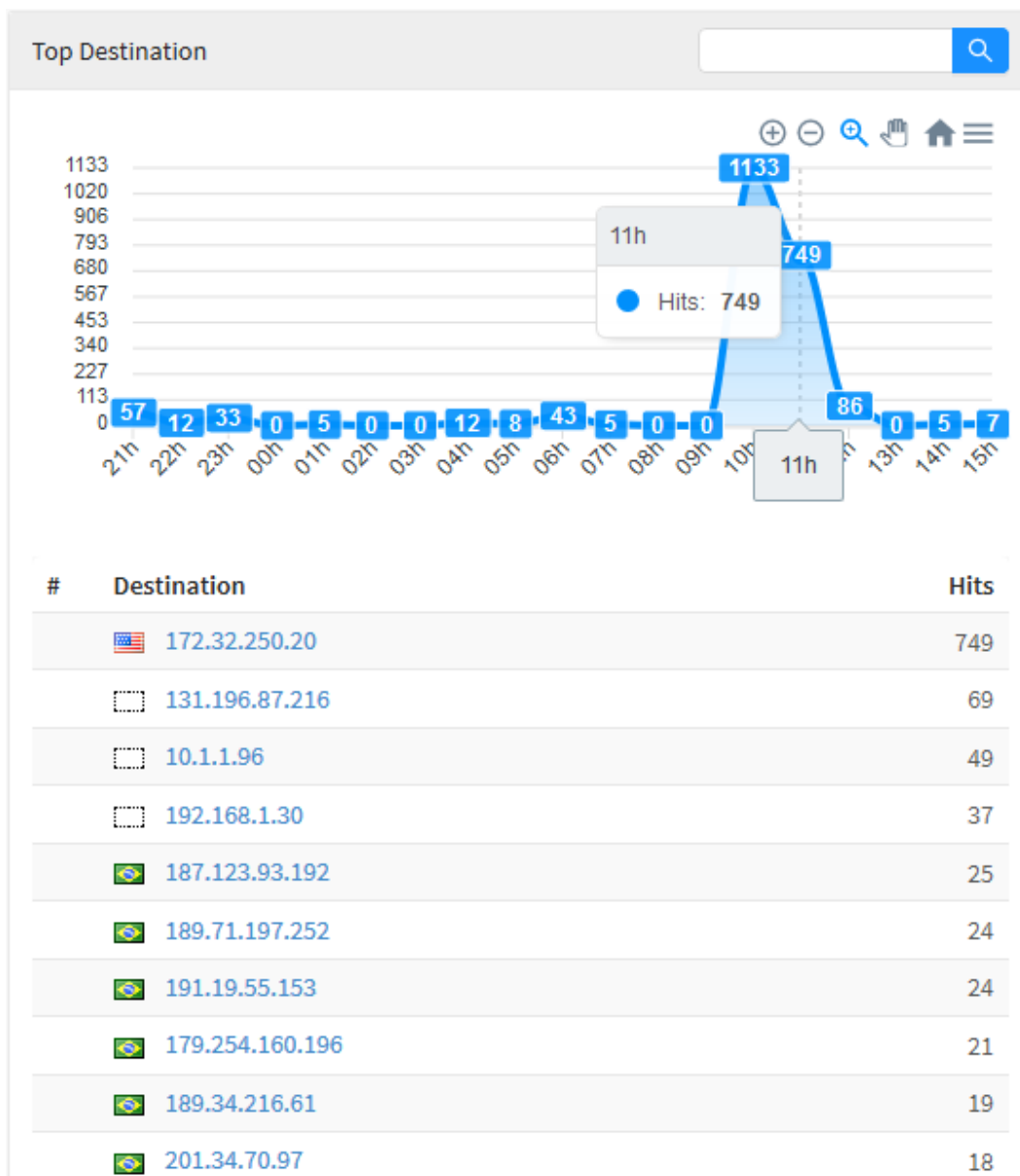
In "Top Destination" a graphic is displayed representing the ten most recurrent threat destinations in relation to the previously specified period of time, when hovering over the graphic it will show the date and the amount of accesses to these sources in general. Below is a list showing the IPs of these same ten destinations previously mentioned and these are classified in order of the highest amount of accesses. When you click on one of the IPs, you will be redirected to [Events](#) using the item that was clicked as a filter, thus creating a more specific report in order to have a more accurate view of the selected threat source.

Top Destination

Hour	Hits
21h	57
22h	12
23h	33
00h	0
01h	5
02h	0
03h	0
04h	12
05h	8
06h	43
07h	5
08h	0
09h	0
10h	1133
11h	749
12h	86
13h	0
14h	5
15h	7

#	Destination	Hits
1	172.32.250.20	749
2	131.196.87.216	69
3	10.1.1.96	49
4	192.168.1.30	37
5	187.123.93.192	25
6	189.71.197.252	24
7	191.19.55.153	24
8	179.254.160.196	21
9	189.34.216.61	19
10	201.34.70.97	18

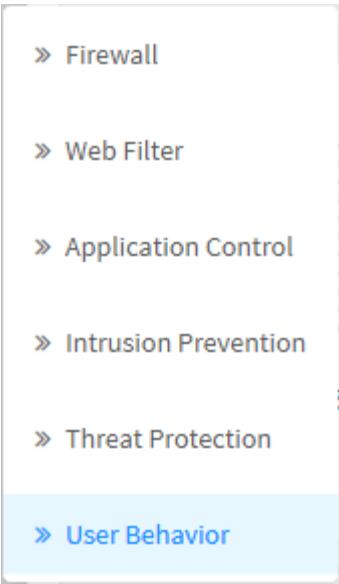
When hovering the mouse over the graph, a summary of the results within the selected period is displayed, as shown in the image below:



Threat Protection – Top Destination - Summary

# User Behavior

To access the reports available in "User Behavior", click on the "Analysis" icon located on the left side, a dropdown menu will be displayed, select the "User Behavior" option.

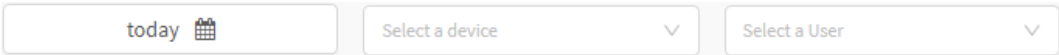


User Behavior

The "User Behavior" report is a summary of the behavior of a given user of a device, within a specific period of time. The reports provided are a summary of the information previously mentioned, but being applied specifically to that user.

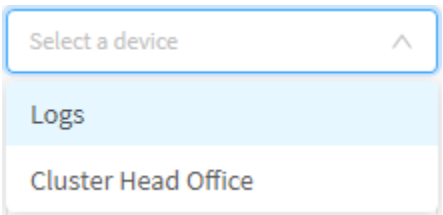
To generate a new report, it will be necessary to select the desired device, then the user to be analyzed and finally, to determine a date. Once these three data are selected, the reports will be generated.

Locate the checkbox that is positioned at the top right of the screen, as shown below:



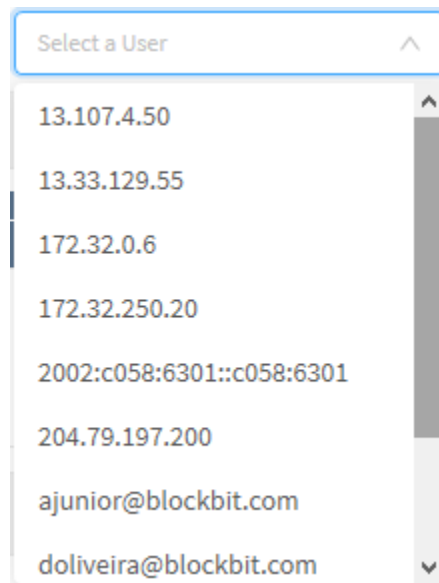
Selection box

In the "Select a device" selection box, all devices (or groups of devices) previously registered in [Device Manager](#) will be listed, to create a report, select the desired device.



Selecting Device

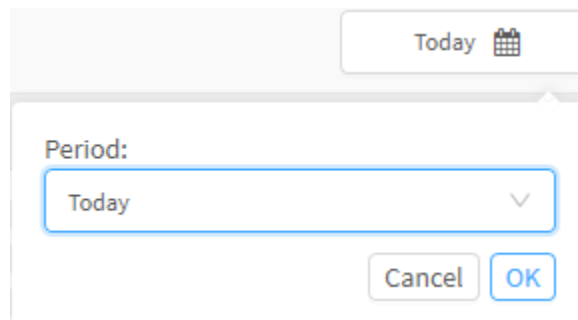
In the "Select a User" selection box, all users of the previously selected device will be listed, select the desired user.




*Selecting the user*

Finally, the date selection box aims to allow more accurate filtering of results, the possible options are:

- **By date:** Determines a specific date;
- **By period:** Displays results from an initial date ("Start date") to an end date ("End date");
- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.









*Date Selection*

Select the desired date and click [  ] button;


Most of the graphics on this tab have a navigation menu and a search bar.

The navigation menu has the following buttons:

- [  ]: Its function is to zoom in;
- [  ]: Its function is to remove the zoom;
- [  ]: It serves to make a selection zoom;
- [  ]: It serves to move the graph;

- []: Reset the graph to the starting position;
- []: Allow to download this diagram in svg, png or csv format.

The search bar allows you to search for a specific item and modify the diagrams according to the search results.

To perform a search, type a term in the search bar and click the search [] button.

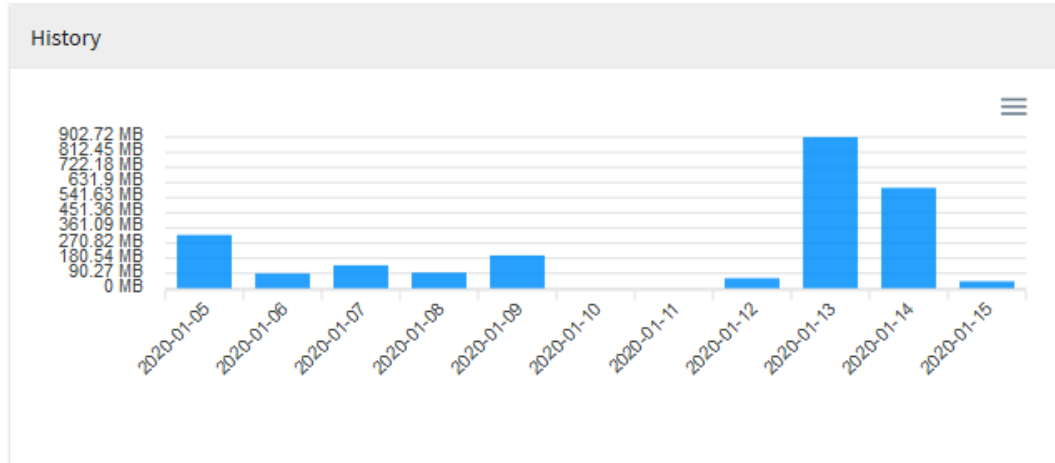
Below, we will analyze each of these reports in detail:

- [History](#);
- [Analysis Panel](#);
- [Geolocation Information](#).

## User Behavior - History

In "History" a vertical bar graph is displayed showing the traffic consumption in Megabytes in relation to the pre-selected days, the arrow in the middle of the graph represents the average consumption of users in general. When you hover your mouse over one of the columns in the graph, the exact amount of traffic in Megabytes for each day is displayed.

For more information about the navigation menu at the top of this graph check this [page](#).



### User Behavior - History

# User Behavior - Analysis Panel

In "Analysis Panel" we have a summary of various information cited in the reports previously analyzed, but this time, applied specifically to the user in question.

For more information about the navigation menu at the top of this graph, check this [page](#).



## Analysis Panel

### Network Traffic

Total Traffic

 2.37 GB





#### Top Services



#	Services	Traffic
1	<a href="#">https</a>	1.08 GB
2	<a href="#">admin</a>	548.79 MB
3	<a href="#">ssh</a>	548.9 MB
4	<a href="#">http</a>	4.06 MB
5	<a href="#">rdesktop</a>	221.56 MB





#### Top Source



#	Source	Traffic
1	 <a href="#">172.32.250.20</a>	48.74 KB
2	 <a href="#">172.16.13.246</a>	123 Bytes
3	 <a href="#">172.16.102.130</a>	81 Bytes
4	 <a href="#">192.168.254.252</a>	43 Bytes
5	 <a href="#">172.16.12.27</a>	30 Bytes

Top Destination



#	Destination	Hits
1	 172.16.13.245	2.916
2	 172.16.13.246	2.502
3	 172.16.12.171	1.063
4	 172.31.0.50	558
5	 172.16.13.57	485

## Policy Usage

Policy Tags

w

SSL

Top Profiles



#	Policies	Hits
1	Default (Allow) (Wifi)	24.647
2	Default (Allow) (Wifi) (Copy)	12.246
3	SMB	5.412
4	FORWARD LOCAL	3.962
5	Content Filtering (Wifi)	3.138

## Application Usage

Total Application

 1.74 KB

Top Applications



#	Applications	Hits
1	CDN - Content Delivery Network	1.043
2	Microsoft Update	547
3	HTTP	50
4	Google API SSL	48
5	MSN	18

## Web Usage

Total Traffic

 0

Allowed Sites

 0

Denied Sites

 0

### Top Categories



#	Categories	Hits
1	<a href="#">Information Technology</a>	1.628
2	<a href="#">Search Engines and Portals</a>	763
3	<a href="#">Freeware and Software Download</a>	527
4	<a href="#">Business and Economy</a>	145
5	<a href="#">Web Hosting</a>	91


### Top Destination



#	Ip	Hits
1	<a href="#">2.23.98.145</a>	476
2	<a href="#">201.0.217.42</a>	449
3	<a href="#">13.107.4.50</a>	273
4	<a href="#">52.114.142.2</a>	117
5	<a href="#">191.252.51.215</a>	111

## THREAT PROTECTION

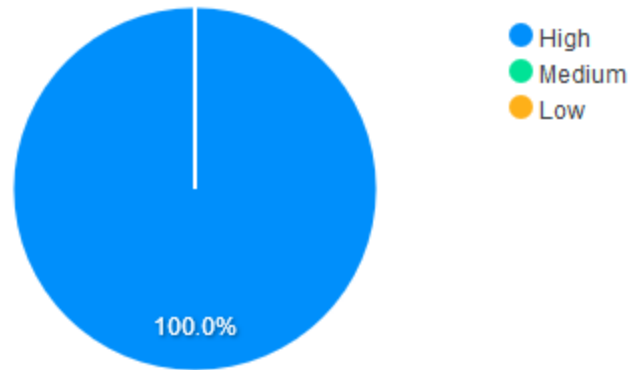
Total Threats

 1,198

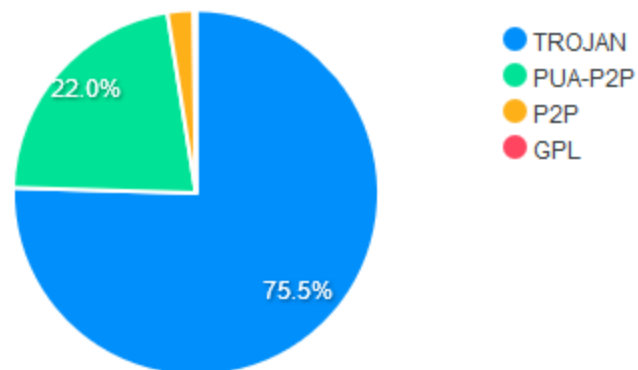
Total Malwares

0

### Impacts



### Malicious IP Classification



### Top Threats

#	Threats	Hits
1	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275

4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

#### Top Malwares



#	Malwares	Hits
---	----------	------



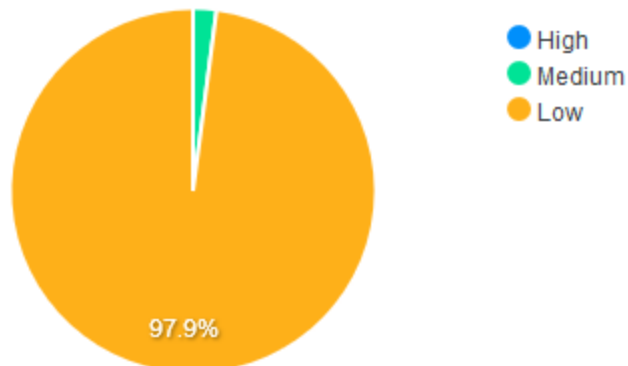
No Data

### INTRUSION PREVENTION

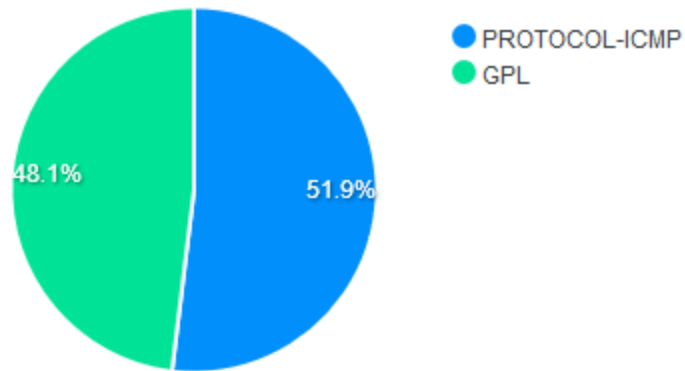
Total Alerts

100,666

#### Impacts



### Intrusion Protection



### Top Alerts

#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Host Unreachable	8.511
4	PROTOCOL-ICMP Destination Unreachable Host Unreachable	8.511
5	GPL ICMP_INFO PING	2.081

User Behavior - Analysis Panel

# User Behavior - Analysis Panel - Network Traffic

Below "Network Traffic" we have:

"Total Traffic", showing the total user traffic in Gigabytes, in "Top Services" a list is displayed with the 10 most used services by the user in question, "Top source" shows the largest sources of user access and "Top Destination" a list of IPs of the destinations most accessed by the user.



## Network Traffic

Total Traffic

 2.37 GB






### Top Services



#	Services	Traffic
1	<a href="#">https</a>	1.08 GB
2	<a href="#">admin</a>	548.79 MB
3	<a href="#">ssh</a>	548.9 MB
4	<a href="#">http</a>	4.06 MB
5	<a href="#">rdesktop</a>	221.56 MB

### Top Source



#	Source	Traffic
1	 <a href="#">172.32.250.20</a>	48.74 KB
2	 <a href="#">172.16.13.246</a>	123 Bytes
3	 <a href="#">172.16.102.130</a>	81 Bytes
4	 <a href="#">192.168.254.252</a>	43 Bytes
5	 <a href="#">172.16.12.27</a>	30 Bytes

Top Destination			
#	Destination	Hits	
1	<input type="checkbox"/> 172.16.13.245	2.916	
2	<input type="checkbox"/> 172.16.13.246	2.502	
3	<input type="checkbox"/> 172.16.12.171	1.063	
4	<input type="checkbox"/> 172.31.0.50	558	
5	<input type="checkbox"/> 172.16.13.57	485	

*User Behavior - Analysis Panel - Network Traffic*

# User Behavior - Analysis Panel - Policy Usage

In "Policy Usage" we have:

"Policy Tags" that shows which Policy Tags were most applied to that user, in "Top Policies" we have the most applied policies for that specific user.

Policy Usage

Policy Tags

w

SSL

Top Profiles

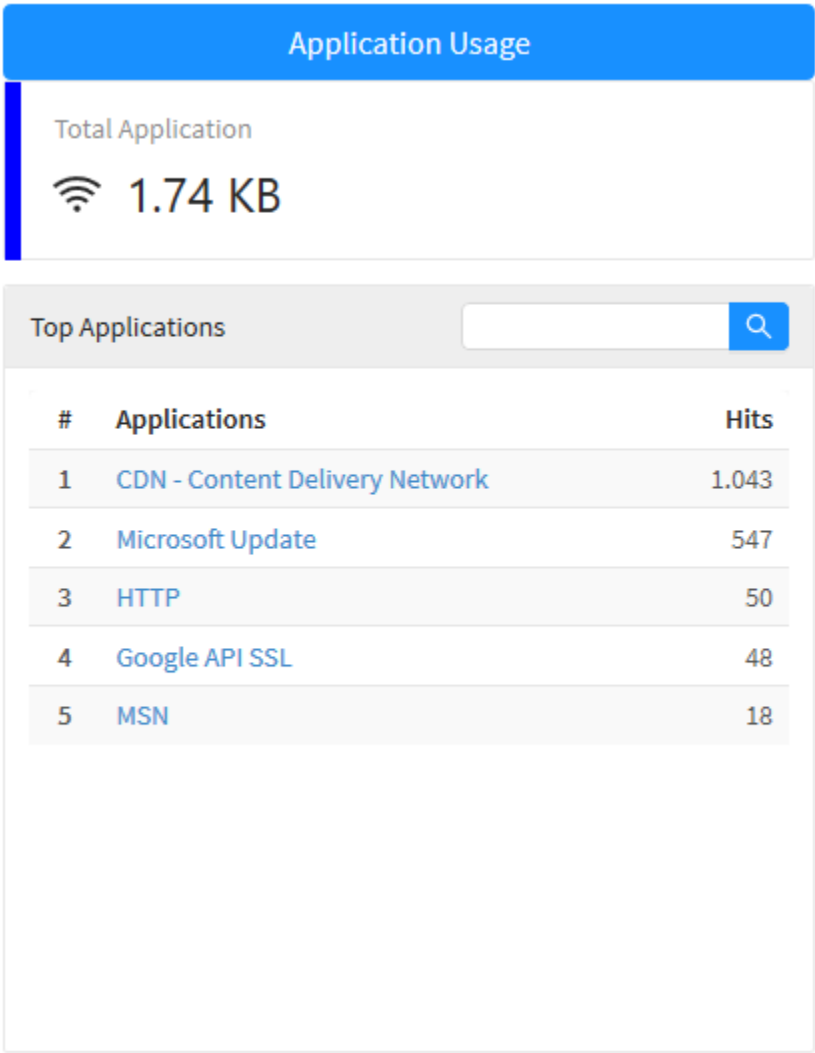
#	Policies	Hits
1	Default (Allow) (Wifi)	24.647
2	Default (Allow) (Wifi) (Copy)	12.246
3	SMB	5.412
4	FORWARD LOCAL	3.962
5	Content Filtering (Wifi)	3.138

Analysis Panel - Policy Usage

# User Behavior - Analysis Panel - Application Usage

In "Application Usage" we have:

"Total Applications" mentions the total number of applications used by the user and "Total Application" which serves to demonstrate the most used applications by the user and the amount of accesses made to them.



Analysis Panel - Application Usage

# User Behavior - Analysis Panel - Web Usage

In "Web Usage" we have:

"Total Traffic" showing a total of the user's network traffic, "Sites Allowed" showing the total number of accesses to permitted sites made by the user, "Sites Denied" showing the total accesses to refused sites made by the user, "Top Categories" a list of user accesses by category and finally, in "Top destination" a list of user accesses by destination showing the IP and amount of accesses to that same.

## Web Usage

Total Traffic

 0

Allowed Sites

 0

Denied Sites

 0

Top Categories



#	Categories	Hits
1	<a href="#">Information Technology</a>	1.628
2	<a href="#">Search Engines and Portals</a>	763
3	<a href="#">Freeware and Software Download</a>	527
4	<a href="#">Business and Economy</a>	145
5	<a href="#">Web Hosting</a>	91

Top Destination



#	Ip	Hits
1	<a href="#">2.23.98.145</a>	476
2	<a href="#">201.0.217.42</a>	449
3	<a href="#">13.107.4.50</a>	273
4	<a href="#">50.111.110.0</a>	117

4	52.114.142.2	117
5	191.252.51.215	111

*Analysis Panel - Web Usage*

# User Behavior - Analysis Panel - Threat Protection

In "Threat Protection" we have:

"Total Threats" showing the total number of threats, "Total Malwares" shows the total number of malware detected on that user, the "Impacts" graph shows the impact levels of the threats previously mentioned, "Malicious IP Classification" displays a graph showing a summary of the classification of malicious IPs accessed by the user, in the "Top Threats" list the 5 most recurring threats to that user are displayed and the amount of accesses made and in "Top Malware" a list of the 5 most detected malware is displayed on the user in question.



## THREAT PROTECTION

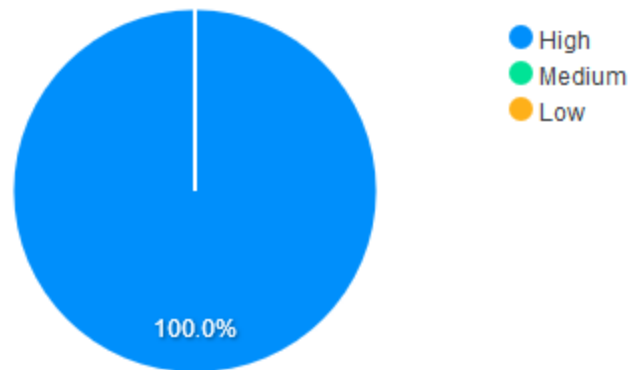
Total Threats

📶 1,198

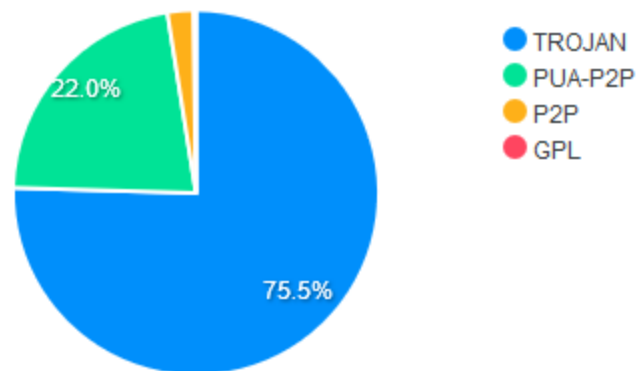
Total Malwares

📶 0

### Impacts



### Malicious IP Classification




### Top Threats

#	Threats	Hits
	TROJAN Possible	

1	Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 1)	308
2	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 5)	298
3	TROJAN Possible Downadup/Conficker-C P2P encrypted traffic UDP Ping Packet (bit value 4)	275
4	PUA-P2P BitTorrent transfer	176
5	PUA-P2P Bittorrent uTP peer request	88

Top Malwares

#	Malwares	Hits
 No Data		

Analysis Panel - Threat Protection

# User Behavior - Analysis Panel - Intrusion Prevention

In "Intrusion Prevention" we have:

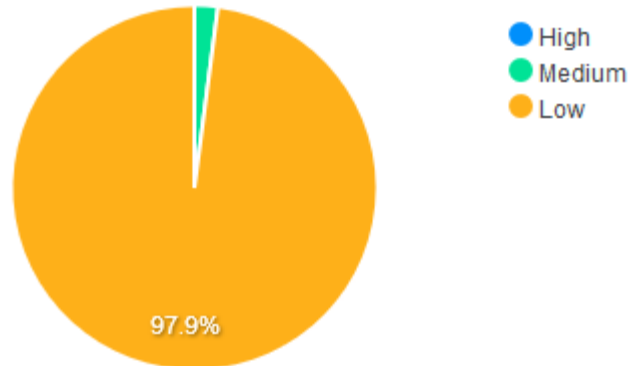
"Total Alerts" showing the total number of alerts for this user, in "Impacts" we have the impact levels of the alerts previously mentioned, "Intrusion Protection" displays a donut chart where it is possible to see the types of intrusions detected by the system and finally, in "Top Alerts" we have a list of the 5 alerts for this user and how many times they occurred.

## INTRUSION PREVENTION

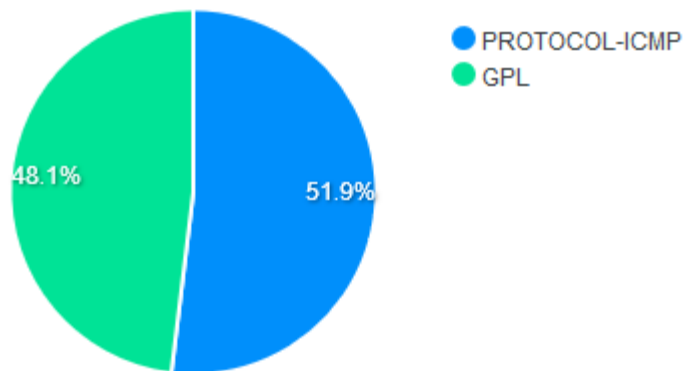
Total Alerts

📶 100,666

### Impacts



### Intrusion Protection



### Top Alerts

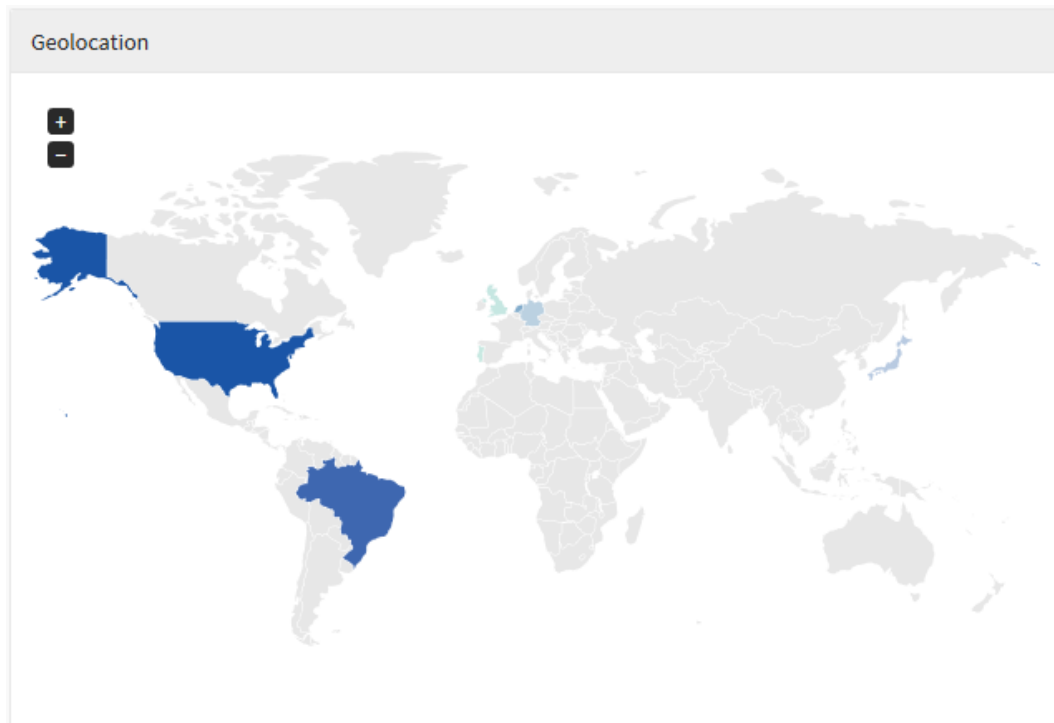
#	Alerts	Hits
1	GPL ICMP_INFO Destination Unreachable Port Unreachable	37.678
2	PROTOCOL-ICMP destination unreachable port unreachable packet detected	37.659
3	GPL ICMP_INFO Destination Unreachable Port Unreachable	8.511

	Unreachable Host Unreachable	
4	PROTOCOL-ICMP Destination Unreachable Host Unreachable	8.511
5	GPL ICMP_INFO PING	2.081

*Analysis Panel - Intrusion Prevention*

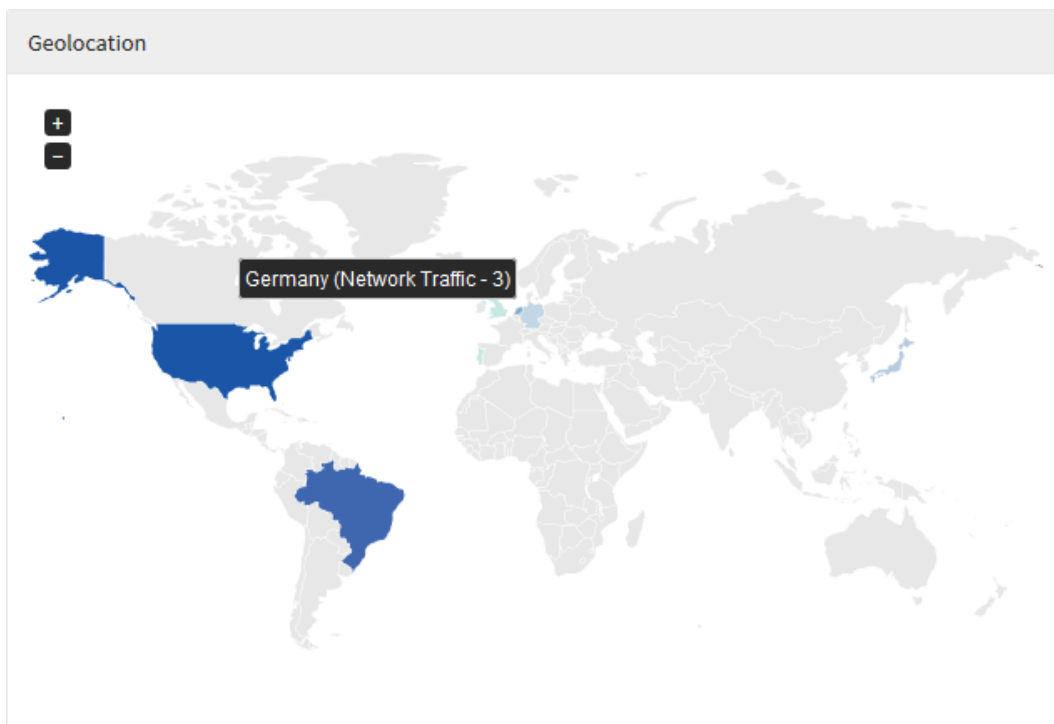
# User Behavior - Geolocation Information

In "Hits by Geolocation" the destination of the connections of that specific user is displayed, the global map shows through a colored legend the amount of accesses made by users for each country.



*User Behavior - Geolocation*

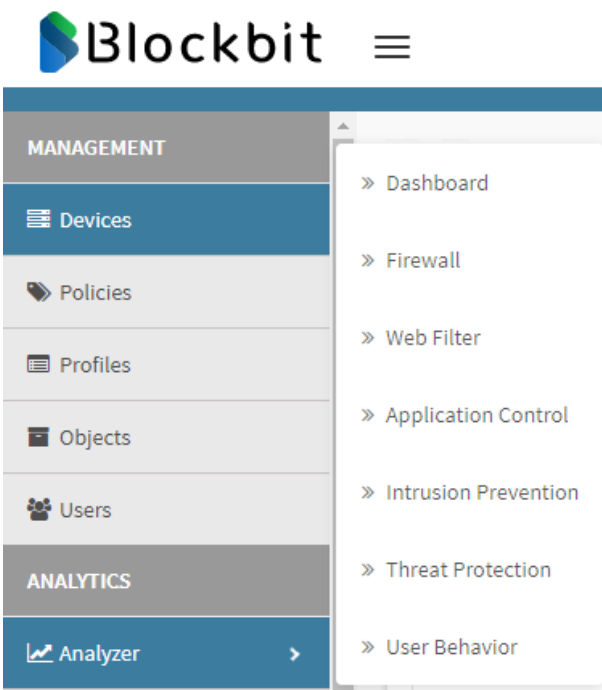
When hovering the mouse over the countries a total number of accesses is displayed, when doing the same with the legend it is possible to view an average, in addition, the country referring to this value is highlighted on the map.





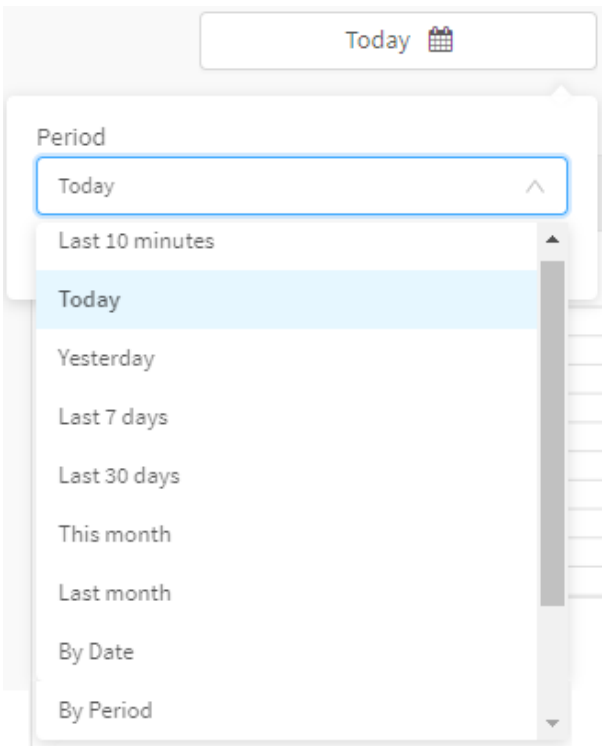
# Dashboard

The Dashboard displays consolidated information from the logs generated by the device or a group of devices in the GSM. The displayed sections are: Firewall, Web Filter, Application Control, Intrusion Prevention, Threat Protection and User Behavior.



Analyzer menu - Dashboard

To see this information on the Dashboard first, select the period of time to be covered and a Device (or all of them), to have them displayed on the user interface:







#### Dashboard - Time period selection

1. This option allows filtering by the following periods of time:
  - a. Today;
  - b. Last 10 minutes;
  - c. Yesterday;
  - d. Last 7 days;
  - e. Last 30 days;
  - f. This Month;
  - g. Last Month;
  - h. By Date;
  - i. By Period;

Dashboard

Today 

Select a Device/Group 

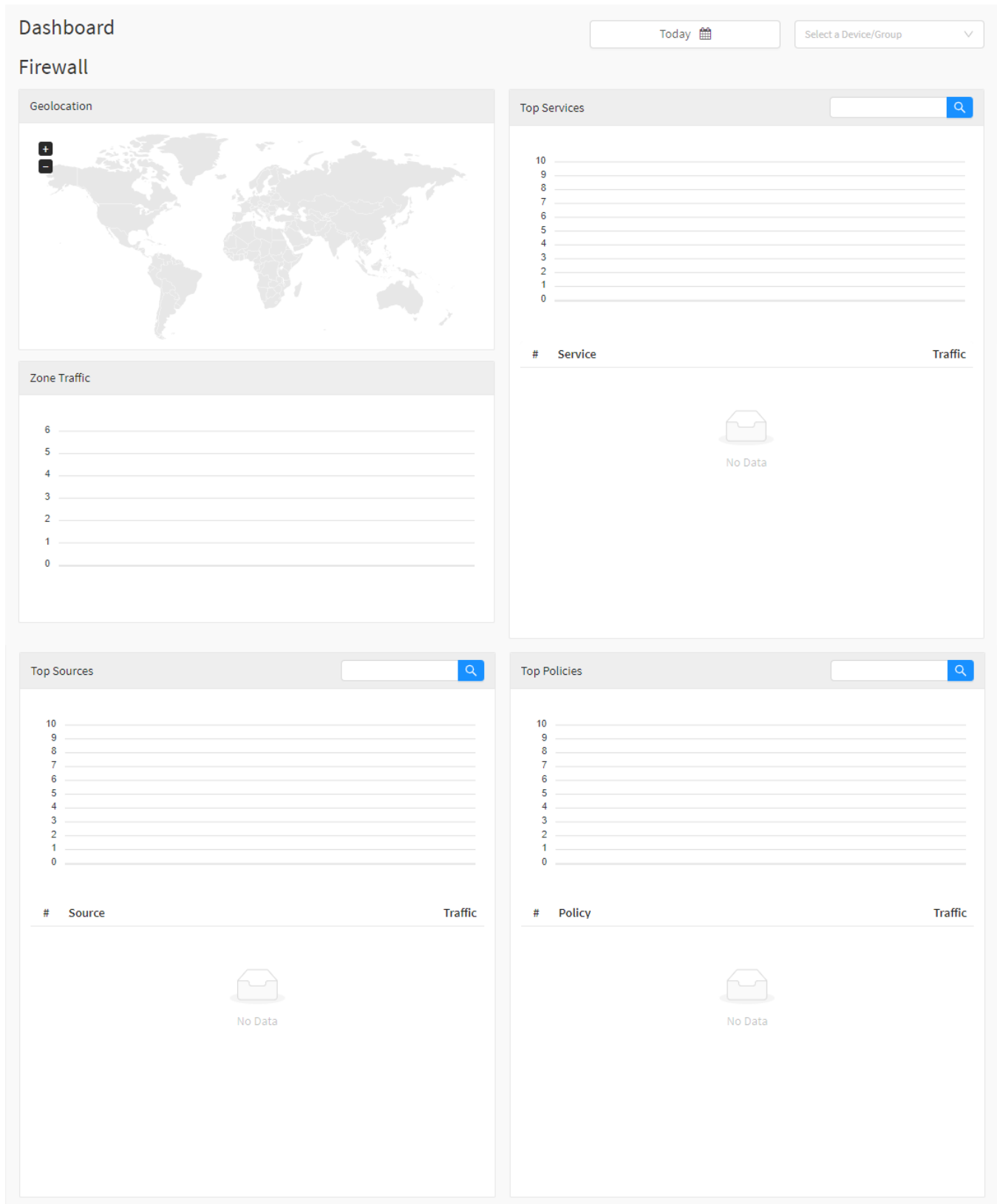
#### Dashboard - Device group selection

Next, we will see more sections displayed on Dashboard.

## Firewall

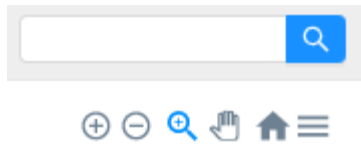
On the Firewall section are displayed the data of the following logs:

- Geolocation
- Top 10 Services
- Top 10 Zone Traffic
- Top 10 Origins
- Top 10 Policies

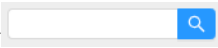



Firewall - Dashboard


When selecting the Device, or Device group, the following tools will be available for exploring the displayed information:





Dashboard - Exploring tools


Search bar [  ] : Allows the filtering of specific items, looked up by keywords.

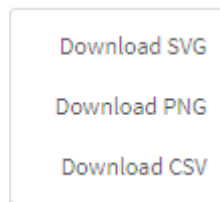
Zoom In/Out [  ] : Zoom increase/decrease buttons respectively.

Zoom [  ] : Allows the zoom selection mode.

Drag [  ] : Select to move the visualizer and access the displayed data.

Home [  ] : Returns the zoom to point zero and resets the position of the visualizer.

Download [  ] : Allows the download of the report in SVG, PNG and CSV formats.



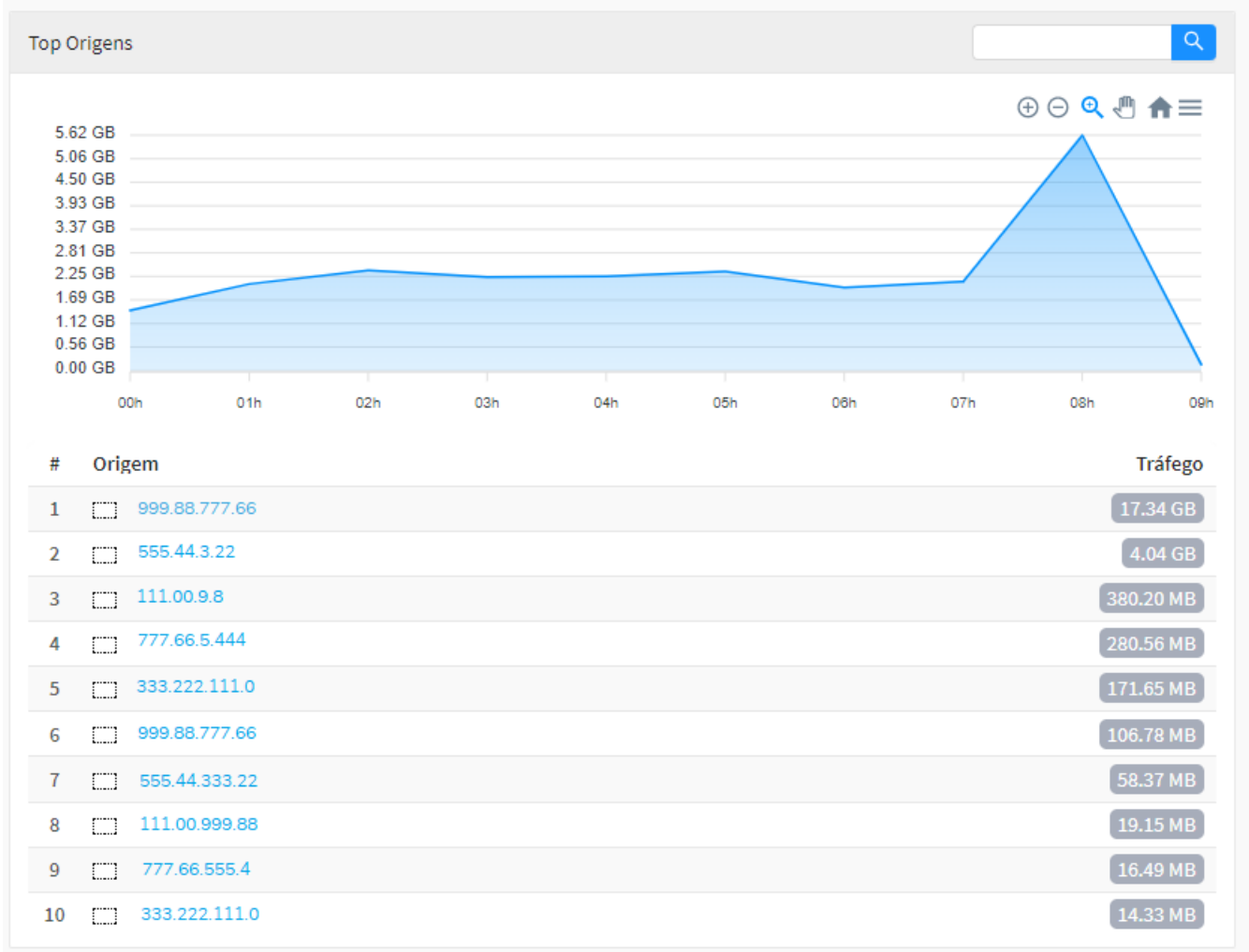
Download options

## Geolocation

Verifies all the IPs and displays the Geolocation's drawing, summing up the Devices' IPs (or all of them) in real time. Just browse the pointer over the regions in blue to check the data:

## Top 10 Origins (Firewall)

The service validates all the logs, and sums them up by IP, displaying then the top 10, from the same device or not. When clicking on the information, the user is redirected to the logs screen, that contains more details. The total traffic used by the IP is also informed:

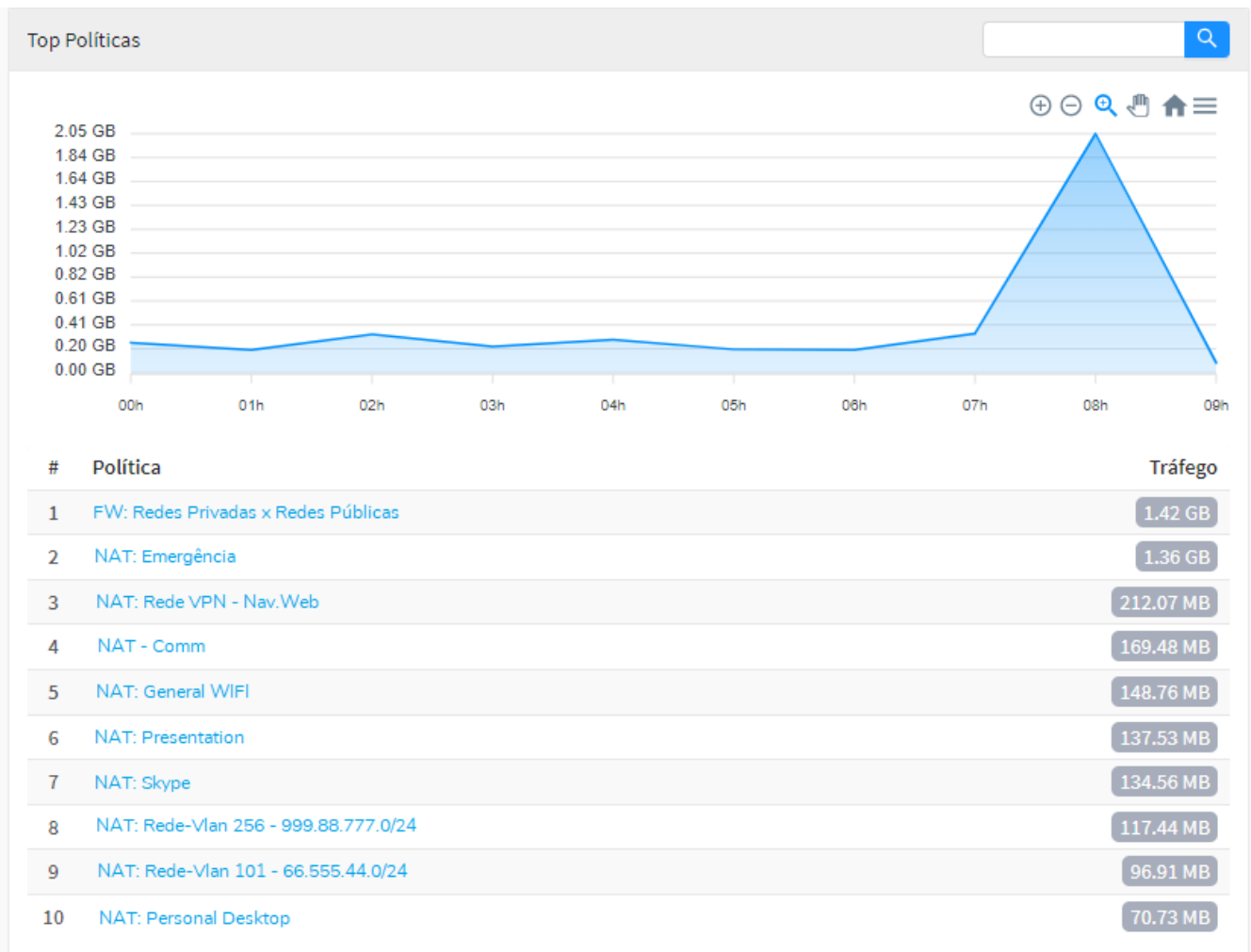


### Top 10 Services (Firewall)

The service validates all the logs, sums them up by service, and displays the Top 10, from the same device or not. It is also possible to access the detailed logs screen, by clicking on the information. The total used traffic is also displayed:

### Top 10 Policies (Firewall)

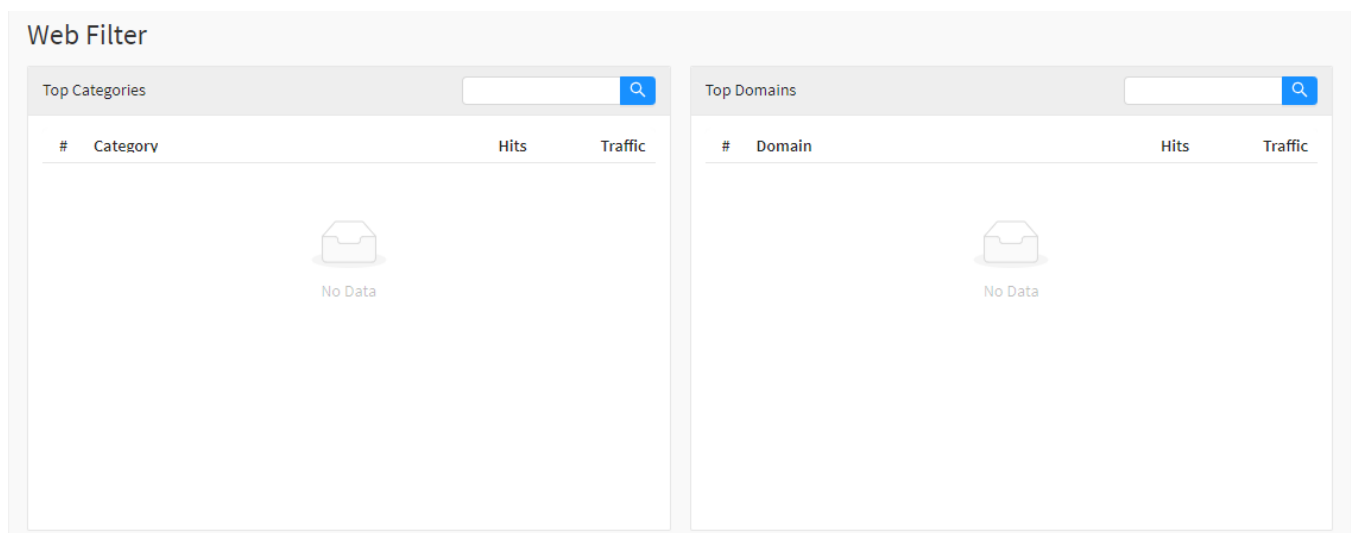
The service validates all the logs, sums those used in the Device's policies, and displays the top 10. The service allows the user to be redirected to the detailed logs screen (just click on the data) and also displays the total traffic used by the policy, as shown on the image below:



## Web Filter

On Web Filter, are displayed the data of the following logs:

- Top 10 Domains
- Top 10 Categories



Web Filter - Dashboard

Top 10 Domains (Web Filter)

The service validates all the logs, summing them up by the domain type, and displays the top 10, if they are from the same device or not. The service allows the user to be redirected to the detailed logs screen, by simply clicking on the information. It also displays the the amount of domain hits displayed on the top 10, as well as the total traffic used by the domain:

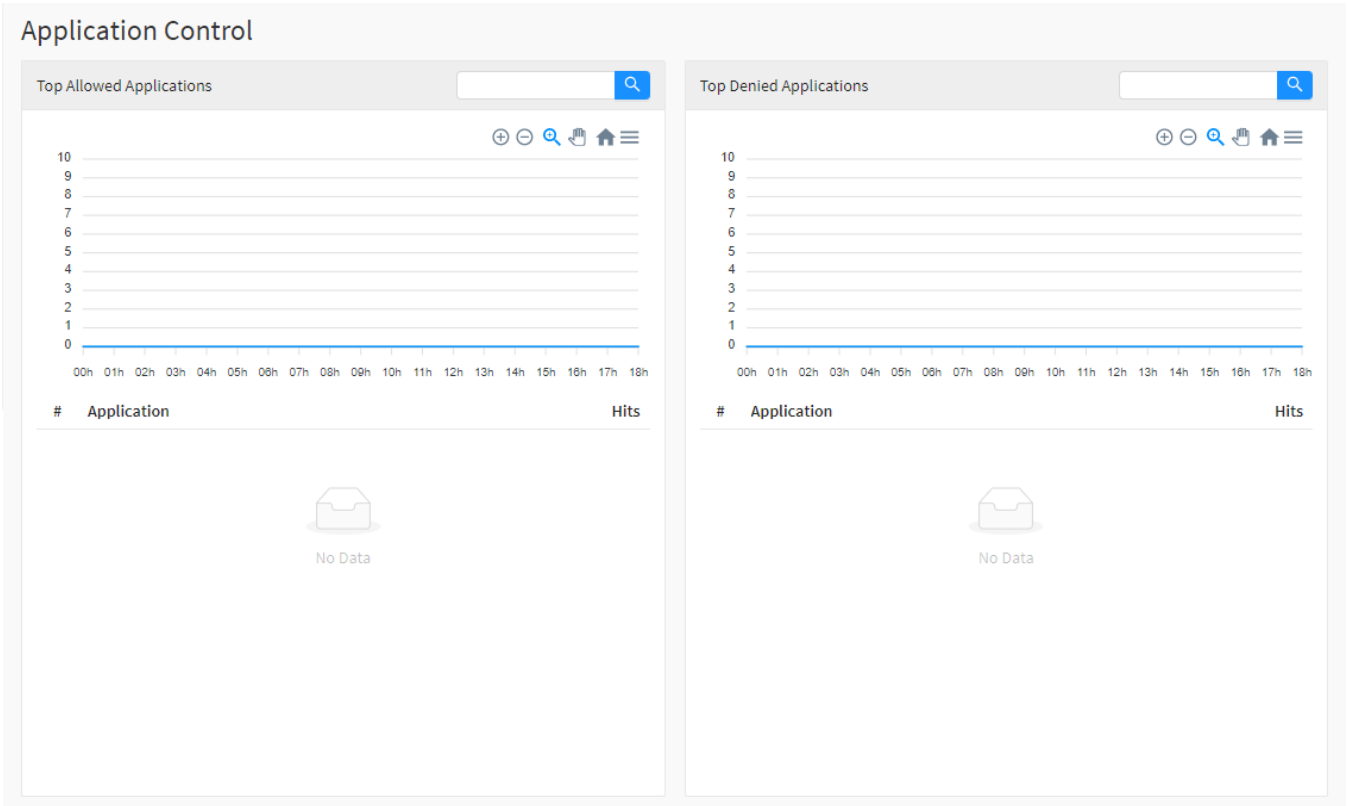
Top 10 Categories (Web Filter)

The service validates all the logs, sums up the categories' logs and displays the Top 10, if they are from the same device or not. The service allows the user to be redirected to the detailed logs screen, by clicking the information. Displays the amount of hits of the displayed categories on the top 10 and the total traffic used by the category:

Application Control

On Application Control is displayed data from the following logs:

- Top 10 Allowed applications
- Top 10 Denied applications



Dashboard - Application Control

Top 10 Allowed Applications (Application Control)

The service validates all the logs, sums up the applications' logs and displays the Top 10, if they are from the same device or not. The service allows the user to be redirected to the detailed logs screen, by clicking on the information. It also displays the amount of hits per application on the Top 10:

Top 10 Denied Applications (Application Control)

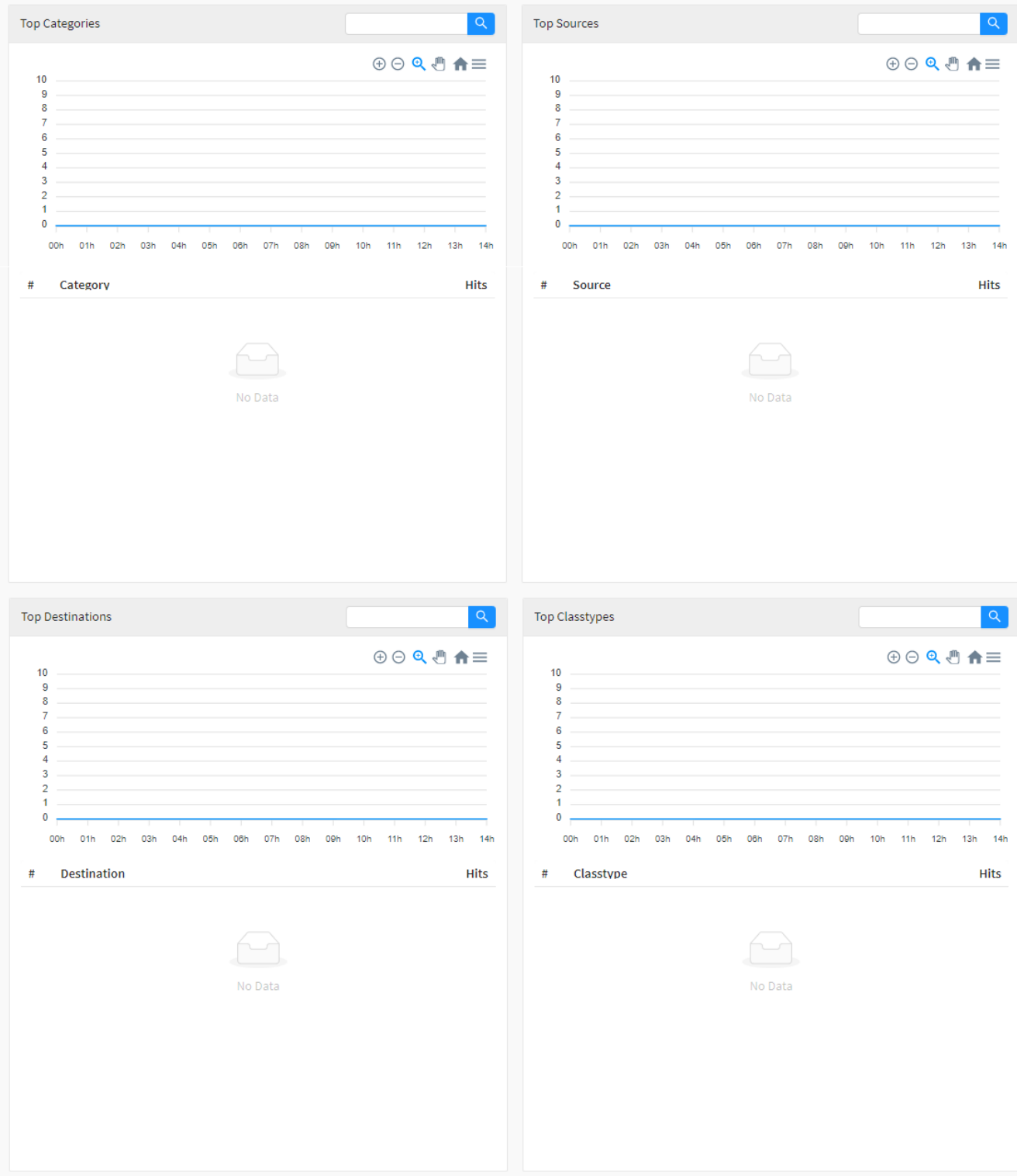
The service validates all the logs and sums the applications logs to display the Top 10. The service allows the user to be redirected to the detailed logs screen, same way as the previous ones. Displays the amount of hits per application on the Top 10:

## Intrusion Prevention

On Intrusion Prevention is displayed information from the following logs:

- Top 10 Categories
- Top 10 Origins
- Top 10 Destinations
- Top 10 Classtypes

## Intrusion Prevention



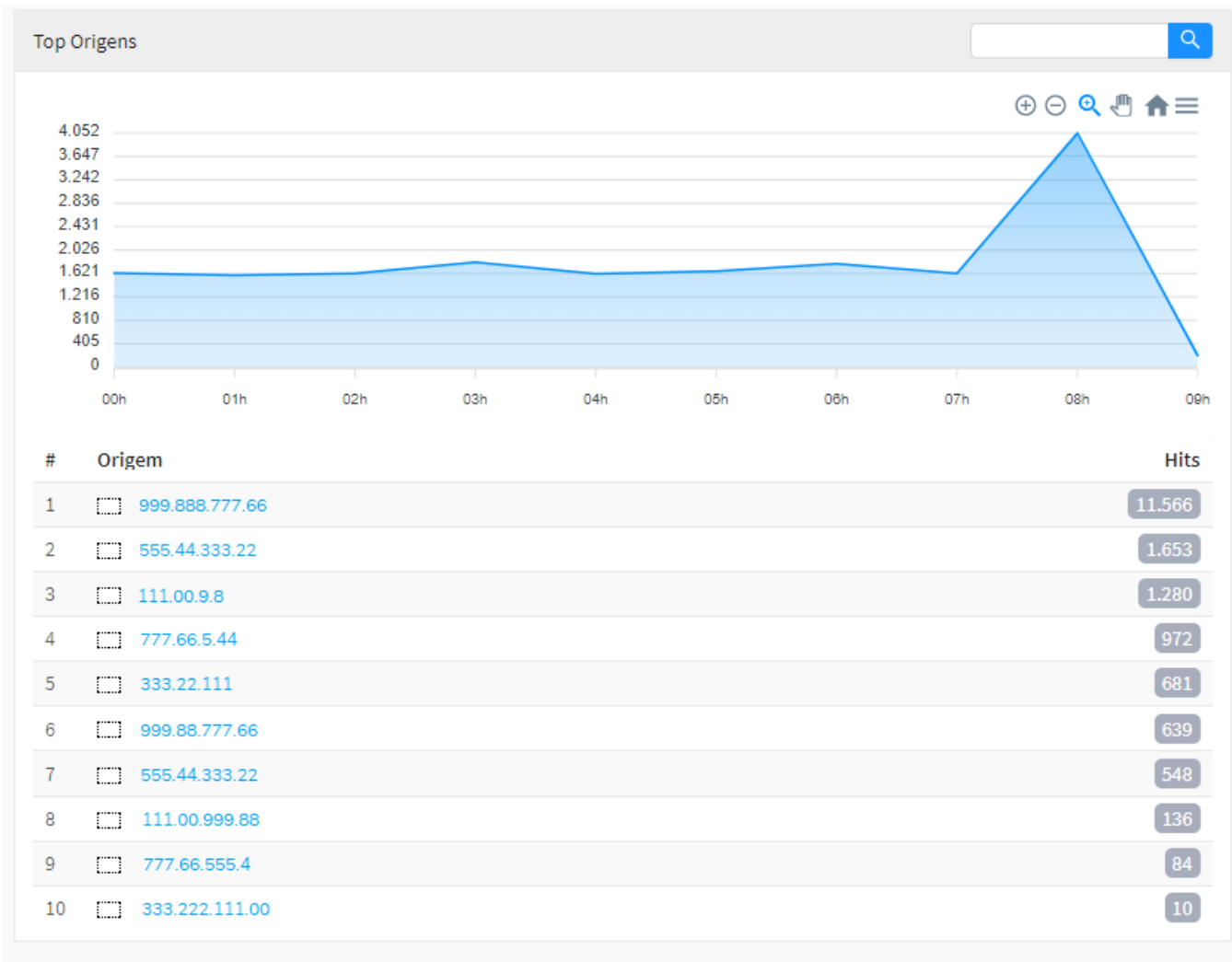
### Top 10 Categories (Intrusion Prevention)

The service validates all the logs, sums up the categories and displays the Top 10 from the same device or not. The service allows the user to be redirected to the detailed logs screen, by clicking on the information. It also displays the amount of hits from the category on the Top 10:



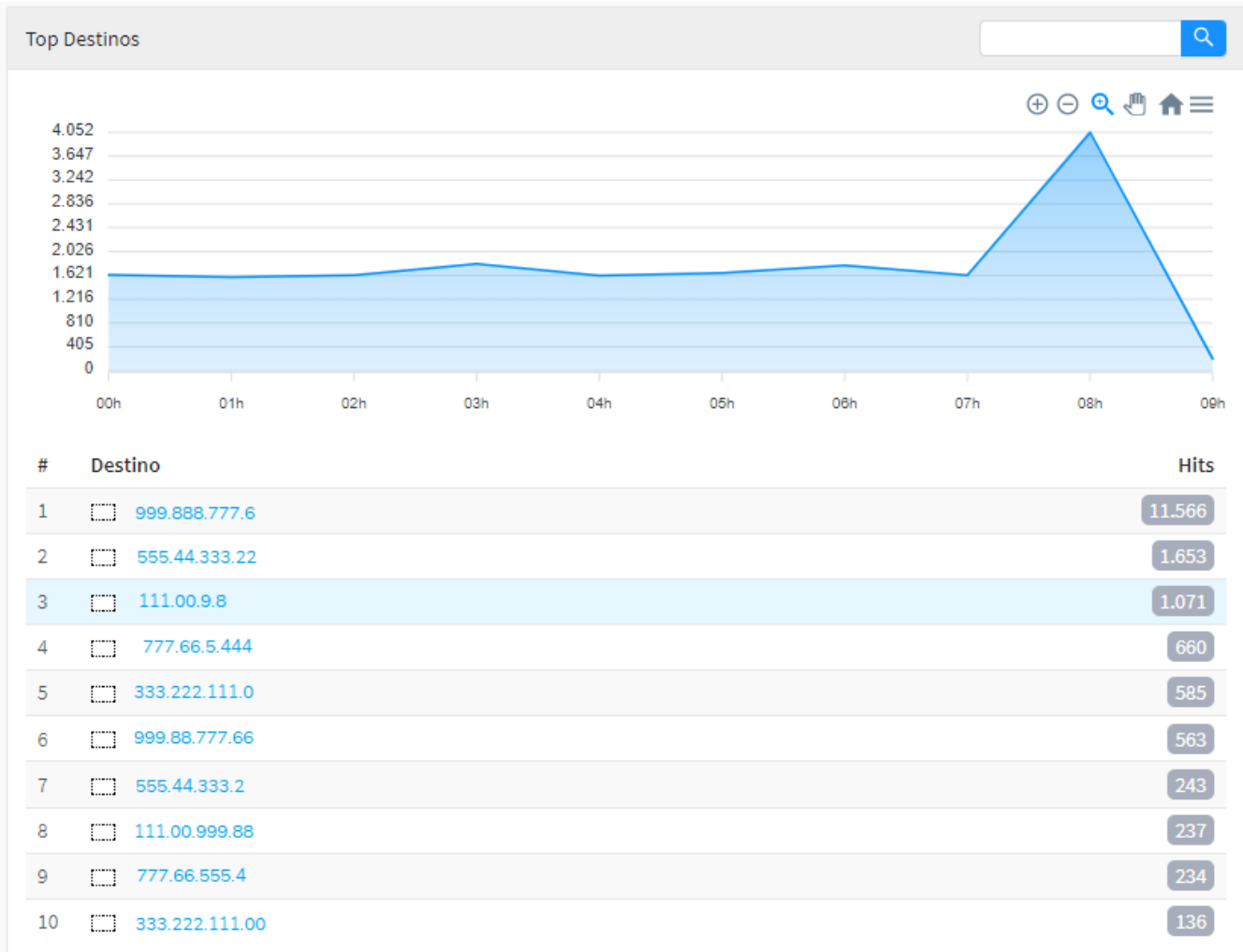
Top 10 Origins (Intrusion Prevention)

The service validates all the logs, and sums up the Origin logs, and displays the Top 10, from the same device or not. The service also allows the user to be redirected to the detailed logs screen, as well as displays the amount of hits from the Origin IPs on the Top 10:



Top 10 Destinations (Intrusion Prevention)

The service validates all the logs, sums up the Destination IPs logs, and displays the Top 10. The service allows the user to be redirected to the detailed logs screen, and displays the amount of hits from the Destination IPs displayed on the Top 10:



#### Top 10 Classtypes (Intrusion Prevention)

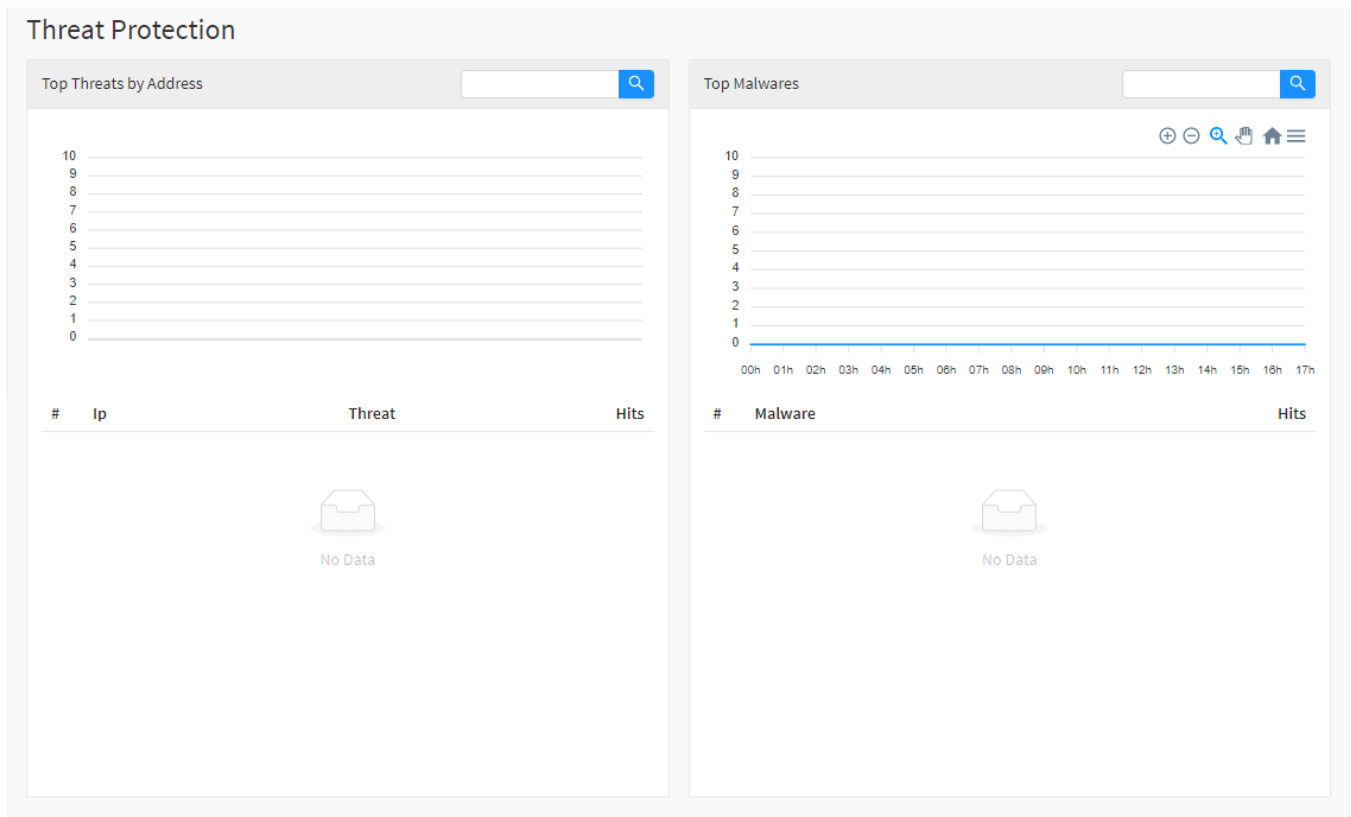
The service validates all of the logs and sums up the logs from the malware type, then displays the Top 10. The service allows the user to be redirected to the detailed logs screen and displays the amount of hits from the Top 10:



## Threat Protection

On Threat Protection, are presented the following logs' data:

- Top 10 Threats by Address
- Top 10 Malwares



#### Top 10 Threats by Address (Threat Protection)

The service validates all the logs, sums the threats up and displays the Top 10, if from the same device or not. The service allows the user to click on the threat and be redirected to the detailed logs screen. Displays the amount of hits from the threats displayed on the Top 10.


#### Top 10 Malwares (Threat Protection)

The service validates all the logs, sums up all the malwares and displays the Top 10, if from the same device or not. The service allows the user to click on the malware, and be redirected to the detailed logs screen. Displays the amount of hits from the malwares on the Top 10.

# Loggers

The loggers have the function of capturing information from the Blockbit UTM administered by the system and using this data, create the reports in the Blockbit GSM.

In addition, this feature also centralizes the management of the automatic backup routines of this feature, it acts by storing the log events generated remotely for each of the Logger devices.  
The backup routines are managed and sent to the backup server by the Logger itself, and can be stored on SMB, NFS and SFTP servers.

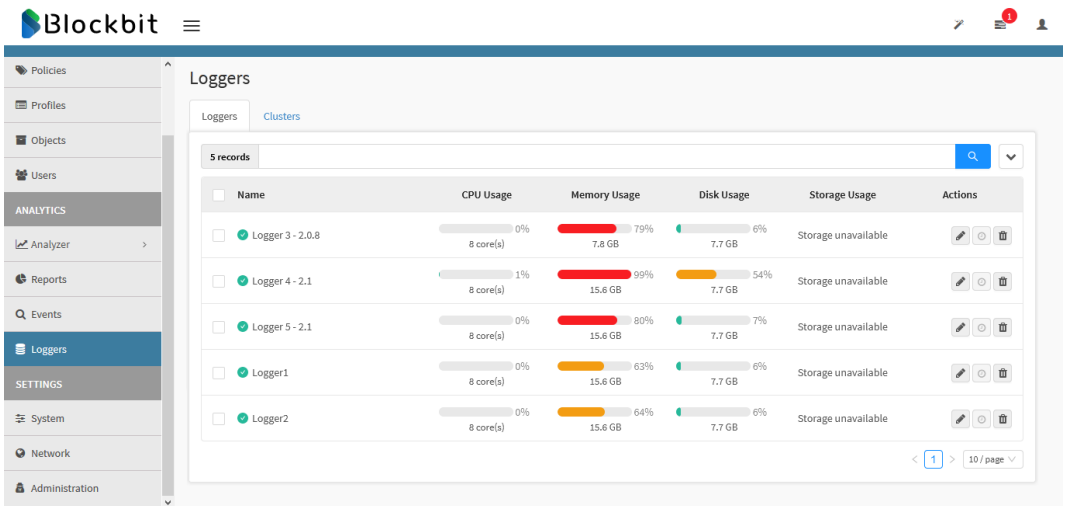
 For more information regarding backup of the Loggers, see this [page](#).

To manage the loggers, click on the icon located on the left side:



Analytics - Loggers

The following screen will appear:



Analytics - Loggers

This screen is made up of the tabs:

- [Loggers](#);
- [Clusters](#);

Initially we will analyze the step by step how to [install a Logger](#).

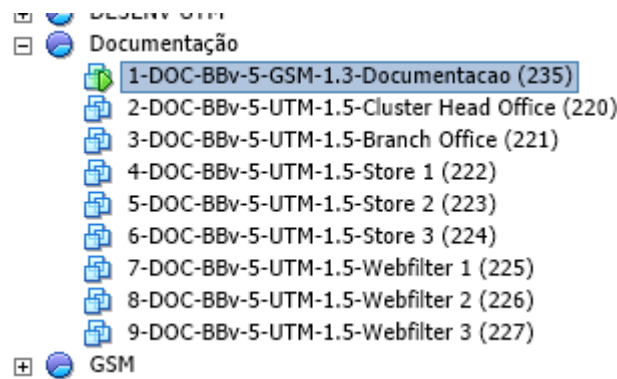
# Logger installation

This section will present the step by step to install a logger on Blockbit GSM.

We will demonstrate the installation using the VMware vSphere Client software as an example, procedures already performed in the step-by-step mentioned in the chapter regarding [GSM installation](#) will not be redone, if there is any doubt check the [appropriate section](#).

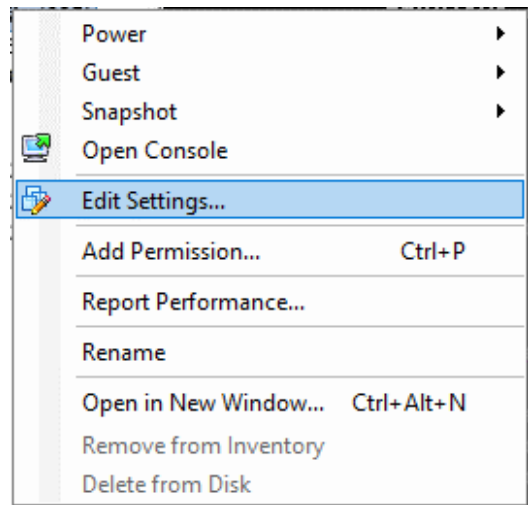
To install the logger on the Blockbit GSM, follow the guidelines below.

First, start VMware and browse your directory structure to the desired virtual machine, as shown below:



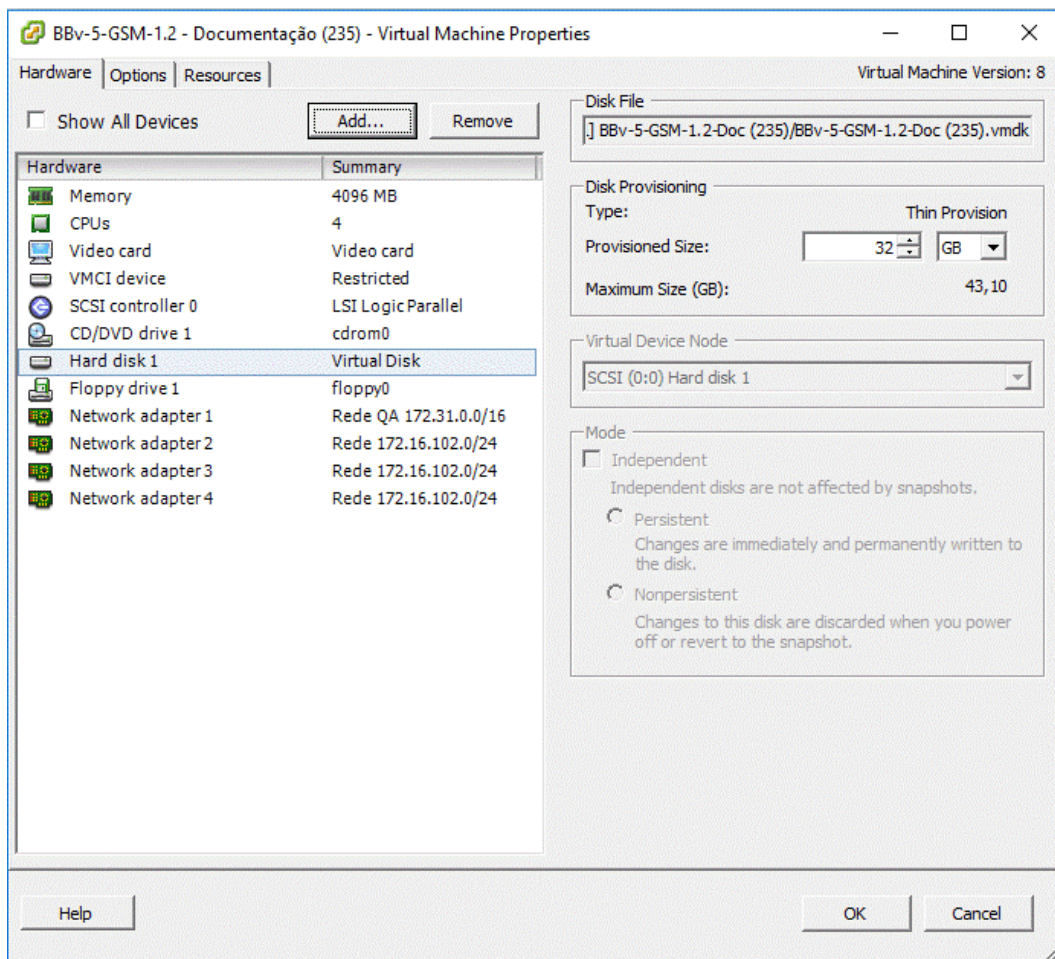
Logger Installation - Virtual Machine

In order to have disk storage space for installing the Logger, we will insert a hard disk into the virtual interface. Right click on the desired machine and select the option “Edit Settings ...” as illustrated by the image below:



Virtual Machine - Edit Settings

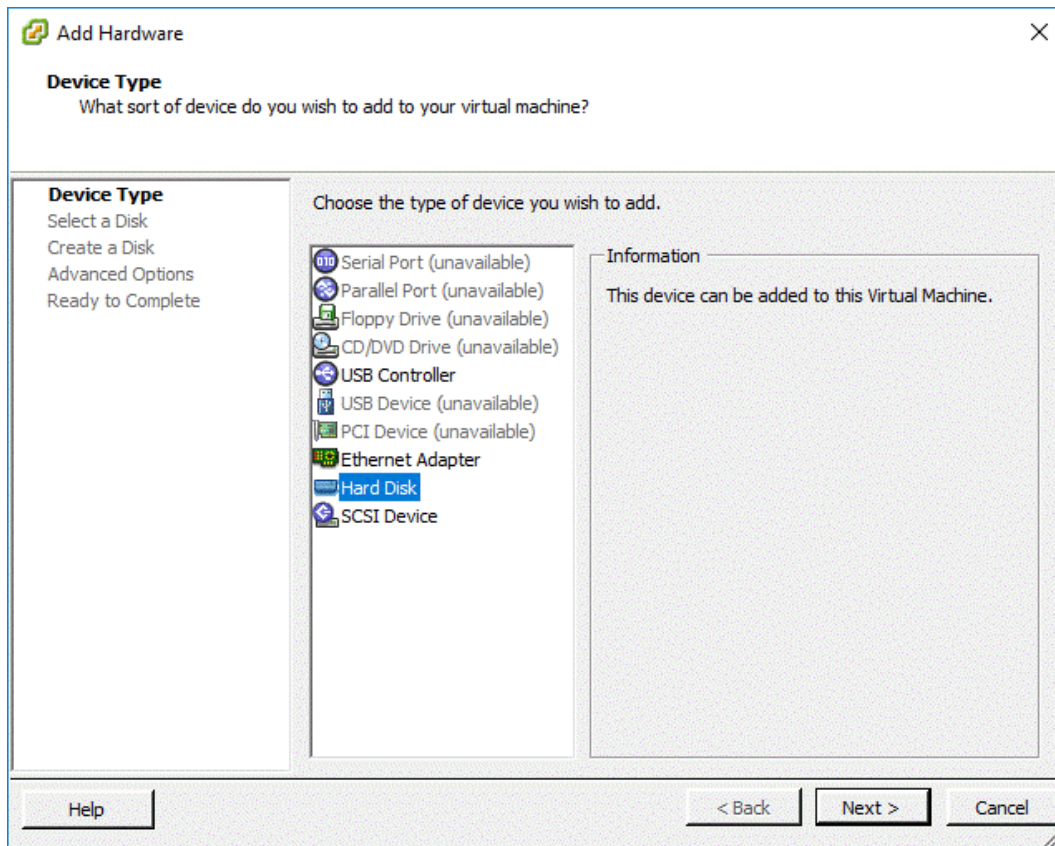
A screen displaying the hardware settings for your virtual machine will be displayed, as shown by the image below:



Virtual Machine - Add

Click on the "Add ..." button located at the top of the screen, on the right side of the "Show All Devices" checkbox.

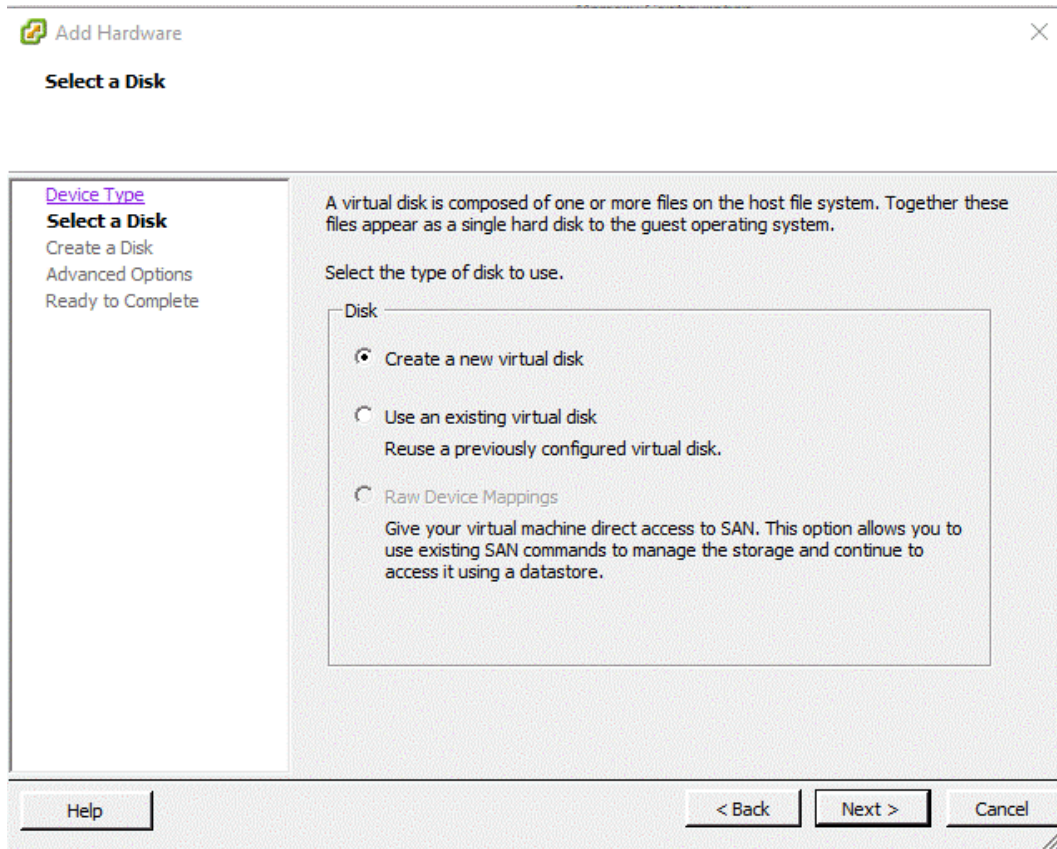
A screen requesting the type of device you want will appear:



Virtual Machine - Device Type

Select the "Hard Disk" option by clicking on the icon in the list in the middle of the screen, once this is done, click on the "Next" button to proceed to the next step. As shown by the image below, in the next window you will be asked what type of disc you want to create:





Virtual Machine - Select Disk

Select "Create a new virtual disk" if this option is not previously selected. Click on the "Next" button.

**Add Hardware**

**Create a Disk**  
Specify the virtual disk size and provisioning policy

[Device Type](#)  
[Select a Disk](#)  
**Create a Disk**  
[Advanced Options](#)  
[Ready to Complete](#)

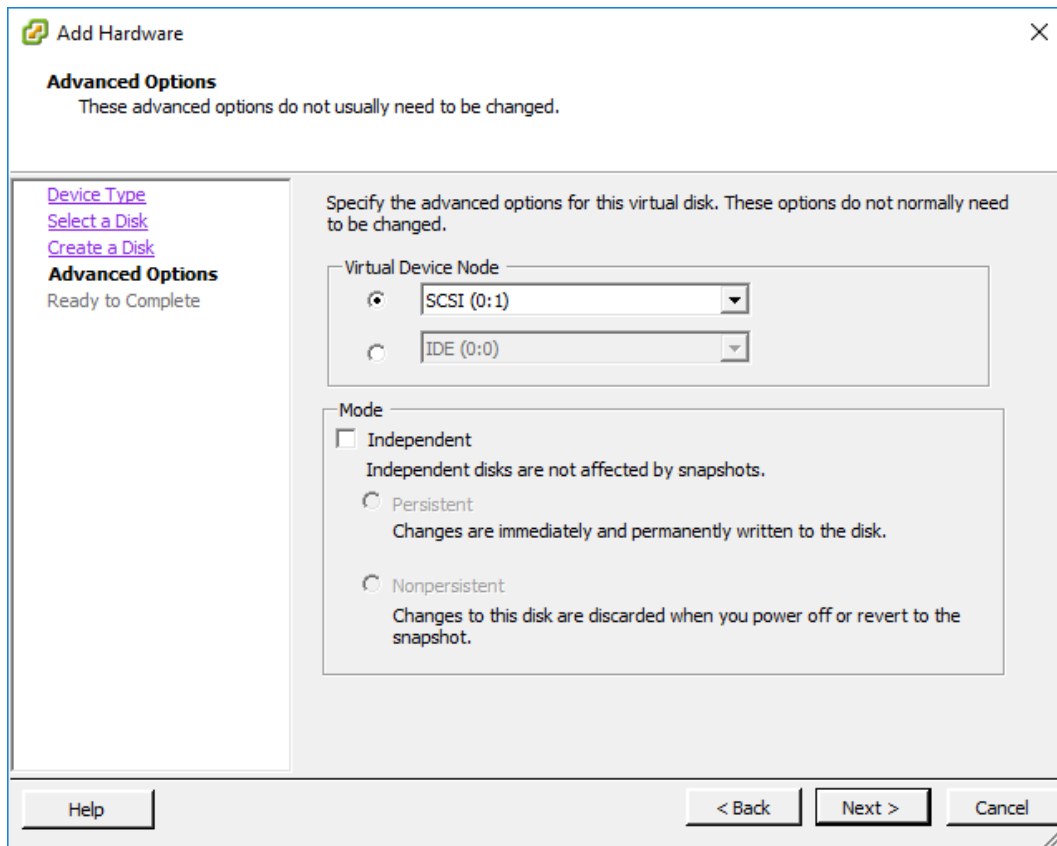
**Capacity**  
Disk Size:

**Disk Provisioning**  
☐ Thick Provision Lazy Zeroed  
☐ Thick Provision Eager Zeroed  
☒ Thin Provision

**Location**  
☒ Store with the virtual machine  
☐ Specify a datastore or datastore cluster:

Virtual Machine - Create a Disk

In this new window, determine the desired disk size in "Disk Size" and select the "Thin Provision" option in "Disk Provision". Once this is done, click on "Next", ignore the options that will appear in the next window ("Advanced Options") and click on "Next".



Virtual Machine - Advanced Options

Finally, the finalization screen will appear:

**Add Hardware**

**Ready to Complete**  
Review the selected options and click Finish to add the hardware.

[Device Type](#)  
[Select a Disk](#)  
[Create a Disk](#)  
[Advanced Options](#)  
**Ready to Complete**

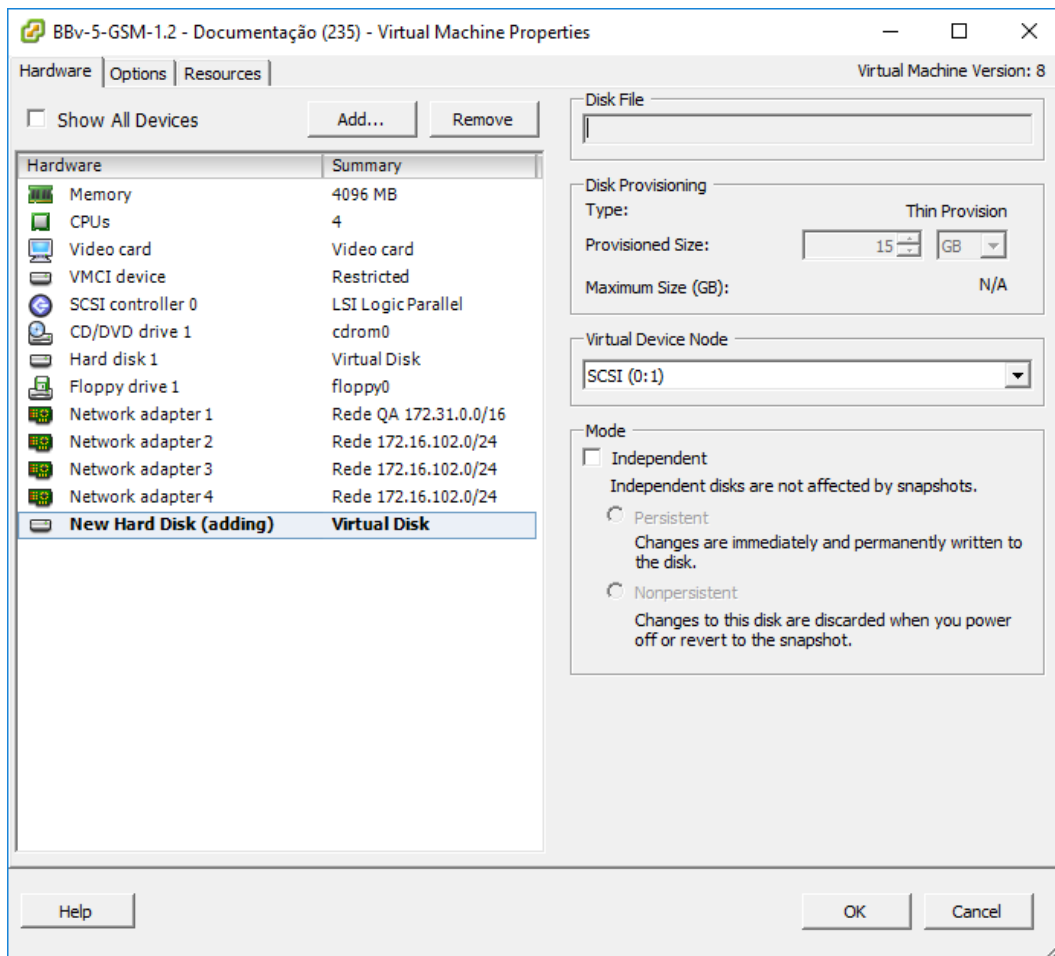
**Options:**

Hardware type:	Hard Disk
Create disk:	New virtual disk
Disk capacity:	15 GB
Disk provisioning:	Thin Provision
Datastore:	datastore1
Virtual Device Node:	SCSI (0:1)
Disk mode:	Persistent

[Help](#) [< Back](#) [Finish](#) [Cancel](#)

Virtual Machine - Ready to Complete

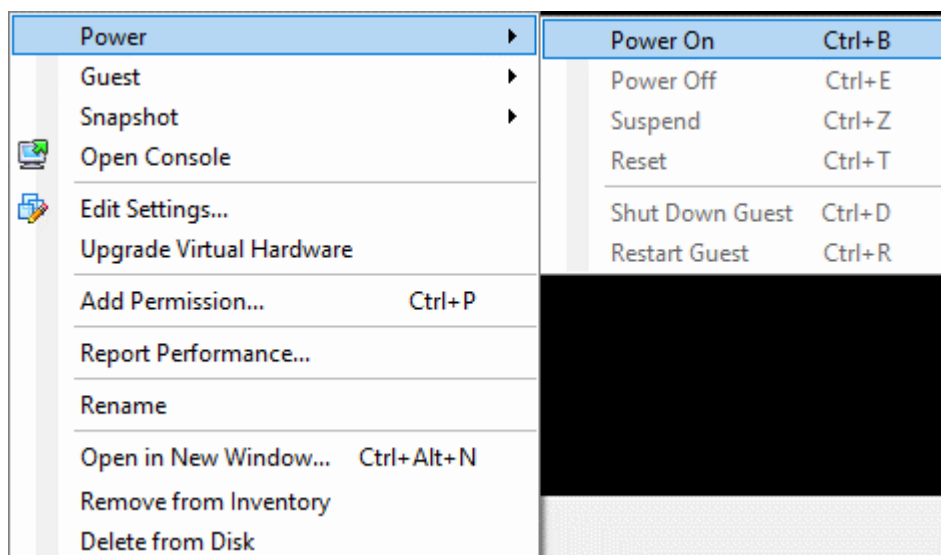
If all the configurations are in accordance with the desired one, click on "Finish", otherwise click on "Cancel" to cancel the process.



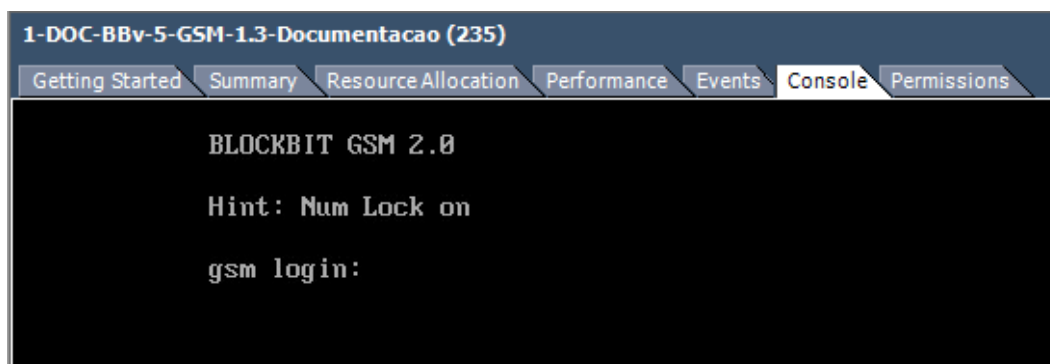
Virtual Machine - Adding virtual Disk

The machine will begin the process of adding the disk, click "OK" to exit this screen.

If the virtual machine is not connected, right click on it and select the option "Power" and "Power On", the selection of which can be seen in the image below:



After this step, when the machine is finished turning on, click on the "Console" tab (which can be seen in the image below) or access the machine's IP via SSH.



Virtual Machine - Console tab

After logging in, enter the CLI command "[logger-config](#)" to start the logger installation wizard. There are two operating modes for the logger, Standalone and Integrated.



Note that if the user chooses that a key is not generated when the prompt displays "Generate Key?", He can use the command "[logger-key -c](#)" or perform "[logger-config](#)" again.

## Standalone

In this mode of operation, the server is exclusive for remote logger, its use for any other function is not possible, thus making it necessary to use Blockbit's firmware. This example will detail the installation of an integrated logger.



It is recommended to execute this command directly on the machine's console, because during its configuration the SSH connection is dropped.



Note that the upgrade process interferes with the interfaces configured in standalone loggers. For more information about the [upgrade-blockbit](#) command, see this [page](#).

Here is a quick example of your installation:

```

admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.200.80
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
Hostname (ex: logger): gsmlogger
DNS (ex: 1.1.1.2): 172.31.0.100
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sda: 128.8 GB  SYSTEM
Disk /dev/sdb: 16.1 GB  EXT4
Disk (ex: /dev/sdb): /dev/sdb
mkfs2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
983040 inodes, 3932160 blocks
196608 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5f1fd31d110bfa221ae5e812311b838210546609b76aa5600820d1652f3dd95becb35ef5df77ece5952
7c3979b16741098b2329bda5b39e0057aca51725c4c74a7ec30e34142fca78300b428fe551a89f465d73ef628dff2f910b
3ea33e4f09f3146feb57a9fb23d2ac0e2e274acff2d6d70ba6cf e641f4e3e5499c9290ca6cf41c2b8b8eb7cc0ebd7dcfe9f
2fdefca61d98a28882b8c915d9f7e16745f4968c28ce6e030114163042744d0c1dd9000310c9f6c2ed7378f25c7592444e
84bc3a0301d6ee2a8a27cf732a938311da3cd05ebf54675fd2f5719fdbc8ec14e33d3d5e265b56806f8860d6c30e398fbc7
9b4b0c3caf d17ae7fef536014aff35554d9cfe81149b819b0659730b29740b6a8d38f2daf9d85716ba1fc1f1b468732ac6f
9b23f113ac1925a38fa79e8f39f98dd8f9357774842c0bf f5a93f69c0346240b03f7cc930604634fc8a1c51af8de1248fd
7ad25b8a828e0480bee015860d75b5b4829f05f984dff115d0c8d3d66451e327ab00f67dc8f3b29475e55d25657026ac2e
f3ca8275b3eb42d2744f0c15c14bd09ff1e54078c6b3cb0bf f3b8a9ce904e2b81b861da2f62b0b35b8f869505e2c9b127c
56aed9c9999ad3f180f9834c9eca59a3517708d6e2ed39515aeb87f46c635d45a3e73fcffe36ad00568d8c5f1964ce1e36f
5a2ba9f59f3b319a00a35c13f031df14cd98e0322d93adc4cae29a1ed4b362da5fe0f171d724d68449c59a99bf6d00b0f8f
22e8e3709f5ae1562948b12e3f5be5c716b0d9cd4f51b331143819c6d6e345bc10cc1bf2a9d95f40b75a1fc8eccebf94e1f
0983396d70a88596d6276234289b46bc427af1f158e25ceb39807ed37a9238d939031f2cfc4fc8a9d3a448b612ccabf54f
b8398b70e0e3c71c961c27572832024ff32e32960a3e929dcf18980f0f10ab35d8fcf399057b

Completed

Now configure the logger in administrative interface

```

*Logger – logger-config - Standalone*



For more information on how to set up a standalone Logger, see this [page](#).

After this step, just perform the same procedures when [installing the GSM](#).

## Integrated

In this operation mode it is possible to use the local GSM where the manager is installed as a logger server. However, it is necessary to dedicate an entire disk just for this function, regardless of whether it will be virtual or physical.

As an example, this guide will perform the installation of an integrated logger, as can be seen in the image below:

```
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated
```

#### Logger – logger-config

After selecting the “integrated” option, the system will recognize all the disks installed on the machine (physical or virtual) and will request that one of them be selected for the installation of the logger, however, it is important to note that the entire disk will be used for this, as well any data that is stored on it will be removed during installation. This fact can be seen in the image below:

```
Disk /dev/sda: 34.4 GB  SYSTEM
Disk /dev/sdb: 16.1 GB  AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
```

#### Logger – Entire device, not just one partition.

To continue, it is necessary to confirm by typing “y” and pressing “enter”. Once this procedure is done, the wizard will start creating the logger, as shown in the image below:

```
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
983040 inodes, 3932160 blocks
196608 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

#### Logger - Creating Logger

After these steps, the system will ask if you want the secret key to be generated, it is recommended to confirm with “y”, copy this information and keep it in a safe place. The only way to recover this key is using the command “logger-key” on the CLI (for more information, access this [link](#)), the image below demonstrates the process of creating a secret key:

```
Generate key? [y/N]: y
Key:
53616c7465645f5f87f0a3eef40c61f07896ce4f6f9e00ce2547017356e39f8db0c10aead6f64100110dc-b9ddf5d49d90584f02252db75d28da5f751b273d00c3a196a353
2c55f8a41bbf46e8c6330aafccbb4c73cfecf26acabf5d67f85b27a888c9d33da3c8d854f7b45f249c84f54dea4bbdef3c1fe2bac75818c91a9dcdb4d5bfa9c158e97eac
d5cb485accdaaacadc6dddf3374bab0e5e5ad65ce8c8768700c7c75d0a23ddcea0b7f1f844f63234629ddd447b4e2eb4db79007a5e2bca15b76c228efc7d2daa04bba78d1
5c58dfb7e4af612a64bb523c962b7638d55d2afc3c24126b6e14df62e9e325d9bb9e0c222ed4d91be2f02738324475cc19caff4ed24325868d41366ff1ca5b57f275bebb
0827fa116428f9ab1ac4dd77a60a5397f5fea906c4702cddb93a8c661b4f7ea6473fafb66dcf04ea4f1159f097234b62feada09efe2375ea3841f81aca37a7b4a04e77ec
b4956b555b513566d8f1b1f198e772dde47da4f318706fcf7122f0e80651e32761f06eb3c853e9d93beaeb7b5cc0cbfb57c44b6cca5b38e4b79a26f9de9379ef4ead81401
5b8ad768a826118980e0d9f6503fb7d2b6c9d9a1d3a49dc9a57ed33115aab596e3d75836ba2c9b3a3e7a2242225d792e0df91c0ea367d5048c7063d905abf0d6bedccf23
f4cca62c90ab90574b3d98b7980ec2801d4655c37b6738771dc000200c64e9eb0c8c404039a9e7a72b60c90962f694983f2f8206228c05654128ae7f961e718f35163daf5
bf45ed074f92ca3e25a12c29f94da9a8ac83b2a80aa9276c836835915fe78617a4be0cd04f1bda1c0f7cb9bd2791edef465967283865cc73f0bfd3d7b8c65af31c3a8a3d6
fc762dac09bc767736946f334e94ec758d126f476e713b3e4f368f234be3357ef1b190d3f8fbed50f15764b5c703012ad7aaeebbcb2bb23db0f5d1ab3ac0cd896029b951
ee7d5b
```

#### Logger – Secret Key.

After this step, as can be seen thanks to the wizard's own message, the Logger is already installed on the GSM.



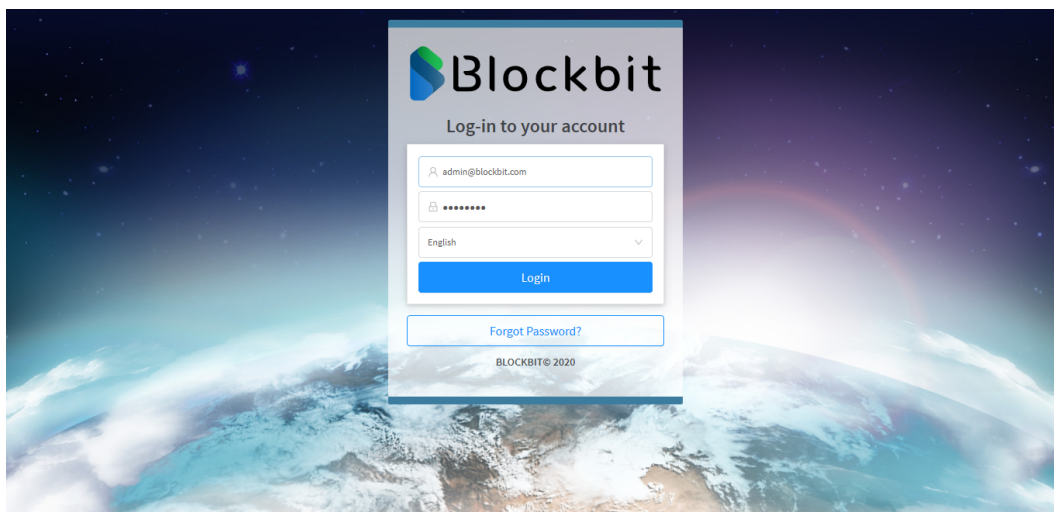
```
Completed  
Now configure the logger in administrative interface  
admin >
```

*Logger – Completed*

The step using the CLI has been successfully completed. The next step will be in the GSM administrative interface:

## Installation on GSM

Log in through the browser.



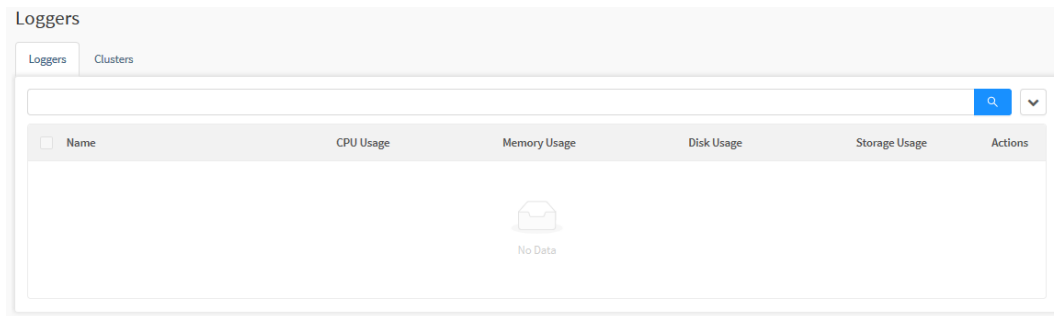
*GSM – Login.*

Click on the "Loggers" button in the vertical menu on the left.



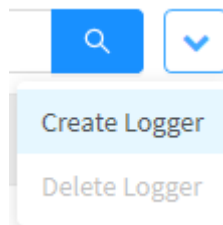
*Loggers*

The following screen will be displayed:



Loggers – Loggers

Add a logger by selecting the **actions menu** [  ] and clicking on the "Create Logger" option:



Loggers - Actions Menu - Create Logger

The following form will be displayed:

Create Logger Device

Settings

Storage

General

\* Name

\* Mode

Integrated

\* Description

\* Interface

\* Address

\* Secret Key

Devices & Devices Group

Select a type

Cancel

Save

Loggers – Create Logger Device

Complete the fields as per the standard (for more information visit this [link](#)):

### Loggers - Create Logger Device - Filled fields

After this step, click the  button.

Loggers - Create Logger Device - Logger created successfully

The next step is to connect the Logger to the devices. To do so, access the **Devices** option located on the left side menu.

## Devices







### GSM – Devices

In this example, the Logger will be applied to the UTM's of Store 1, 2 and 3. Click or search for the group name, in this case "Stores".

Devices


Inventory Communities Templates Provisioning

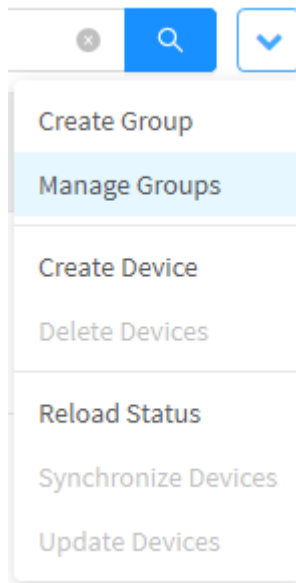
3 records group:"Stores"

<input type="checkbox"/>	Name	Group	Model	License Status	Version	Template	Policy IPv4	Policy IPv6	Actions
<input type="checkbox"/>	Store 1	Stores	BBv-5	B30D-8ED9-8C7D-543C	BLOCKBIT UTM 1.5.7 build 19072620				 
<input type="checkbox"/>	Store 2	Stores	BBv-5	715E-93F2-CCED-FBDF	BLOCKBIT UTM 1.5.7 build 19072620				 
<input type="checkbox"/>	Store 3	Stores	BBv-5	D92E-91C4-25B3-751A	BLOCKBIT UTM 1.5.7 build 19072620				 

< 1 > 10 / page

### GSM – Stores

In the **actions menu** [  ], select the option "Manage Groups".



Actions Menu - Manage Groups

The following screen will be displayed:

Manage Groups

4 records

<input type="checkbox"/>	Name	Description	Devices	Actions
<input type="checkbox"/>	Branch Office	Branch Office device group	1	<div></div> <div></div>
<input type="checkbox"/>	Head Office	Head Office device group	1	<div></div> <div></div>
<input type="checkbox"/>	Pool Web Filters	Webfilter device group	3	<div></div> <div></div>
<input type="checkbox"/>	Stores	Store device group	3	<div></div> <div></div>


<

1

>

Done

Manage groups

Select the desired group and click on the edit button  the following window will appear:

Edit Group

\*

Name

Stores

Description

Store device Group

Devices

Store 1 X

Store 2 X

Store 3 X

Logger

Cancel

Save

Manage Groups – Edit Group

Select the appropriate logger, as shown below:

Edit Group
X

\* Name

Stores

Description

Store device Group

Devices


Store 1 X Store 2 X Store 3 X


Logger

Logger

Cancel
Save

Manage Groups - Edit Group - Logger selected

Click the save [  ] button to finish editing.

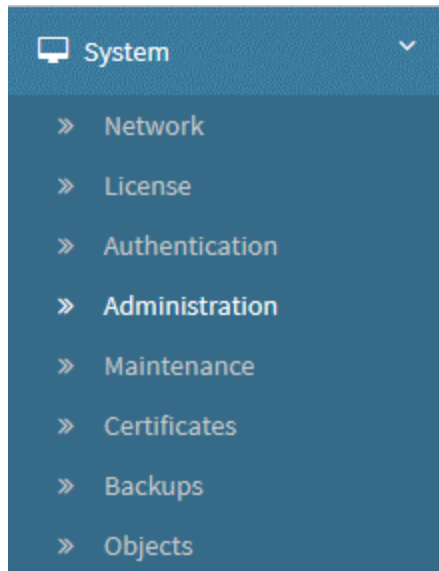

**Group updated with success!**  
 Group updated with success

With that, all devices in the group will use the selected logger.

After performing this process, click on the **Access Interface Web icon** [  ] to access the desired UTM.

If necessary, log in.



Go to "System" and click on the "Administration" option as exemplified by the image below:



UTM – System - Administration

Access the "Central Management" tab:

UTM – Central Management

Check the checkbox “Enable Analyzer”, in “Analyzer Address” type the GSM IP (or the Analyzer IP if it is Standalone), in “Logger Service”, type the logger service. That done, click on the save icon [  ] and access the task queue by clicking on the **saved settings queue icon** [  ] and apply the settings. If everything goes correctly, the “Status” (on the right side of “Analyzer Address”) will be changed to “Online”.

Returning to GSM, again access the “Loggers”. It is now possible to observe them acting normally, as shown below.



Loggers

1 records

<input type="checkbox"/>	Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
<input type="checkbox"/>	<div><div></div>Logger</div>	<div><div></div>0% 4 core(s)</div>	<div><div></div>79% 7.8 GB</div>	<div><div></div>6% 7.7 GB</div>	Storage unavailable	<div><div></div><div></div><div></div></div>

<

1

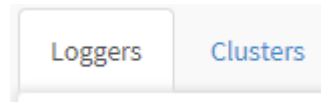
>

10 / page

# Loggers - Loggers

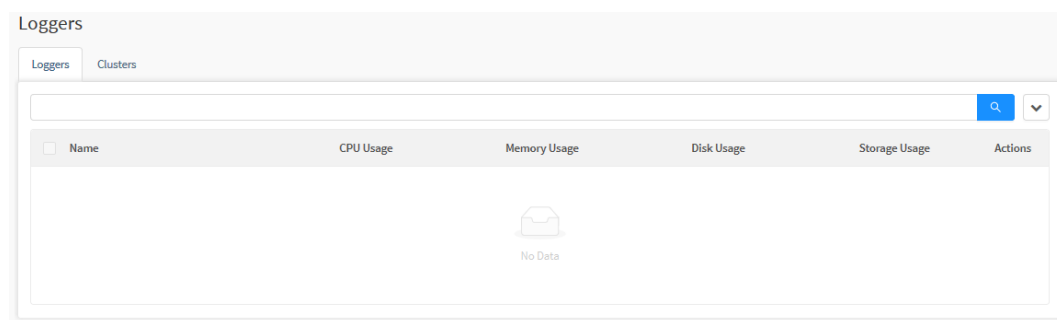
Nesta aba temos acesso aos recursos para criação de *loggers* e de rotinas automáticas de *backup*, possuindo também ferramentas para visualizar o desempenho e estado atual dos dispositivos de *log* e de possibilidade de visualizar o histórico dos *backups*.

Para acessar estas funções, selecione a aba "Loggers":



Aba Loggersb

The following screen will be displayed:



Loggers - Loggers

In this session we will analyze:

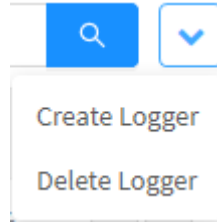
- How to [create](#), edit and [remove](#) a logger and backup routine;
- [Backup history details](#);
- [The components of the columns on this screen](#).

Below we will detail the options of the [actions menu](#).

# Loggers - Menu de ações



By clicking on the actions menu button [ ] at the top right it is possible to add the logger or remove it.



Loggers - Logger actions menu

The menu consists of the following options:

- [Create Logger](#);
- [Delete Logger](#).

Next, each action menu option will be detailed.

# Create Logger

To register a logger click on the option "Create Logger" in the upper right corner of the screen, the following window will be displayed:

The screenshot shows a 'Create Logger Device' window. It features a sidebar on the left with 'Settings' and 'Storage' tabs. The 'Settings' tab is active, showing a 'General' section with the following fields: a required text field for 'Name', a required dropdown for 'Mode' (currently set to 'Integrated'), a required text area for 'Description', a required text field for 'Interface', a required text field for 'Address', and a required text area for 'Secret Key'. Below these is a 'Devices & Devices Group' section with a dropdown menu labeled 'Select a type' and a list area with '+' and '-' buttons. At the bottom right of the window are 'Cancel' and 'Save' buttons.

Loggers – Create Logger Device



For more information on how to install a logger device, check this [page](#).

This window is divided into two tabs that can be accessed on the left side:

- [Settings](#);
- [Storage](#).


In addition, the [Archiving](#) tab has the panels:

- [Backups](#);
- [Log Rotation](#).

Next we will analyze the components of the Settings tab:

## Settings

This panel has the function of determining the settings of the Logger. To do so, configure the form according to the instructions below:

 Note that the upgrade process interferes with the interfaces configured in standalone loggers. For more information about the upgrade-blockbit command, see this [página](#).

Create Logger Device

Settings

Storage

General

\* Name

\* Mode

Integrated

\* Description

\* Interface

\* Address

\* Secret Key

Devices & Devices Group



Select a type

Cancel

Save

Create Logger Device - Settings

- **Name:** Determines the name of the Logger to be registered. Ex.: *Logger 1*;
- **Mode:** Defines how the Logger will operate. It can be:
  - Standalone;
  - Integrated.
- **Description:** The description of the logger is basically for organizational purposes;
- **Interface:** Defines the interface that will be used to access this logger;
- **Address:** Determines the IP address that will be used to access this logger. In addition, if the logger H.A. has been configured, the address defined in this field will be used in the heartbeat, for more information, see this [page](#). Ex.: 10.0.0.1;
- **Secret Key:** Determines the secret key issued by the UTM. It needs to be pasted in full for the Logger to work. In addition, if the logger H.A. has been configured, the key (ssh) defined in this field will be used in the heartbeat, for more information, see this [page](#);
- **Devices & Devices Group:** It is a checkbox that allows the location of the devices or groups of devices that the logger will use to create

reports. Click [  ] to add them or [  ] to remove them.

This completes the configuration of the logger.  
Next we will analyze how to configure Logger Backups:

# Storage

In this interface, the administrator has the necessary resources to manage the automatic backup routines for each Logger device that is created and to configure their retention.

Create Logger Device

Settings

Storage

Backups

☐ Enable

Remote Storage

Select a type

Number of backup retention

100

% Disk usage retention

70

Log Rotation

☐ Enable

% Log Retention by Disk Space

70

Log Retention by Period

Unlimited

Maintenance Interval

5

Minutes

Cancel

Save

Create Logger Device - Backups

This screen is divided into two panels:

- Backups;
- Log Rotation.

Next, we will analyze each of the components of this window:

## Backups

In this panel are the settings that allow you to create an automated backup routine for each Logger.

Backups

☐ Enable

Remote Storage

Select a type

Number of backup retention

100

% Disk usage retention

70

Archiving - Backups

- ☒ **Enable** [ ☒ ]: Enables the backup of Loggers;
- Remote Storage**: Defines the location where the backups will be stored, the items that appear in this list are created in the Storages tab in the System menu, for more information on this, see this [page](#). Ex.: Backup;
- Number of backup retention**: Determines how many backups will be stored, if this limit is exceeded, the oldest backups will be replaced;
- % Disk usage retention**: Defines how much disk should be used in storage to save the backup. Upon reaching the limit, the backup is not performed. Ex.: 15.

This finalizes the configuration of the logger backup panel.

Next we will analyze how to configure the Log Rotation panel.

## Log Rotation

In this panel are the settings that determine the retention of the logs stored by the Analyzer for each Logger.

Log Rotation

☐ Enable

% Log Retention by Disk Space

70

Log Retention by Period

Unlimited

Maintenance Interval

5

Minutes



Archiving - Log Rotation

- ☒ **Enable** [ ☒ ]: Enables retention of logs;
- % Log retention by disk space**: Determines the log retention limit by percentage of disk space. The default value is: 70%; The maximum is: 90%.

- **Log retention by period:** Defines the log retention period, the first field determines the number of days, months and years, while the second field defines the period itself, the available options are:
  - **Unlimited:** Disables the first field and defines that the retention of the logs will be unlimited.
  - **Days:** Defines that the logs will be retained on certain days;
  - **Months:** Defines that the logs will be retained in certain months;
  - **Years:** Defines that the logs will be retained annually.
- **Maintenance Interval:** Defines the maintenance time of the logs, the first field determines the number of minutes and hours, while the second field defines the period itself, the available options are:
  - **Minutes:** Disables the first field and defines that the retention of the logs will be unlimited;
  - **Horas:** Defines that the logs will be retained on certain days.

This completes the configuration of the Log Rotation panel.

A blue rectangular button with the word "Save" in white text.A light gray rectangular button with the word "Cancel" in blue text.

To finish creating the logger, click [  ]. If you want to cancel the process, click [  ].



Next, we'll look at how to [remove a logger](#).




# Delete Logger

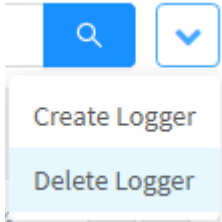
To delete the loggers, follow these steps:

- 1. Select the group you want to delete by clicking on the **selection** [  ];

<input checked="" type="checkbox"/>	Name	CPU Usage	Memory Usage	Disk Usage	Actions
<input checked="" type="checkbox"/>	Logger	<div><div></div><div>0 core(s)</div></div> 0%	<div><div></div><div>0 GB</div></div> 0%	<div><div></div><div>0 GB</div></div> 0%	 

Loggers - Selected Logger

- 2. Click the **actions menu** [  ] icon;
- 3. Click on the “Delete Logger” option;



Loggers – Menu Actions – Delete Logger

- 4. A confirmation message will appear, verifying if you want to delete the selected logger:

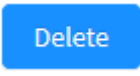
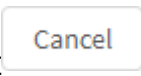
Are you sure?


Are you sure you want to delete the logger Logger?

Cancel

Delete

Inventory - Delete logger message

Click the [  ] button or click [  ] to return to the previous panel.

 **Loggers deleted successfully**  
*Loggers deleted successfully*

The logger was successfully removed.

Next we will analyze the components of the [columns](#).

# Loggers - Columns

The following explains each column in the Loggers panel:

Loggers




Loggers Clusters

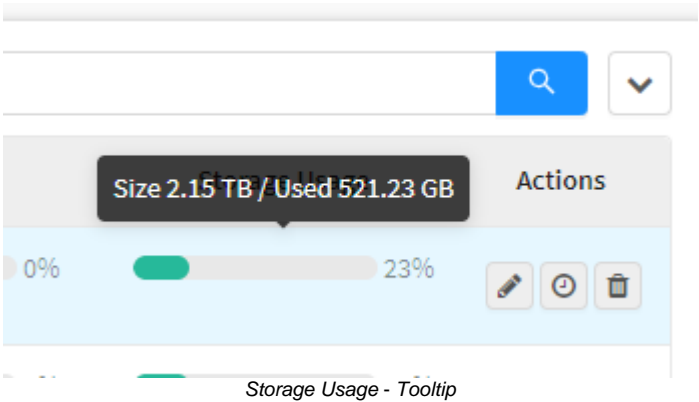
3 records

Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
<div><div></div><div>LOGGER</div></div>	<div><div></div><div>4 core(s)</div><div>0%</div></div>	<div><div></div><div>7.8 GB</div><div>76%</div></div>	<div><div></div><div>14.64 GB</div><div>5%</div></div>	<div><div></div><div>23%</div></div>	<div><div></div><div></div><div></div></div>
<div><div></div><div>LOGGER BLOCKBIT</div></div>	<div><div></div><div>0 core(s)</div><div>0%</div></div>	<div><div></div><div>0 GB</div><div>0%</div></div>	<div><div></div><div>0 GB</div><div>0%</div></div>	<div><div></div><div>Storage unavailable</div></div>	<div><div></div><div></div><div></div></div>
<div><div></div><div>LOGGER TEST</div></div>	<div><div></div><div>0 core(s)</div><div>0%</div></div>	<div><div></div><div>0 GB</div><div>0%</div></div>	<div><div></div><div>0 GB</div><div>0%</div></div>	<div><div></div><div>Storage unavailable</div></div>	<div><div></div><div></div><div></div></div>




< 1 > 10 / page

Loggers panel

- Select** [  ]: Allows you to select a logger;
- Status**: Displays the current state of the logger. If the icon is green [  ], the Logger is functioning normally, however, if the icon is red [  ], there is an error in the Logger.
- Name**: Displays the name of the registered logger;
- CPU Usage**: Represents CPU usage, percentage of consumption and total capacity. It is demonstrated in amount of colors and GigaBytes;
- Memory Usage**: Represents memory usage, percentage of consumption and total capacity. It is demonstrated in GigaBytes;
- Disk Usage**: Represents disk usage, its percentage of consumption and total capacity. Shown in GigaBytes;
- Storage Usage**: Represents the percentage of use of the total logger storage space. For more information, hover your mouse over this bar to display a tooltip, as shown in the image below:



Storage Usage - Tooltip

- Actions**: Provides the following essential actions:
  - Edit** [  ]: Allows you to edit the settings of the Logger added in the [Create Logger](#) option of the actions menu;
  - Backups History** [  ]: Displays a panel with the centralized history of Logger backups, including information on what is currently being done, for more information, see this [page](#);
  - Delete** [  ]: Allows you to remove the logger, it is equivalent to the [Delete Logger](#) option.































Next, we'll dive into the components of the [Backups History](#) window.

# Loggers - Backups History

Through the Backups History window, it is possible to have access to a list of all logger backups already carried out or currently in progress. Below, we will detail each component of this window:

Backups history LOGGER BACKUP ×








11 records 🔍



Name	Size	Last status	Status	Actions
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Running	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Running	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Running	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Waiting	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	25/10/2020 11:36	Waiting	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Error	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Success	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Success	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Success	  
4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap	1.00 GB	13/10/2020 11:36	Success	  

< 1 2 > 10 / page ⌵

Close

Loggers - Backups History

- **Name:** Displays the name of the backup snapshot;
- **Size:** Displays the size of the backup;
- **Last Status:** Displays the date for when the backup last changed in its state;
- **Status:** Displays the current status of the Backup routine execution, which can be:
  -  **Running**: The backup routine is currently running;
  -  **Error**: Something went wrong that caused the backup routine to fail;
  -  **Waiting**: The routine is in waiting time. This can occur when the system detects a process that might interfere with the backup that is currently running (for example, another backup routine);
  -  **Success**: The backup was successful.
- **Actions:** It consists of a set of buttons with useful actions, which are:
  -  **Stop**: If a backup routine is running, this button is used to interrupt its execution;
  -  **Restore**: By clicking on this button the system evaluates whether the disk space makes it possible to restore the backup, if possible the backup procedure is performed on the Device again. However, if you do not have enough space, the restoration will be rejected and the user will be informed in the graphical interface;
  -  **Delete**: When you click this button, the backup is removed.


To close this window, just click on the [] located at the top of the screen or on [].


For more information on the columns, visit this [page](#).


Next, we will detail the contents of the [Clusters](#) tab.

# Loggers - Clusters

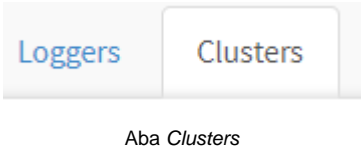
The "Clusters" tab allows the configuration of the High Availability service of the log storage servers, allowing the administrator to define redundant logger servers, which also have the functionality to automatically replicate the logs of the primary cluster in real time to the secondary. The importance of this feature is to guarantee the availability of the service and to perform a failover, if any discrepancy is detected in the network, the secondary server is activated, replacing the primary and ensuring that the Logger remains functional.

**ATTENTION:** To configure the H.A. the following requirements must be met:  
  
It is mandatory that the two servers have the same computational capacities (Memory, Processor, Storage, etc.), the same models and the same versions, regardless of whether it is a physical or virtual appliance.  
  
The H.A. functionality in the Manager settings can only be enabled when there is no integrated Local Logger.  
  
The primary server must be properly licensed.

If the logger is on standby, external storage is interrupted, backups only reoccur when the logger is active.

GSM supports a maximum of 125 configured clusters.

To configure this feature, click on the "Clusters" tab:



Aba Clusters













The following screen will appear, as shown by the image below:

Loggers

Loggers

Clusters


2 records

<input type="checkbox"/>	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
<input type="checkbox"/>	Logs 1	 Logger 4	 Logger 5	172.31.240.244	Replica Active	-	   
<input type="checkbox"/>	Logs 2	 Logger 6	 Logger 7	172.31.240.246	Primary Active	-	   

< 1 >

10 / page

Loggers - Clusters

Note that in systems with a version lower than 2.1.0, it is not possible to use a cluster of loggers in standalone mode.  
  
To use Cluster of loggers it will be necessary to use loggers with version 2.1.0 and later.

In this session we will analyze:

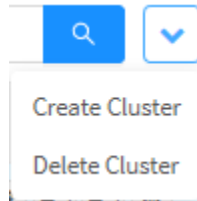
- How to [create](#), edit and [remove](#) a cluster;
- [The components of the column](#);

Next, we will analyze the [actions menu](#).

# Clusters - Actions Menu



By clicking on the **actions menu** [ ] button at the top right it is possible to add a Cluster or remove it.



Clusters - Actions menu

The menu consists of the following options:

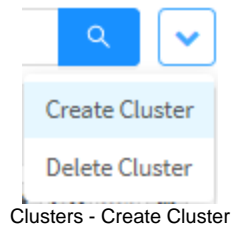
- [Create Cluster](#);
- [Delete Cluster](#).

Next, each action menu option will be detailed.



# Clusters - Actions Menu - Create Cluster

Note that the system will not allow you to register loggers already used in another cluster, integrated loggers or with versions prior to 2.1.0. To create a Cluster for the Logger, click on the "Create Cluster" option in the options menu, as shown below:



In this panel are all the configurations of the Cluster used by the high availability features of the Logger, next we will delve into how to configure each field.

Create Cluster

X

\* Name

\* Secret Key

\* Primary Logger

\* Replica Logger

\* Virtual IP

\* Netmask

\* Heartbeat Interval (seconds)

5

\* Failover Threshold

5

☐ Notifications to e-mail ⓘ

☐ Auto Activation Replica

Cancel

Save

Clusters - Create Cluster

When creating a Logger H.A. cluster, the administrator must inform the following configuration parameters:

- **Name:** Defines the Name that will be used to identify the cluster. Required field;
- **Secret Key:** Sets the secret key for the high availability cluster. The definition of this password is mandatory, in order to guarantee the trust relationship between both devices;
- **Primary Logger:** Defines the logger to be used as the primary cluster. The items that appear in this field are configured on the Logger tab, see [this page](#) for more information. This field is required;

- **Replica Logger:** Defines the logger to be used as a secondary cluster. The items that appear in this field are configured on the Logger tab, see this [page](#) for more information. Evidently the replica will not be able to use the same logger selected for the primary cluster. This field is required;



In the Primary and Replica logger fields, only loggers that are not currently being used as a cluster will be listed, in addition, the system will not allow registering integrated type loggers or that use a version prior to 2.1.0.

- **Virtual IP:** Defines the virtual IP address that will be associated with the High Availability cluster. The IP address configuration used by the high availability service cluster supports only IPv4. This field is required. Virtual IP should be added to the Blockbit Next Generation Firewall as an analyzer address for the use of Logger redundancy, for more information, see this [page](#);



**Attention:** Even if the firewall is configured to use a real IP, if it is clustered, it will still be replicated to a secondary server. However, still considering this situation, if the server fails, it will not transmit logs to the secondary server.

- **Netmask:** Determines the netmask that will be used by the virtual IP address. This field is required;
- **Heartbeat Interval:** Determines the monitoring interval, defining when the connection and synchronism tests between the devices will be made. This field is required;
- **Failover Threshold:** Determines the limit of failures in the Heartbeat tests, if the maximum value of errors generated by the Heartbeat tests is reached, the secondary Logger will be activated and the primary will go into standby making the failover automatically. *This field is required;*
- **Notifications to E-mail** ☐: If the checkbox is enabled, the administrator will be able to register an address for receiving notification emails, messages will be sent in real time in failover and synchronism events. In addition, the language used by e-mail is not the same as that used in the interface, but the one configured in the system, for more information, see this [page](#). For the sending of notifications to be carried out, it is necessary to configure the e-mail tab in Network, for more information, see this [page](#);



When changing the language, keep the two Loggers on, otherwise the configuration will not be synchronized for the Logger that is turned off.

If you have changed the language in the System menu, General tab, Settings option in the Language field, it will be necessary to save the cluster again to start receiving emails in the new selected language.

- **Auto Activation Replica** ☐: If the check box is enabled, the failover of the primary logger by the secondary will be done automatically. The activation of the Primary Logger is done manually through the Active Primary Logger button, for more information see this [page](#).



**Attention:** To ensure that the backup is recorded when the secondary server is Active, it is recommended to make sure that the automatic backup routine on the secondary server is active. For more information, see this [page](#). The Secondary server will not write backups to external storage while it is in standby.

Save

Cancel

To finish creating the cluster, click [ Save ]. If you want to cancel, click [ Cancel ].

Having created the Cluster correctly and having the Notifications to E-mail field correctly configured, the administrator will be notified every time the secondary logger server is activated, as shown below:

Failover Loggers Cluster: Replica active



Responder Responder a Todos Encaminhar ...  
ter 02/03/2021 13:01

**Failover Loggers Cluster: Replica active**


The cluster was switched to the replica logger in 02/03/2021 - 13:01:11. After the primary logger is restored, to return the active cluster to that logger, it is necessary to activate the primary logger manually.

*E-mail Notification*


Next, we will detail the [Delete Cluster](#) option.

# Clusters - Actions Menu - Delete Cluster

Through the button "Delete Cluster" it is possible to delete the selected Clusters. To delete from the Actions Menu, follow these steps:



After deleting the Cluster, the Blockbit Next Generation Firewall will stop sending logs, as the registered virtual IP, will no longer exist, thus entering the status of "STOPPED".

1. Select which Cluster (s) you want to delete. To select, just click with the mouse on the checkbox that is located next to the Name. In the selected clusters the checkbox will change from white to blue ;

Loggers


Loggers Clusters

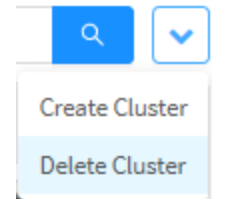
2 records

<input type="checkbox"/>	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
<input checked="" type="checkbox"/>	TEST	Logger 4	Logger 5	172.31.240.244	Replica Active	-	
<input type="checkbox"/>	Cluster Logger 1-2	Logger1	Logger2	172.31.240.241	Replica Active	-	

< 1 > 10 / page

Clusters - Selection of Clusters to delete

2. Enter the **actions menu**  and click on the option "Delete Profile".



Clusters - Delete Cluster

3. The notification message will appear asking if you really want to delete the selected Clusters:

Delete Cluster

Are you sure you want to delete the following cluster ?

- TEST

Cancel Delete

Clusters - Delete Cluster

Cancel

Delete

If you wish to cancel, click on the [ ] button. To finish, click on the [ ] button.



Cluster deleted successfully

*Cluster deleted successfully*

After performing these procedures, the Clusters will have been successfully deleted.



After deleting the cluster, the linked loggers will again be available for editing and use as a *normal logger*.

Next, we will detail the components of the [columns](#).

# Clusters - Columns

Below we will detail each column of the Clusters tab:

Loggers

Loggers Clusters

2 records

Name

Primary Logger

Replica Logger

Virtual IP

Status

Synchronization

Actions

Cluster Logger 4-5

Logger 4

Logger 5

172.31.240.244

Replica Active

61%

Cluster Logger 1-2

Logger1

Logger2

172.31.240.241

Primary Active

<

1

>

10 / page

Loggers - Clusters Tab

- **Select**[]: Allows you to select one or more clusters;
- **Name**: Displays the name of the Logger Cluster;
- **Primary Logger**: Displays the name and connection status of the Primary server, which can be:
  - []: Represents that the logger is online;
  - []: Represents that the logger is offline;
- **Logger Replica**: Displays the name and connection status of the Secondary server, which can be:
  - []: Represents that the logger is online;
  - []: Represents that the logger is offline;
- **Virtual IP**: Displays the Virtual IP added in [Create Cluster](#);
- **Status**: This column displays the current status of the Loggers, which can be:
  - []: Represents that the primary logger is active;
  - []: Represents that the secondary logger is active;
- **Sync Progress**: Displays the sync progress bar between clusters;
- **Actions**: Provides the following essential functions;
  - **Edit**[]: Allows you to edit one of the servers created in the [Create Cluster](#) option in the actions menu;
  - **Active Primary Logger**[]: This button allows you to manually activate the primary cluster;
  - **Active Replica Logger**[]: This button allows you to manually activate the secondary cluster;
  - **Delete**[]: Allows you to delete a cluster, it is equivalent to the [Delete Cluster](#) option in the actions menu.

After a manual activation or after failover detection, the secondary interface takes at least 30 seconds to activate.

Despite this, synchronization can take a much longer time depending on the amount of information and the network structure of the administrator.

For more detailed information about the synchronization process, it is possible to follow the progress through the CLI command [\[debug-ha\]](#).

In addition to the status and the sync progress bar, it is possible to check the status of the synchronism and activation of the Logger clusters by accessing the CLI and using the [\[debug-ha\]](#) command;

```
admin >debug-ha
date="2021-03-02 17:20:50" status="threshold" status_message="peer error 4/5"
date="2021-03-02 17:20:57" status="threshold" status_message="peer error 5/5"
date="2021-03-02 17:21:00" status="failover" status_message="can't connect to primary logger"
date="2021-03-02 17:21:01" status="error" status_message="Sync peer connection error, progress: 0%"
date="2021-03-02 17:21:05" status="failover" status_message="secondary server, new status: active"
```

CLI - debug-ha

When activating the Loggers manually, an audit log is generated, which can be analyzed in the Settings menu, Administration option, in the [Audit Log](#) tab, as shown in the image below:

Administration

AdministratorsUsers ProfilesAuth ServersIdentity ProviderAudit Log

137 records

Date	User	Interface	Activity	IP	Actions
2021-03-05 09:50:13	admin	loggers-clusters	Update	192.168.200.5	
2021-03-05 09:50:11	admin	loggers-clusters	Update	192.168.200.5	
2021-03-05 09:29:13	admin	loggers-clusters	Update	192.168.200.5	
2021-03-04 15:37:48	admin	loggers-clusters	Update	192.168.111.77	
2021-03-04 15:05:30	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:03:48	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:02:34	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:34:02	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:33:59	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:31:53	admin	loggers-clusters	Delete	192.168.111.77	

< 1 2 3 4 5 ... 14 > 10 / page

Administration - Audit Log

When activating one of the loggers, the activity event is listed as an update. You can consult more information about clicking on the button.

Audit View

```
"Audit Information" : {
  "logger_id" : "4"
  "logger_name" : "Logger 5"
  "activate-logger" : true
}
```

Close


Audit Log - Audit view

As shown in the image above, when performing manual activation, the "activate-logger" line will be marked as "true";

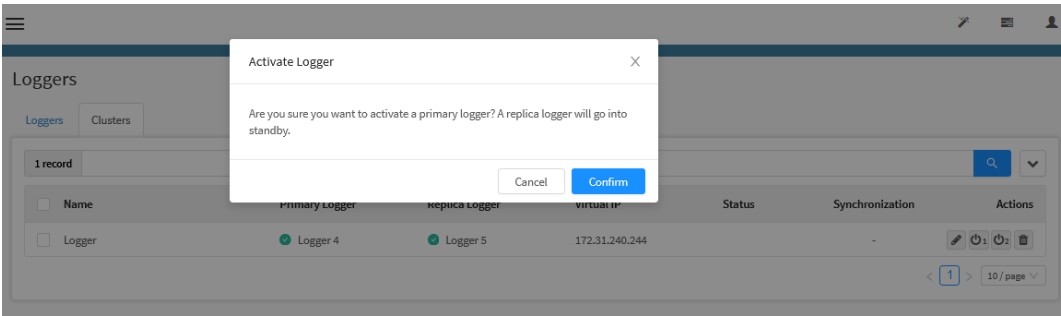
For more information on the loggers see this [page](#).

# Clusters - Active Primary Logger


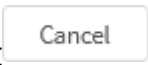
When you click the **Active Primary Logger**  button, a confirmation message will be displayed on the screen, as shown below:




As mentioned in the email received in a failover event, the primary logger must be activated manually when there is a guarantee that it is stable, thus avoiding the loss of logs during instability.



Clusters - Activate Logger

Click  to activate the Primary Logger manually and leave the Secondary Logger in Standby. Otherwise, click  to close this window.

When activating the logger, the following confirmation will be displayed:




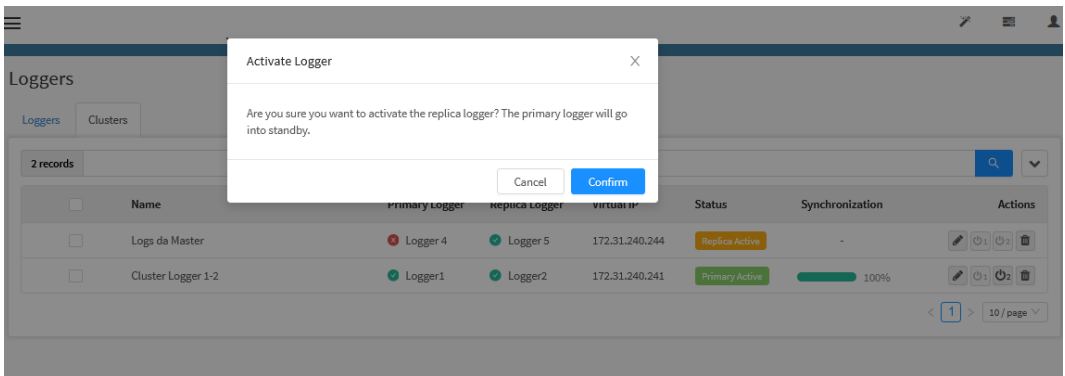
Logger activated successfully. Wait the synchronization to finish in a few minutes.

Logger activation message


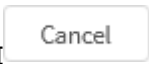
The procedure described on this page is very similar to that performed on the [Active Replica Logger](#) button.  
For more information about the other options displayed in the columns in Clusters, see this [page](#).

# Clusters - Active Replica Logger


When you click the **Active Replica Logger**  button, a confirmation message will be displayed on the screen, as shown below:



Clusters - Activate Replica Logger

Click  to activate the secondary logger manually and leave the primary logger in standby. Otherwise, click  to close this window.

When activating the logger, the following confirmation will be displayed:

 **Logger activated successfully. Wait the synchronization to finish in a few minutes.**

Logger activation message

The procedure described on this page is very similar to that performed on the [Active Primary Logger](#) button.  
For more information about the other options displayed in the columns in Clusters, see this [page](#).



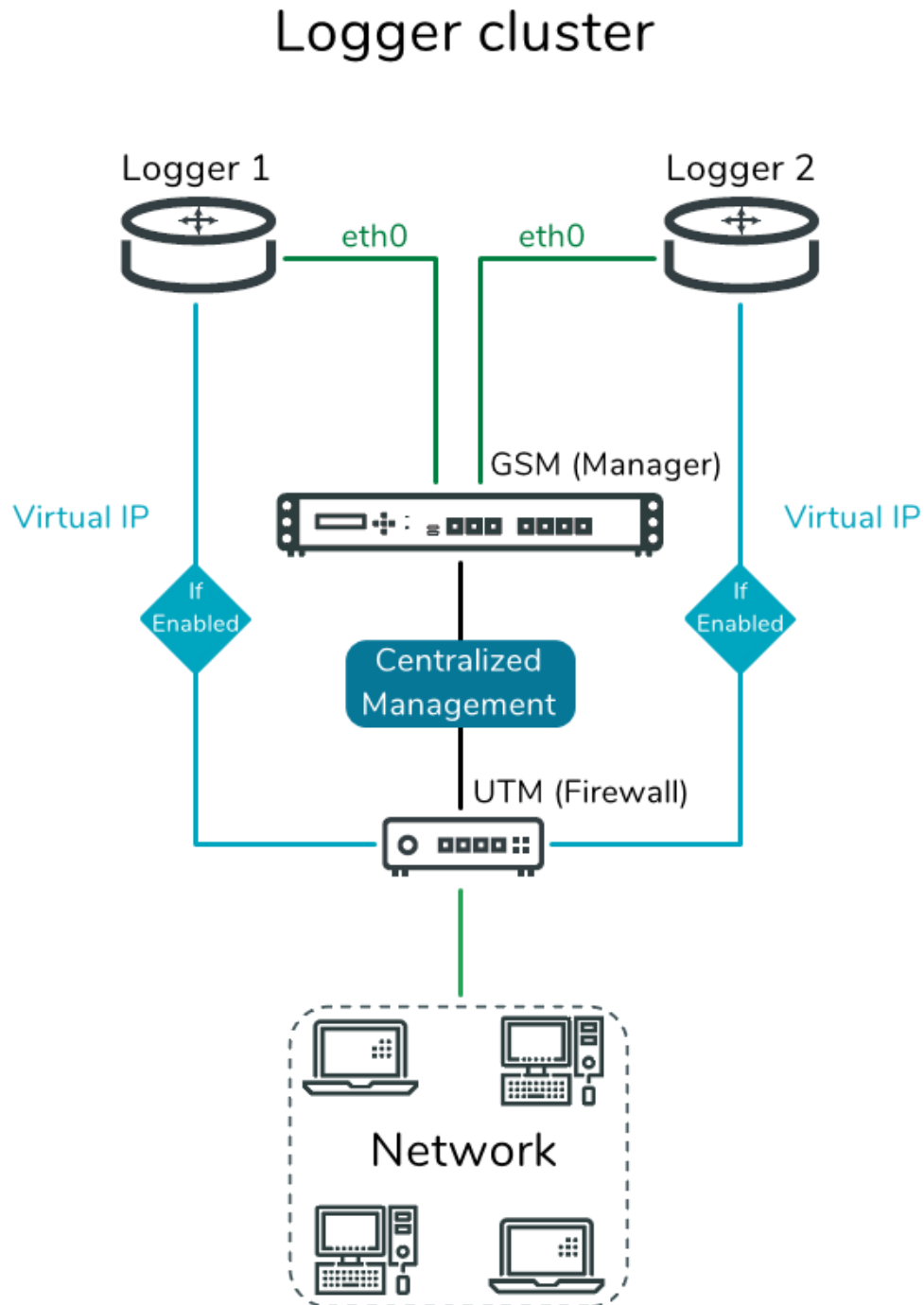
# Clusters - Example

This section will present the step by step to configure a primary and secondary Cluster Logger.



For more information about Logger Clusters see this [page](#).

This demonstration will consider the following structure:



Logger Cluster - Structure

The following IPs will be used in this example:

Logger Cluster - IP Addressing

Name	IP adress	Virtual IP
Primary Cluster	172.31.240.1	172.31.240.241
Secondary Cluster	172.31.240.2	

The steps we will take in this demonstration will be:

- [Configuration of Interfaces and Loggers](#);
- [Clusters configuration](#);
- [Settings Validation](#).

We will start the demo by configuring the [Interfaces and Loggers](#).

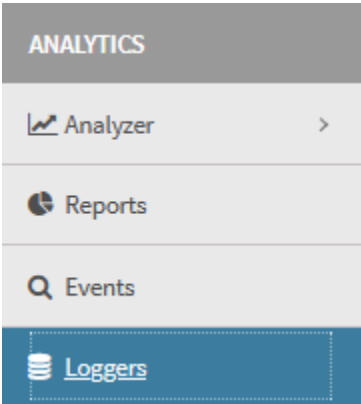
# Clusters - Configuration of Interfaces and Loggers

In this example we will make the following settings:

- First, it is necessary to install the loggers that will be used, follow the guidelines on this [page](#) and store the secret key in a safe place;
- Loggers configuration.

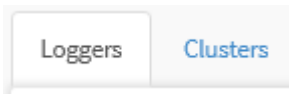
## Logger settings

Access the Analytics menu and click on the option Loggers:



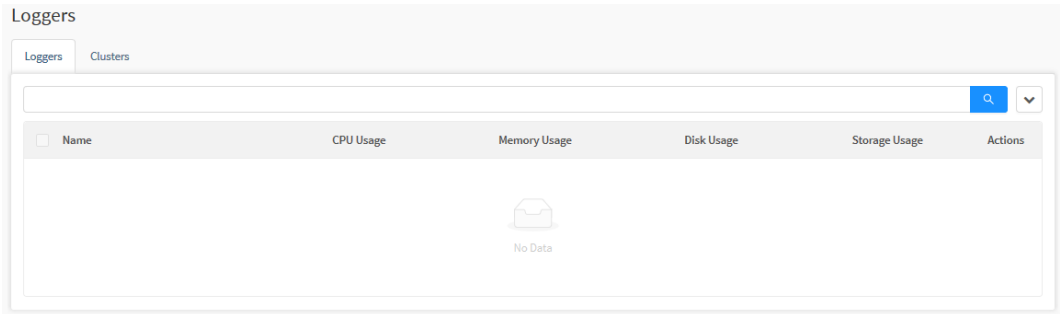
Analytics - Loggers

Click on the Loggers tab:



Loggers tab

The following screen will be displayed:



Loggers - Loggers

Next we will detail the panels that will be configured.

# Logger Device

Complete the form as shown below:

Create Logger Device

Settings

Storage

General

\* Name

Logger 1

\* Mode

Standalone

\* Description

Logger 1

\* Interface

eth0

\* Address

172.31.240.1

\* Secret Key

53616c7465645f5f4acdb42d25e6c954fb6629ebed20d33fa393d37661d56d7aea665beb18045ed40e1f04c4007a3fecb9b5ab6ee20ebc0de9f86845797e25fe0df00ff40984613fdb94dd8985eea409ca2ee4526e3d9516d879f1b0b08aa91bab28249e9cdf29f7d7212a072cd0ff

Devices & Devices Group

Select a type

Cancel

Save

Loggers - Create Logger Device

- **Name:** We will name the logger "Logger 1";
- **Mode:** We will use a "Standalone" logger;
- **Description:** As a description we will simply type "Logger 1";
- **Interface:** In this field, the same interface that was configured in the logger installation process is added;
- **Address:** In this field the IP that was configured when installing the Logger is added, in this example we will use the IP 172.31.240.1;
- **Secret Key:** In this field you must paste the secret key that was generated when installing the Logger;
- **Devices & Devices Group:** Add the inventory devices you want to use with the logger. This example will not consider this step.

We will not configure the other fields, click [ 

Save

 ] to save the settings.

Next, we will configure the secondary Logger, we will use the following settings:

712

Edit Logger Device

×

Settings

Storage

General

\* Name

Logger2

\* Mode

Standalone

\* Description

Logger 2

\* Interface

eth0

\* Address

172.31.240.2

\* Secret Key

53616c7465645f5f40eae74aa339f8937fa8dc535c63931cf9a7d4dd1e78b122330e94  
b6d2ab42a90061be740b04ead3e786c8db8efb6bd58ff4d0fa8680d228027e37512585  
c6c0380e997dd4f8002c081ba35341bf5e992bd327e051c66c3c09f280d59eb46472610

Devices & Devices Group

Select a type

+

UTM211

-

Cancel

Save

#### Loggers - Create Logger Device

- **Name:** We will name the logger "Logger 2";
- **Mode:** We will use a "Standalone" logger;
- **Description:** As a description we will simply type "Logger 2";
- **Interface:** In this field, the same interface that was configured in the logger installation process is added;
- **Address:** In this field the IP that was configured when installing the Logger is added, in this example we will use the IP 172.31.240.2;
- **Secret Key:** In this field you must paste the secret key that was generated when installing the Logger;
- **Devices & Devices Group:** Add the inventory devices you want to use with the logger. This example will not consider this step.

We will not configure the other fields, click  to save the settings.

When finishing all the configurations, the screen will be as shown below:

Loggers

Loggers

Clusters

2 records

Loggers

Clusters

<input type="checkbox"/>	Name	CPU Usage	Memory Usage	Disk Usage	Storage Usage	Actions
<input type="checkbox"/>	<div> <div></div> <div>Logger1</div> </div>	<div> <div></div> <div>0%</div> <div>8 core(s)</div> </div>	<div> <div></div> <div>62%</div> <div>15.6 GB</div> </div>	<div> <div></div> <div>6%</div> <div>7.7 GB</div> </div>	Storage unavailable	<div> <div></div> <div></div> <div></div> </div>
<input type="checkbox"/>	<div> <div></div> <div>Logger2</div> </div>	<div> <div></div> <div>0%</div> <div>8 core(s)</div> </div>	<div> <div></div> <div>62%</div> <div>15.6 GB</div> </div>	<div> <div></div> <div>6%</div> <div>7.7 GB</div> </div>	Storage unavailable	<div> <div></div> <div></div> <div></div> </div>

< 1 >

10 / page

Loggers - Loggers

This finalizes the configuration of the loggers, next we will [configure the cluster of Loggers](#).

# Clusters - Configuration Validation

To carry out the validation, we will access the CLI of the Primary and Secondary Logger and run some commands, if you need more information about this, consult this [page](#).

One of the simplest tests to validate the communication between the Loggers is to [ping](#) the Primary (172.31.240.1) to the Secondary (172.31.240.2) and check for an answer, as shown in the image below:

```
admin >ping 172.31.240.2
PING 172.31.240.2 (172.31.240.2) 56(84) bytes of data.
64 bytes from 172.31.240.2: icmp_seq=1 ttl=64 time=2.04 ms
64 bytes from 172.31.240.2: icmp_seq=2 ttl=64 time=0.454 ms
64 bytes from 172.31.240.2: icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from 172.31.240.2: icmp_seq=4 ttl=64 time=0.533 ms
64 bytes from 172.31.240.2: icmp_seq=5 ttl=64 time=0.483 ms

--- 172.31.240.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4065ms
rtt min/avg/max/mdev = 0.454/0.957/2.041/0.622 ms
admin >
```

CLI - Validation of communication from the Primary to the Secondary Logger

It is also possible to carry out these same steps at the other end, following a demonstration using the [ping](#) command to verify the communication from the Secondary Logger (172.31.240.2) to the Primary (172.31.240.1):

```
admin >ping 172.31.240.1
PING 172.31.240.1 (172.31.240.1) 56(84) bytes of data.
64 bytes from 172.31.240.1: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from 172.31.240.1: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 172.31.240.1: icmp_seq=3 ttl=64 time=0.281 ms
64 bytes from 172.31.240.1: icmp_seq=4 ttl=64 time=0.298 ms
64 bytes from 172.31.240.1: icmp_seq=5 ttl=64 time=0.246 ms
64 bytes from 172.31.240.1: icmp_seq=6 ttl=64 time=0.241 ms

--- 172.31.240.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5078ms
rtt min/avg/max/mdev = 0.241/0.351/0.754/0.182 ms
admin >
```

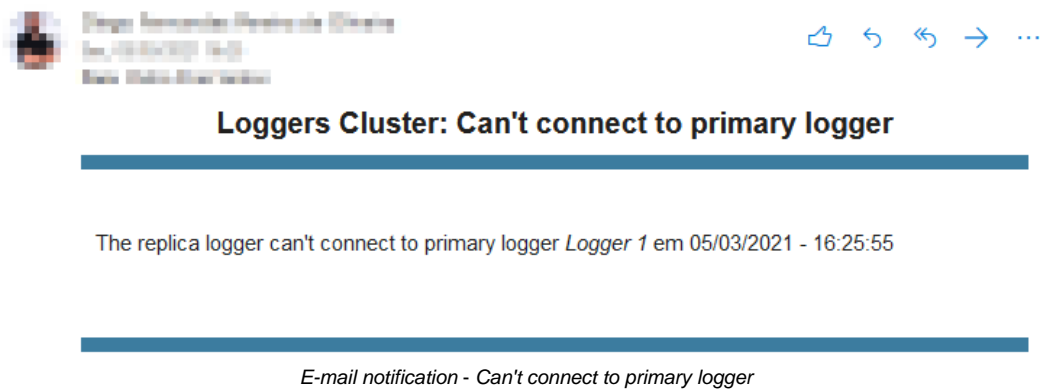
CLI - Secondary to Primary Logger communication validation using the Ping command

Another test that we can perform is: Use the [\[shutdown\]](#) command on the active primary Logger to check through [\[debug-ha\]](#) if the secondary one will fail over and be activated automatically, following what should be displayed in the CLI of the secondary Logger:

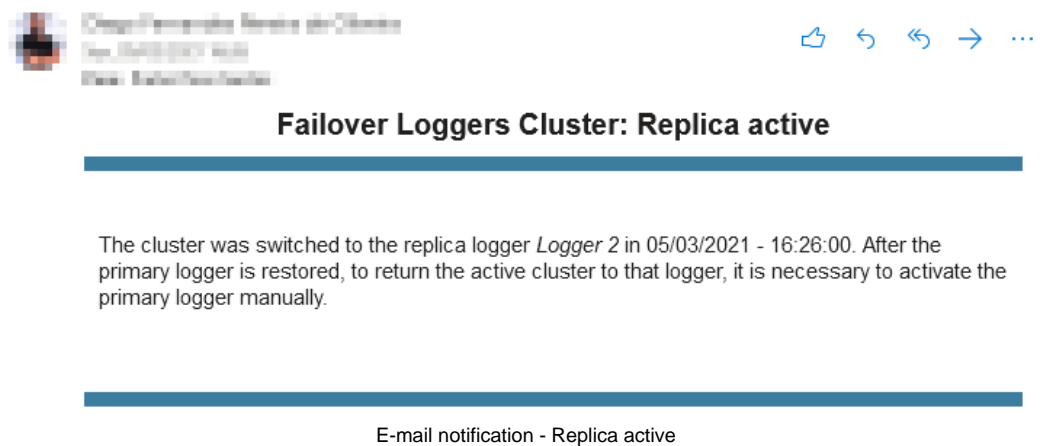
```
admin >debug-ha
date="2021-03-05 16:25:09" status="threshold" status_message="peer error 1/5"
date="2021-03-05 16:25:19" status="threshold" status_message="peer error 2/5"
date="2021-03-05 16:25:29" status="threshold" status_message="peer error 3/5"
date="2021-03-05 16:25:39" status="threshold" status_message="peer error 4/5"
date="2021-03-05 16:25:49" status="threshold" status_message="peer error 5/5"
date="2021-03-05 16:25:55" status="failover" status_message="can't connect to Primary logger"
date="2021-03-05 16:25:57" status="error" status_message="Sync peer connection error, progress: 0%"
date="2021-03-05 16:26:00" status="failover" status_message="secondary server, new status: active"
```

CLI - debugging H.A. on the Secondary Logger displaying failover

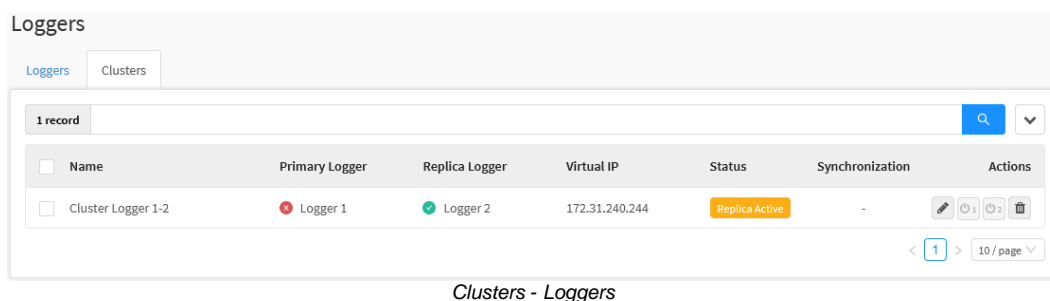
If an e-mail has been registered, as exemplified when [configuring the Cluster](#), a notification will be sent all notifying that the primary logger is offline:




And after the failover has successfully run, a notification that the secondary logger has taken priority in the cluster:



In addition, these changes are represented in the interface, as shown in the image below (For more information see this [page](#)):



When rewiring the Primary Logger, [\[debug-ha\]](#) will recognize that it has been turned on, however, it will not automatically activate, this behavior is normal. To actually activate the primary, it will be necessary to access the system interface and perform this process manually through the **Activate**

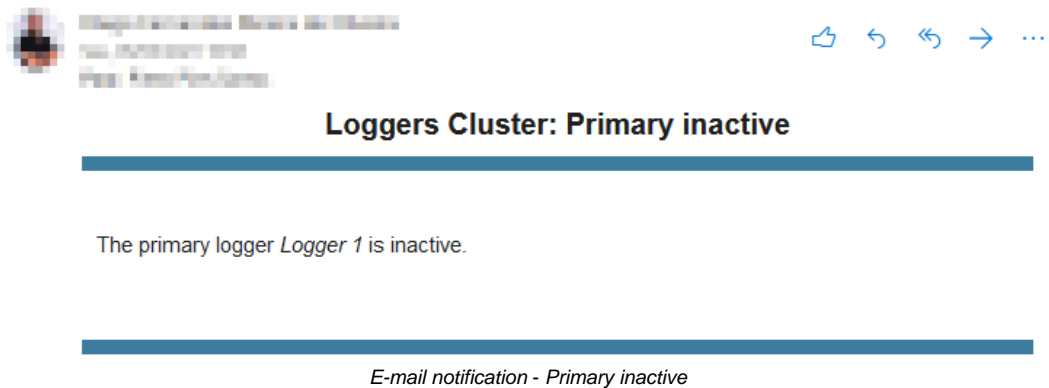
Primary Logger [  ], button, following what is displayed in the CLI:



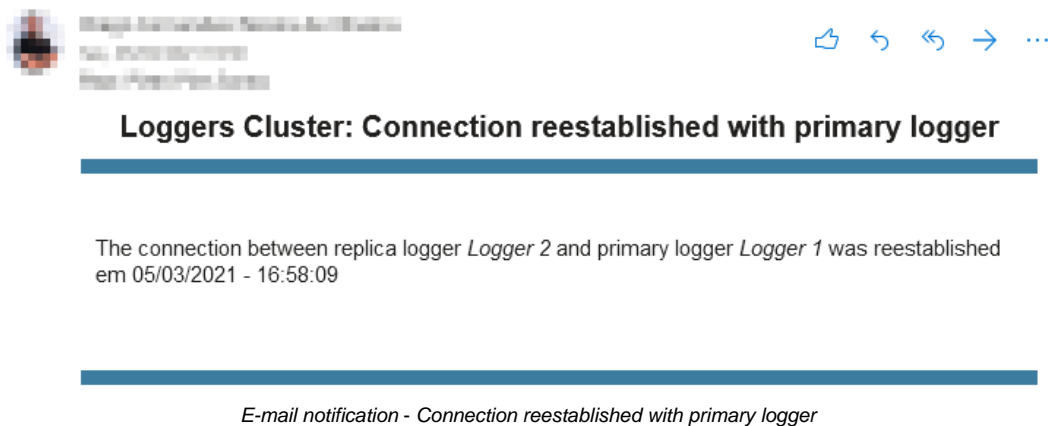
```
admin >debug-ha
date="2021-03-05 16:58:09" status="failover" status_message="connection reestablished with Primary logger"
```

CLI - H.A. debug on the Secondary Logger detecting activation of the Primary Logger

When the Primary Logger goes online again, an email will be sent acknowledging this event but detecting that it is inactive, after all, the Secondary Logger is active:



And after the synchronism runs, one more notification will be sent:



The interface will represent this situation with the icon next to the Primary Logger showing that it is online, but the status indicating that the secondary is active:

Loggers


Loggers Clusters

1 record

<input type="checkbox"/>	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
<input type="checkbox"/>	Cluster Logger 1-2	<span>●</span> Logger 1	<span>●</span> Logger 2	172.31.240.244	Replica Active	-	

< 1 > 10 / page

Clusters - Loggers

To activate the Primary Logger when the secondary is online, we must click on the **Activate Primary Logger**  button. Again, it is possible to observe the behavior of the Loggers through the command `[debug-ha]`, in the Primary Logger, the entire synchronization and activation process will be detailed:

```
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 99%"
date="2021-03-05 17:21:38" status="" status_message="Sync , progress: 100%"
date="2021-03-05 17:21:38" status="done" status_message="Sync , progress: 100%"
date="2021-03-05 17:22:57" status="done" status_message="Sync , progress: 100%"
date="2021-03-05 17:22:59" status="failover" status_message="primary server, new status: active"
```

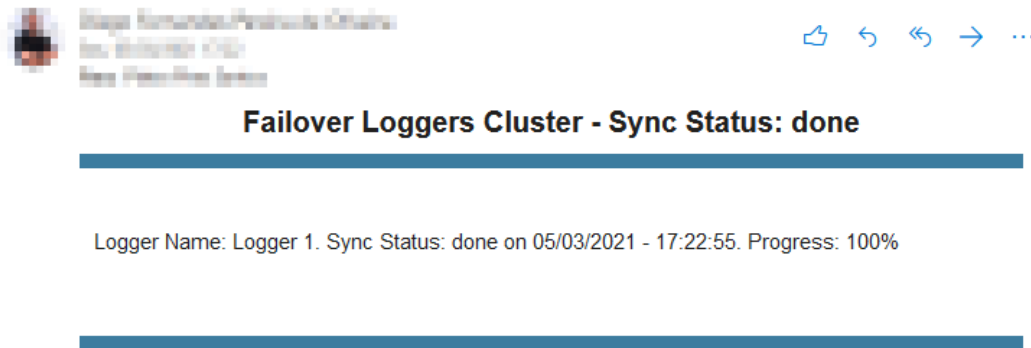
CLI - H.A. debug on the Primary Logger detecting Primary Logger activation and timing

Following is the information that is displayed considering the same scenario mentioned above, however when applying the command `[debug-ha]` in the Secondary Logger:

```
admin >debug-ha
date="2021-03-05 17:23:00" status="failover" status_message="secondary server, new status: inactive"
```

CLI - debugging H.A. on the Secondary Logger

When the synchronization of the Primary Logger is finished, an email will be sent acknowledging this event:



*E-mail - Sync status: done*

Another email will point to the activation of the Primary Logger:



## Failover Loggers Cluster: Primary active

The cluster was switched to the primary logger *Logger 1* in 05/03/2021 - 17:22:59.

*E-mail - Primary Active*

And finally, one last email will recognize that the Secondary Logger has been deactivated:



## Loggers Cluster: Replica inactive

The replica logger *Logger 2* is inactive.

*E-mail - Replica Inactive*

The interface will represent this situation with the icon next to the Primary Logger showing that it is online, and the status denoting that the Primary is active:

Loggers						
Loggers		Clusters				
1 record						
<input type="checkbox"/>	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization
<input type="checkbox"/>	Cluster Logger 1-2	<input checked="" type="checkbox"/> Logger 1	<input checked="" type="checkbox"/> Logger 2	172.31.240.244	Primary Active	-

*Clusters - Loggers*

Finally, when making any manual activation of the Loggers, an audit log is created in [Audit Log](#), detailing more information about the activity performed, as shown in the image below:

Administration

AdministratorsUsers ProfilesAuth ServersIdentity ProviderAudit Log

134 records

Date	User	Interface	Activity	IP	Actions
2021-03-04 15:37:48	admin	loggers-clusters	Updates	192.168.111.77	
2021-03-04 15:05:30	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:03:48	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 15:02:34	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:34:02	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:33:59	admin	loggers	Delete	192.168.111.77	
2021-03-04 12:31:53	admin	loggers-clusters	Delete	192.168.111.77	
2021-03-04 12:22:52	admin	analyzer-reports	Save	192.168.111.77	
2021-03-04 12:19:20	admin	loggers-clusters	Edit	192.168.111.77	
2021-03-04 12:14:30	admin	analyzer-reports	Save	192.168.111.77	

< 1 2 3 4 5 ... 14 > 10 / page

Administration - Audit Log

When activating one of the loggers, the activity event is listed as an update. You can consult more information about clicking on the [] button.

Audit View

```

{
  "Audit Information": {
    "logger_id": "4"
    "logger_name": "Logger 5"
    "activate-logger": true
  }
}

```

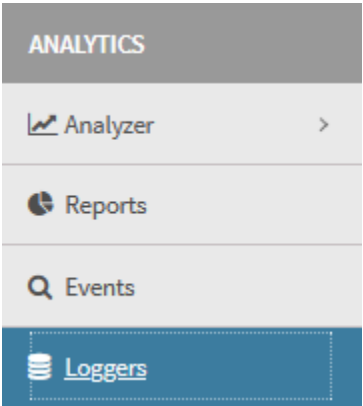
Close

Audit Log - Audit view

This ends the demonstration, for more information about the Cluster of Loggers, see this [page](#).

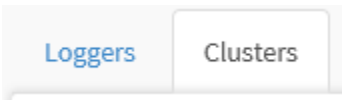
# Clusters - Logger Cluster Configuration

After configuring the [Loggers](#), we will configure the Cluster, access the Analytics menu and click on the Loggers option:




Analytics - Loggers

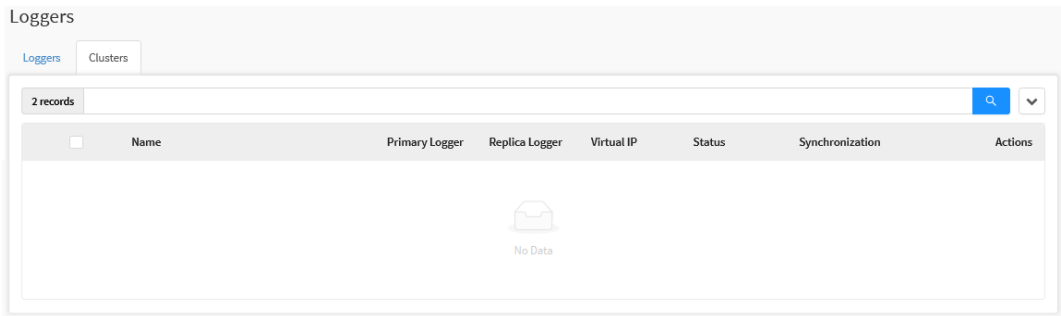
Click on the Clusters tab:



Clusters Tab

 Some details of the Clusters tab will not be considered in this example, if you want more information, see this [page](#).

The following screen will be displayed:



Loggers - Clusters

Configure the Logger Cluster as shown below:

Create Cluster

X

---

\* Name

Cluster Logger 1-2

\* Secret Key

.....

\* Primary Logger

Logger1

\* Replica Logger

Logger2

\* Virtual IP

172.31.240.241

\* Netmask


255.255.0.0

\* Heartbeat Interval (seconds)

5

\* Failover Threshold

5

☒ Notifications to e-mail 



admin@blockbit.com


☒ Auto Activation Replica

Cancel

Save

#### Cluster Settings

- **Name:** We will define the name as "Cluster Logger 1-2";
- **Secret Key:** Enter your secret-key.
- **Primary Logger:** We will use "Logger 1" configured in the previous step;
- **Replica Logger:** We will use "Logger 2", configured in the previous step;
- **Virtual IP:** We will use the virtual IP 172.31.240.241;
- **Netmask:** As a netmask we will use 255.255.0.0;
- **Heartbeat Interval:** We can leave the default of 5 seconds;
- **Failover Threshold:** We can leave the default 5 times;
- **Notifications to E-mail** : We will use the administrator's email to receive notifications from the Cluster;
- **Auto Activation Replica** : We will check the checkbox so that the secondary cluster is activated automatically.

Click  to finish the settings and activate the Cluster.

The screenshot below shows the Cluster already configured and enabled correctly:

Loggers

Loggers

Clusters

2 records

	Name	Primary Logger	Replica Logger	Virtual IP	Status	Synchronization	Actions
<input type="checkbox"/>	Cluster Logger 1-2	<div> <div></div> <div>Logger1</div> </div>	<div> <div></div> <div>Logger2</div> </div>	172.31.240.241	<div>Primary Active</div>	-	<div></div> <div></div> <div></div> <div></div>

<

1

>

10 / page

Network Settings - Interfaces

This finalizes the configuration of the Logger Cluster, next we will [validate the settings](#).

# Reports

This option manages the automatic and periodic creation of customized reports, allowing the selection of specific characteristics of the selected devices.

To access and manage the automatic creation of reports, click on the “Reports” icon located on the left side of the screen:



Analytics - Reports

The reports screen will be displayed:

Reports

3 records

<input type="checkbox"/>	Name	Scheduled	Owner	Period	Status	Actions
<input type="checkbox"/>	<div><div></div>Store 1 report Network traffic analysis on Store 1</div>	<div>09/12/2019 18:37:08</div> <div>Created: 09/12/2019 18:36:35</div>	admin	from: December 09, 2019 to: December 09, 2019	Pending	<div></div> <div></div>
<input type="checkbox"/>	<div><div></div>Intrusion Report Intrusion report on the stores</div>	<div>09/12/2019 18:33:19</div> <div>Created: 09/12/2019 18:35:14</div>	admin	from: December 06, 2019 to: December 08, 2019	<div>Download</div> <div>Visualize</div>	<div></div> <div></div>
<input type="checkbox"/>	<div><div></div>Store 1 report Network traffic analysis on Store 1</div>	<div>09/12/2019 18:32:06</div> <div>Created: 09/12/2019 18:32:17</div>	admin	from: December 04, 2019 to: December 09, 2019	<div>Download</div> <div>Visualize</div>	<div></div> <div></div>

< 1 >

10 / page

Reports

Next, we will analyze the function of each component of this screen.



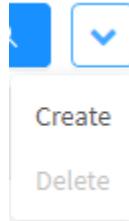
# Reports - Actions Menu

At the top right of the screen we have the actions menu:



Reports – Actions Menu Button

By clicking on this button the menu below is displayed:



Reports – Actions menu

The menu consists of the following options:

- [Create](#);
- [Delete](#).

Next, each action menu option will be detailed.

# Reports - Actions Menu - Create

To create an automatic report click on "Create", the following screen will be displayed:

## Settings tab

Create Report

X

Settings

Datasets

Custom

\* Name

\* Description

Type

Analyzer

▼

\* Scheduled

Select date

Recurrence

Unique

▼

\* Period

Start date

~

End date

\* Device/Logger

Select Device/Logger

▼

☐ Send Report by Email

Cancel

Create

Reports – Create Report - Settings

Next we will analyze each field in this panel:

- **Name:** Displays the report name. Ex.: *Store 1 report*;
- **Description:** Displays the report description. Ex.: *Network traffic analysis on Store 1*;
- **Type:** This collapsible menu determines the options that will be available in the "Datasets" tab, where the following options are:
  - **Analysis:** Allows the creation of the following reports in the Datasets tab:
    - **Network Traffic**;
    - **Policy Usage**;
    - **Web Filter**;
    - **Application Control**;
    - **Intrusion Prevention**;
    - **Threat Protection**;
    - **User Behavior**.

- **Log:** Allows the creation of a personalized report, in Datasets it is possible to use customized Queries and determine the filters to be used. It ensures the export of the logs on the CSV filetype.

- **Scheduled:** Displays the schedule date for when this report will be run;
- **Recurrence:** Recurrence with which the reports will be generated. (A single time, weekly, monthly).
- **Period:** Determines the period when the data will be analyzed by the logger in the UTMs. Ex.: When selecting from September 1, 2018 to October 24, 2018, all the data from beyond that period will not be displayed in the "Report";
- **Device/Logger:** The device from which the data will be analyzed is selected to generate the report.
- **Send report by e-mail:** Mark this option [ ☒ **Send Report by Email** ] to receive the reports generated in the analytics via e-mail, as often as they are generated.

In reports it's possible to clone a report through the edit button. Just click on the view button, then edit the report profile's name and clone the profile. By doing so, it will be possible to replicate reports and charts for editing.

It's important to remember that to receive the reports it is necessary to configure the [e-mail](#) option.

## *Datasets tab*

The "Datasets" tab determines the type of graph that will be generated, as previously mentioned, its components are determined by the "Type" checkbox on the "Settings" tab.

Create Report

X

Settings

Datasets

Custom

Analysis

Network Traffic

▼

Cancel

Create

Reports – Create Report - Datasets

## Custom Tab

In the "Custom" tab it is possible to determine the text that will be shown in the "Footer" and customize the "Logo" that will appear in the report.

Create Report


Settings

Datasets

Custom

Footer Text

Customize Logo



Cancel

Create

Reports – Create Report - Custom

Click on the [

Cancel


] button to exit this window or click on [

Create

] to schedule the report. If you want to issue it immediately, configure it to run on the current date.













# Reports - Actions Menu - Delete

It is possible to delete selected Reports. To delete via the Actions menu, follow these steps:

1. Select which Report (s) you want to delete. To select, just check the desired report's checkbox. In the selected reports the checkbox will change from gray to blue . Ex.: Test;

Reports

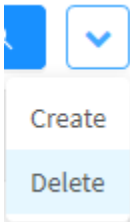
4 records

<input type="checkbox"/>	Name	Scheduled	Owner	Period	Status	Actions
<input checked="" type="checkbox"/>	 Test test	09/12/2019 19:06:02 Created: 09/12/2019 19:06:25	admin	from: December 09, 2019 to: December 09, 2019	Pending	 
<input type="checkbox"/>	 Store 1 report Network traffic analysis on Store 1	09/12/2019 18:37:08 Created: 09/12/2019 18:36:35	admin	from: December 09, 2019 to: December 09, 2019	Pending	 
<input type="checkbox"/>	 Intrusion Report Intrusion report on the stores	09/12/2019 18:33:19 Created: 09/12/2019 18:35:14	admin	from: December 06, 2019 to: December 08, 2019	Pending	 
<input type="checkbox"/>	 Store 1 report Network traffic analysis on Store 1	09/12/2019 18:32:06 Created: 09/12/2019 18:32:17	admin	from: December 04, 2019 to: December 09, 2019	Pending	 

< 1 > 10 / page

Reports – Selection of Reports to delete

2. Enter the **actions menu** [  ] and click on the “Delete” option.



Reports – Delete

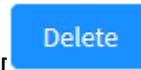
3. A confirmation message will be shown to confirm the deletion of the selected Reports:

Delete Profile

Delete Test reports?

CancelDelete

## Reports – Report deletion message



If you wish to cancel click on the [ ] button. To conclude, click on the [ ] button.



**Profile deleted successfully!**

Profile successfully deleted

After performing these procedures, the reports will have been successfully deleted.

# Reports - Columns

Next, we will go through each column of the *Reports* tab:

Reports

3 records

<input type="checkbox"/>	Name	Scheduled	Owner	Period	Status	Actions
<input type="checkbox"/>	<div><div>Store 1 report</div><div>Network traffic analysis on Store 1</div></div>	<div>09/12/2019 18:37:08</div> <div>Created: 09/12/2019 18:36:35</div>	admin	from: December 09, 2019 to: December 09, 2019	Pending	<div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>Intrusion Report</div><div>Intrusion report on the stores</div></div>	<div>09/12/2019 18:33:19</div> <div>Created: 09/12/2019 18:35:14</div>	admin	from: December 06, 2019 to: December 08, 2019	<div>Download</div> <div>Visualize</div>	<div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>Store 1 report</div><div>Network traffic analysis on Store 1</div></div>	<div>09/12/2019 18:32:06</div> <div>Created: 09/12/2019 18:32:17</div>	admin	from: December 04, 2019 to: December 09, 2019	<div>Download</div> <div>Visualize</div>	<div><div></div><div></div></div>

< 1 >

10 / page

Reports

- **Select** [ ☐ ]: Allows the selection of a *report*;
- **Name**: Displays the name of the report registered in the *Create* option of the action menu. Just below the name is the description registered in the same menu;
- **Scheduled**: Displays the schedule for when the report will be executed, just below that date is marked the date when this process was created;
- **Owner**: This schedule creator's name;
- **Period**: This is the period from which the data will be extracted from the system and recorded;
- **Status**: The current production status of the report is displayed. In this column is also viewable by clicking on the [ 

Visualize

 ] button or downloadable in PDF format by clicking the [ 

Download

 ] button after the report has been generated. Ex.: Pending;
- **Actions**: Buttons with essential functions for interacting with reports:
  - **Visualize**[  ]: Allows the editing of the settings of the Report added in the *Create* option of the actions menu;
  - **Remove**[  ]: Deletes the selected report.



# Events

The Events panel displays all occurrences of a specific logger or group of devices.

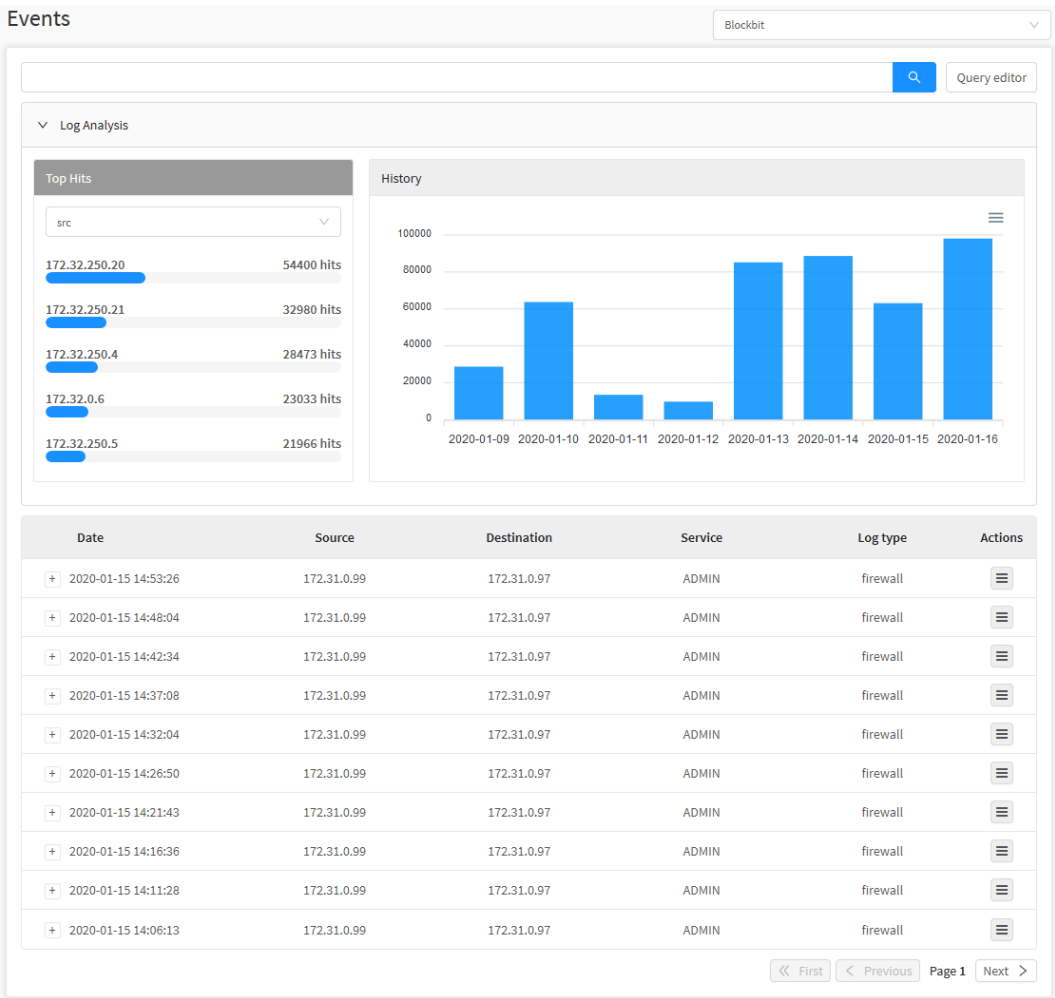
This panel has some features that allow a more detailed in-depth analysis: Through this panel it is possible to perform a search according to personalized queries, to analyze specific incidents and eventualities, allowing a much more precise and efficient administration.

To access the events screen, click on the "Events" icon located on the left side:



Analytics - Events

The "Events" screen will be displayed. It is composed by the internal staff "Top Hits", "History" and "Log Events". In addition, at the upper right of the screen is the search bar and the "query editor".



Events

As soon as "Events" is accessed, a selection box is displayed on the right corner of the screen, to view the Events it is necessary to select the desired logger or group of devices in this selection panel. As shown below:

Blockbit

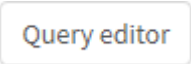
▼

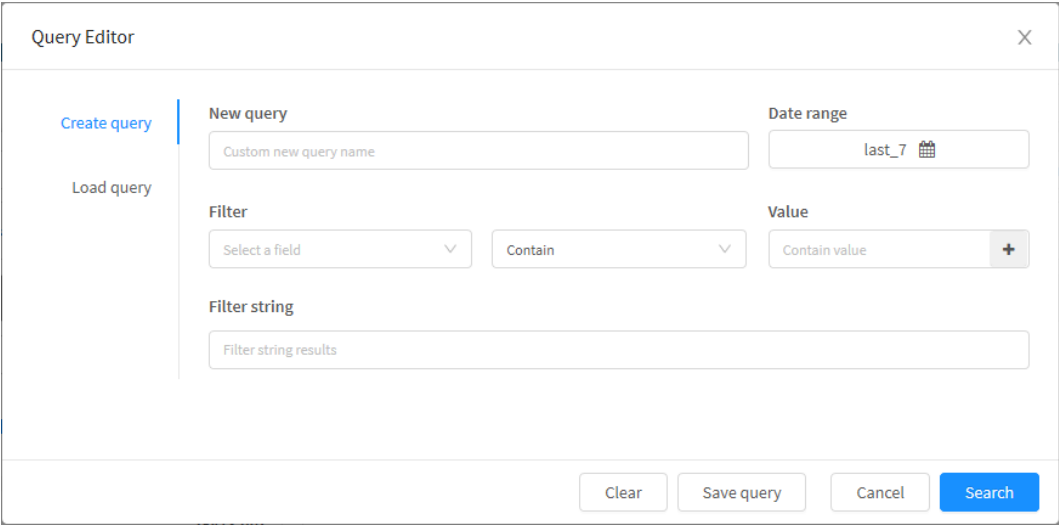
*Events - Logger selection*

After selecting the desired option, the relevant events will be automatically displayed.

Next, the components of the events panel will be analyzed.

# Events - Query Editor

Through the query editor, it is possible to create, edit and save a query to perform an in-depth search of events, by clicking on the [  ] button the following window will be displayed:



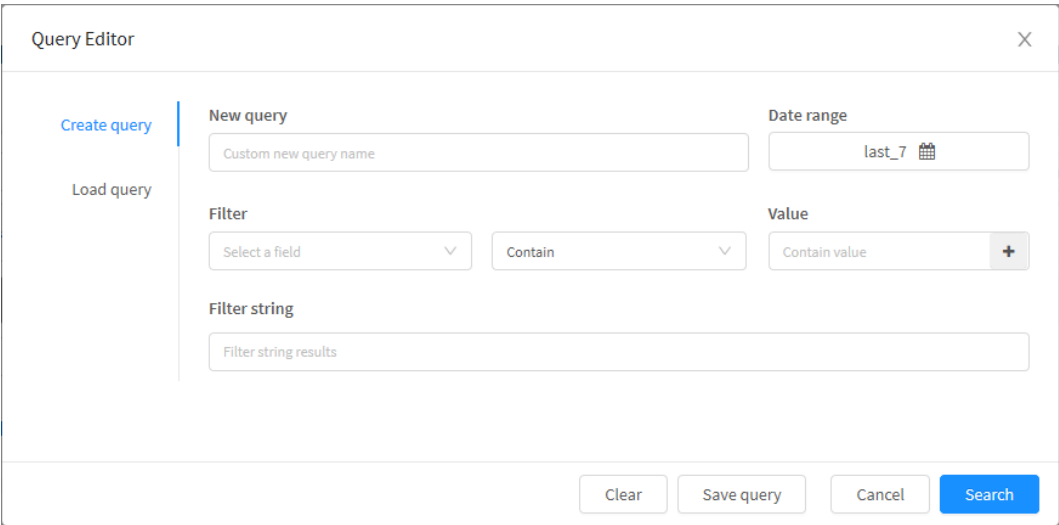
The screenshot shows the 'Query Editor' window with the 'Create query' tab selected. The interface includes a sidebar with 'Create query' and 'Load query' options. The main area contains fields for 'New query' (with a placeholder 'Custom new query name'), 'Date range' (set to 'last\_7' with a calendar icon), 'Filter' (a dropdown menu showing 'Select a field'), 'Value' (a dropdown menu showing 'Contain' and a '+' button), and 'Filter string' (a text input field with 'Filter string results'). At the bottom, there are buttons for 'Clear', 'Save query', 'Cancel', and 'Search'.

Events - Query Editor

Next we will analyze each field in this window:

## Events - Query Editor - Create query

In the "Create query" tab it is possible to configure how the query will act:



This screenshot is identical to the one above, showing the 'Query Editor' window with the 'Create query' tab selected. It displays the same fields and buttons: 'New query' (Custom new query name), 'Date range' (last\_7), 'Filter' (Select a field), 'Value' (Contain), 'Filter string' (Filter string results), and bottom buttons (Clear, Save query, Cancel, Search).


Events - Query Editor - Create query

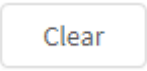
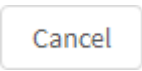
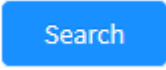
- **New query:** Determines what the query name will be. *Ex.: Last 7 days;*
- **Date range:** Allows you to determine a period to filter results more accurately, possible options are:
  - **By date:** Determines a specific date;
  - **By period:** Displays results from a start date ("Start date") to an end date ("End date");

- **Today:** Displays results specifically for today's date;
- **Yesterday:** Displays results specifically for yesterday;
- **Last 7 days:** Specifically filters the results of the last 7 days;
- **Last 30 days:** Specifically filters results from the last 30 days;
- **This month:** Displays the results for this month;
- **Last month:** Displays the results for the last month.



For more information, regarding the filters shown in the filter selection box, check this [page](#) of the GSM manual.

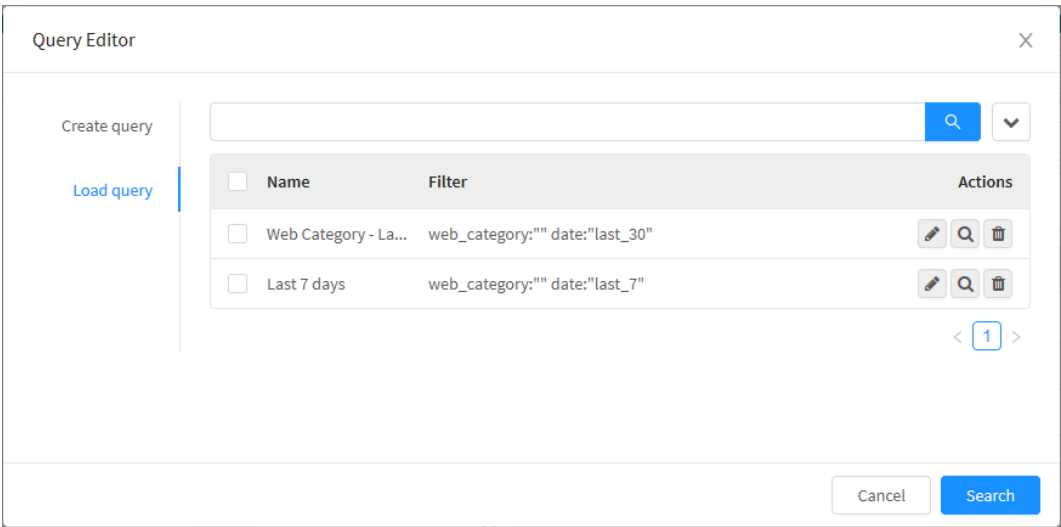
- **Filter:** This check box allows you to select the type of filter used by the query. For more information about filters, check this [page](#).
- **logtype:** Selects the log by its type, the available options for this filter are: webfilter, firewall, dpi, ips, atp;
- **src:** Makes the selection by the origin IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 172.16.12.171;
- **dst:** Makes the selection by the destination IP, this filter accepts IPv4 or IPv6 addresses as value. Ex.: 172.16.12.171;
- **sport:** This filter enables the selection by an origin port, ports are accepted as value. Ex.: 1 to 65535;
- **dport:** This filter enables the selection by a destination port, therefore, ports are accepted as value. Ex.: 1 to 65535;
- **protocol:** This filter allows the selection by protocol, the available options are: tcp, udp, icmp, ip;
- **service:** In this case, the selection is made by service, the accepted values are based on the IANA's table, for more information consult this [page](#);
- **devin:** By making the selection by the entry device, this filter accepts interfaces, in order to learn how to create them, click [here](#);
- **devout:** In this filter the selection is made by the output device, the accepted values are user-created interfaces, for more information on how to create them, check this [page](#);
- **zonein:** This filter enables the selection by the entry zone, the accepted values are zones configured in the UTM's interfaces. Ex.: LAN, WAN, DMZ, etc. For more, click [here](#);
- **zoneout:** This filter makes the selection by output zone possible, the accepted values are the zones that can be configured in the UTM's interfaces. Ex.: LAN, WAN, DMZ, etc. For more information click here [página](#).
- **client\_mac:** This one makes the selection by MAC address, so it accepts physical addresses. Ex.: 94:e6:f7:58:5d:db;
- **client\_user:** This filter makes the selection by user, it accepts e-mails as values. Ex.: [user@blockbit.com](#);
- **client\_ip:** This filter makes the selection by the client's IP, the accepted values are IPv4 and IPv6 addresses. Ex.: 172.16.9.153;
- **geoip\_src:** In this case the selection is made by the GeoIP's origin (IP address Geolocation), the accepted values are each country's abbreviation. Ex.: BR, US, CA, CN, etc;
- **geoip\_dst:** Makes the selection by the GeoIP's destination (IP address Geolocation), the accepted values are each country's abbreviation. Ex.: BR, US, CA, CN, etc;
- **rule\_name:** This filter makes the selection by the rule name, hence the name of the rules created in the UTM are used as value, for more information, click [here](#);
- **rule\_action:** Makes the selection based on the action that the rule takes, this filter accepts the following options as value: *Allow*, *Alert* or *Deny*. Ex.: *Deny*;
- **web\_category:** This filter enables the selection by web category, and accepts them as value. Ex.: Information Technology, Web Mail, Personal Network Storage and Backup, etc.
- **web\_site:** Makes the selection by sites, this filter accepts URLs as value. Ex.: <https://www.blockbit.com>;
- **web\_method:** Makes the selection by the HTTP methods, this filter accepts as value the POST and GET methods. Ex.: POST.
- **web\_mime:** This filter allows the selection by MIME-Type, and also using this parameter as value. Ex.: "application/octet-stream",
- **ips\_profile:** This one makes the selection by the Intrusion Prevention profile system, the accepted value is the profile name, for more on this, click [here](#);
- **app\_name:** This filter makes it possible to select by the application name. Ex.: Google APIs;
- **app\_category:** Makes the selection by the application's category, which is also used as value. Ex.: web;
- **malware\_file:** Makes the selection by the type of *malware* file;
- **malware\_md5:** Selects by the malware's MD5;
- **malware\_status:** Selection by the malware's status;
- **malware\_name:** Selection by the *malware*'s name;
- **threat\_class:** This filter makes the selection by the threat's class. Ex.: Potentially Bad Traffic;
- **threat\_category:** Makes the selection by the threat's category. Ex.: USER\_AGENTS;
- **threat\_sid:** Selects by the threat's SID, this filter uses the threat's SID as value. Ex.: 2027916;
- **threat\_name:** This filter makes the selection by the threat's name. Ex.: Poison Null Byte;
- **threat\_impact:** In this case, the selection is made based on the threat's impact. Ex.: High, Medium, Low;
- **threat\_dump:** Selects by the threat's dump. This filter accepts the threat's dump as value.
- **threat\_payload:** Makes the selection by the threat's payload;
- **flow:** Shows the NAT that has been applied and which was the assigned address, alongside the IP address.
- **Contain/Not Contain:** This checkbox basically acts as a logical query filter operator;
  - **Contain:** It will display all results that contain the value of the next checkbox;
  - **Not Contain:** It will display all results that do NOT contain the value of the next checkbox.
- **Value:** This box determines the value that will be used to filter the query;
- **Filter string:** After editing the previous fields, click on [  ] to display the string used by the search in this text box. You can manually edit this line of code.

To clear the configured query, click the  button. If you want to cancel click on the  button. To perform a search using the query click on the  button.





To save the query, click the  button.

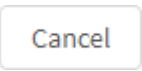
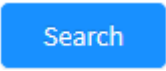
## Events - Query Editor - Load query

In the "Query Editor" tab it is possible to manage saved queries, this panel is composed of a search bar and an action button with the function of deleting all the selected fields, next we will analyze each component of this panel:



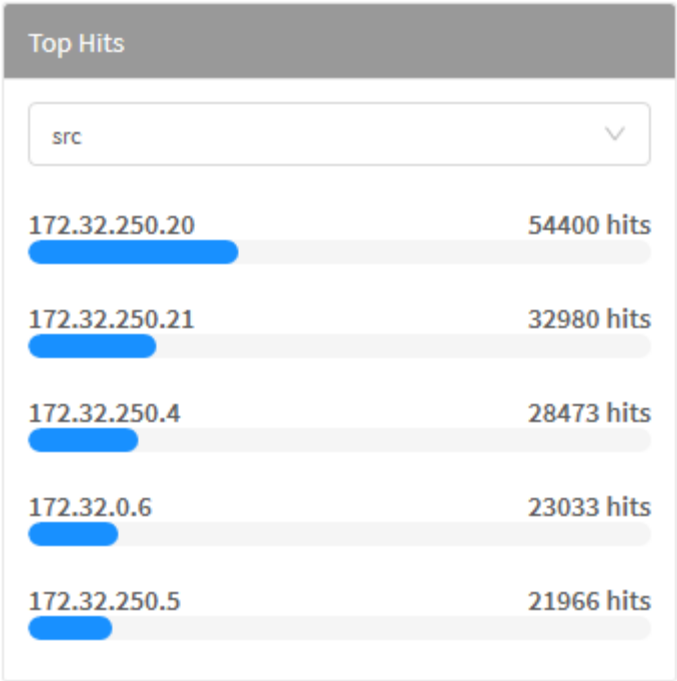
Events - Query Editor - Load Query

- **Select** : Allows you to select the desired query;
- **Name**: Displays the query name;
- **Filter**: Displays the string used by the search;
- **Actions**: Displays a set of contextual buttons;
  - **Edit** : Edit the query settings;
  - **Search** : Performs a search using the query;
  - **Delete** : Remove the query.

If you want to cancel click on the  button. To perform a search using the selected query, click the  button.

# Events - Top Hits

In "Top Hits" we have a selection box composed of several options, when selecting any of them, a graph is displayed further separating the selected option and showing the 5 largest items divided by the amount of accesses related to the selected option, as shown below:



Events - Top hits

The available options are:


Top hits checkbox options

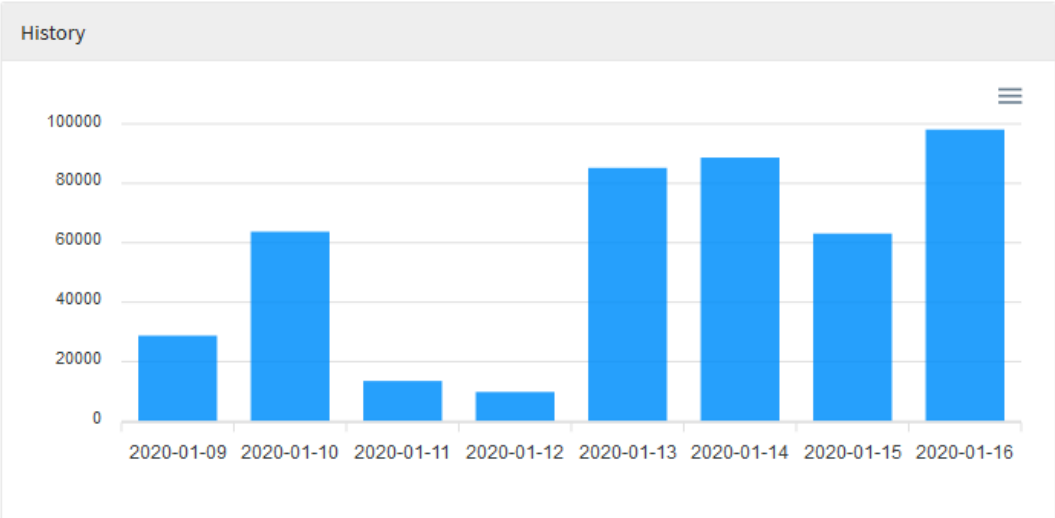
Selection	Detailing
app_category	Most used app categories.
app_name	Names of the most used applications.
client_ip	IPs of customers with the highest number of accesses.
client_user	Users with the highest number of accesses.
client_mac	MAC address with the highest number of accesses.
dport	Numbers of the most active destination ports and the amount of access to each one.
dst	Destination port with the highest number of accesses.
devin	Input device with greater number of accesses.
devout	Output device with greater number of accesses.
geoip_dst	GeoIP destinations with the highest number of accesses.
geoip_src	The origins of GeoIP with the highest number of accesses.
logtype	Log types most generated according to the highest number of accesses.
malware_file	Type of the most detected malware files according to the highest number of hits.
malware_name	Name of the most detected malware according to the highest number of accesses.
malware_md5	MD5 of the most detected malware according to the highest number of hits.

<b>malware_status</b>	The status of the most detected malware according to the highest number of accesses.
<b>protocol</b>	The protocols with the highest number of accesses.
<b>rule_name</b>	The name of the rules with the most accesses.
<b>service</b>	The services with the highest number of accesses.
<b>sport</b>	The source port with the highest number of accesses.
<b>src</b>	The source IPs with the highest number of accesses.
<b>threat_impact</b>	The impact of threats according to the highest number of hits.
<b>threat_sid</b>	The SID with the highest number of accesses.
<b>threat_dump</b>	O <i>dump</i> das ameaças com maior número de acessos.
<b>threat_name</b>	The name of the threats with the most hits.
<b>threat_classification</b>	The rankings of the threats with the highest number of hits.
<b>threat_category</b>	The categories of threats with the highest number of hits.
<b>web_category</b>	The web categories with the highest number of accesses.
<b>web_mime</b>	The MIME-Types with the highest number of accesses.
<b>web_browser</b>	The browsers with the highest number of accesses.
<b>web_site</b>	The sites with the highest number of hits.
<b>web_method</b>	The HTTP methods with the highest number of accesses.
<b>zonein</b>	Entrance zones with the highest number of accesses.
<b>zoneout</b>	Exit zones with the highest number of accesses.

# Events - History

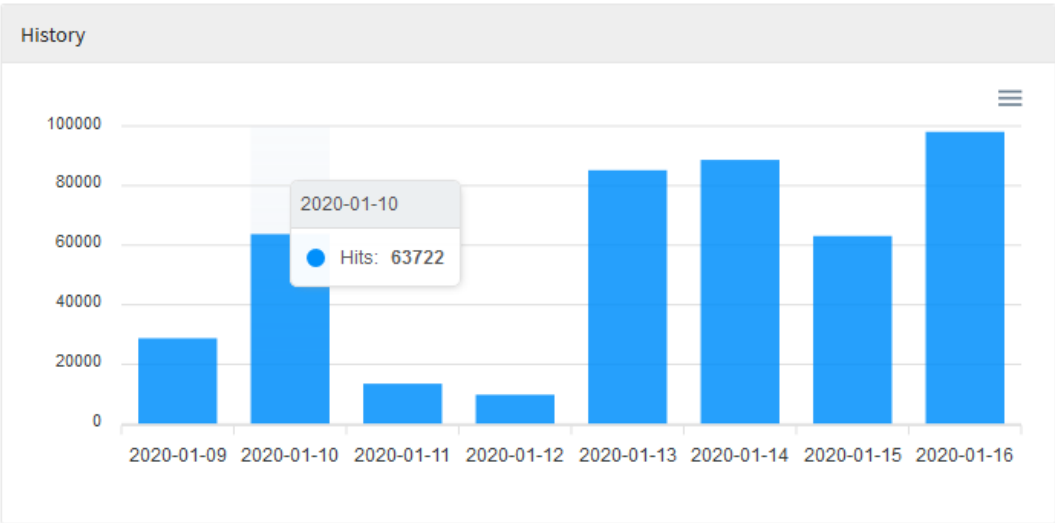
In this panel we have a graph of vertical columns showing the total history of accesses by date, the vertical axis of the graph displays the average of accesses and in the horizontal one the days when they happened.

 The History graph, does NOT represent the Top Hits, but the total access history.




Events - History

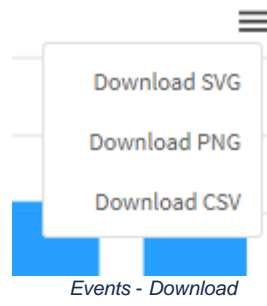
When hovering the mouse over the graph, the exact value of the accesses represented by the selected column is displayed.



Events - History - Exact value of accesses

By clicking on the [  ] button menu, you can download this diagram in svg, png or csv format.





# Events - Log Events


Finally, in “Log Events” we have a record of all events detected on the selected device.

Date	User	Source	Destination	Device	Service	Log type	Action
2021-03-09 17:19:32	-	172.31.0.99:64638	192.168.254.253:443	eth0 - eth0	https	firewall	allow
2021-03-09 17:19:32	-	172.31.0.99:64648	192.168.254.253:443	eth0 - eth0	https	firewall	allow
2021-03-09 17:19:36	user@blockbit.com	172.32.250.109:59439	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:26	-	172.32.0.6:35348	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:41	-	172.32.0.6:35350	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:63367	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:11	-	172.32.0.6:35346	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:63271	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:31	user@blockbit.com	172.32.250.109:53354	172.16.13.246:53	eth1 - eth0	domain	firewall	allow
2021-03-09 17:19:56	-	172.32.0.6:35352	172.31.0.100:8080	eth1 - eth0	http-alt	firewall	allow

## Events – Log Events

This panel consists of 4 columns:


- **Date:** We have the exact date and time for this event;
- **Source:** We have the source of this event, an IP address;
- **Destination:** We have the destination of this event, another IP address;
- **Service:** We have the service tied to this event;
- **Log Type:** Determines the type of record for this event;
- **Actions:** Allows access to the [event view](#).

Right next to the event date we have an icon  which, when selected, will expand the selection and display more information about that specific event.

Information					
date 2023-01-31 12:01:54	client_mac 00:0c:29:29:ba:cd	proto tcp	host utmviola23-14	web_url http://ctdl.windowsupdate.com/msdown load/update/v3/static/trusted/en/pinrule sstl.cab?3d9830f1d6545...	web_site http://ctdl.windowsupdate.com/msdown load/update/v3/static/trusted/en
logtype web	dst 192.16.48.200	service http	client_ip 179.30.0.10	web_referer -	
sessid 1A0ADF6C286FE0AB30A2683E7B639F38	dport 80	devout default	web_method GET	web_agent Microsoft-CryptoAPI/10.0	
src 179.30.0.10	devin eth1	rule_action allow	web_profile Ética de Segurança	bytes 0	
sport 55649	zonein LAN	web_mime application/octet-stream	surfing_time 1	web_protocol HTTP	

## Events – Log Events – Expanded

# Events - Log Events - Event View

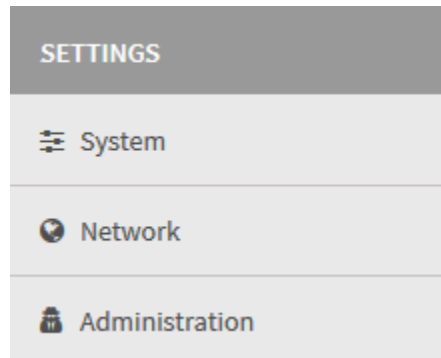
The Event View [  ] displays further details of the event in question, as shown in the image below:



Events - Log Events - Event View

# GSM - SETTINGS

Through the "Settings" menu it is possible to change and verify the administrative, system and network settings.



*Settings menu*

Contains the following options:

- [System](#);
- [Network](#);
- [Administration](#).

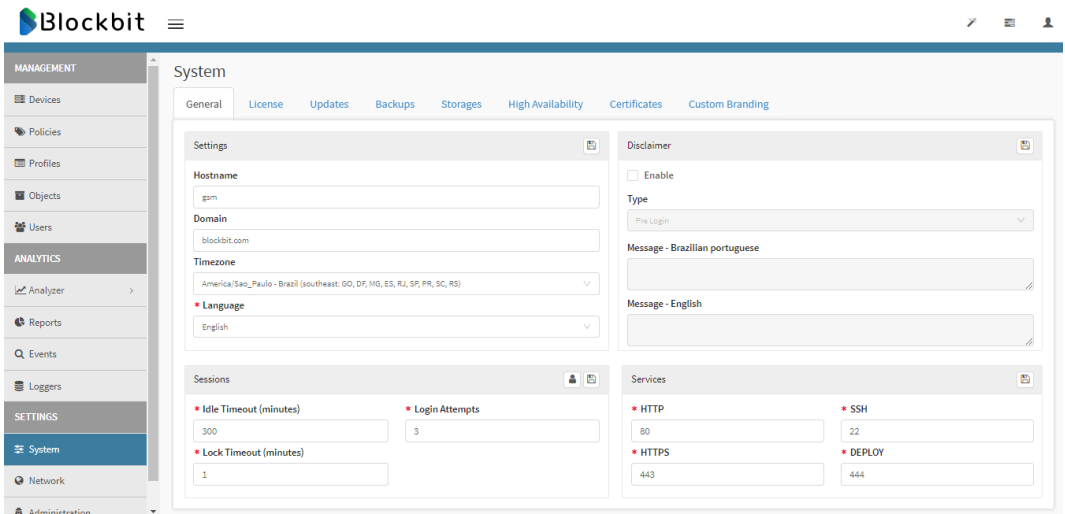
# System

Through the “System” button it is possible to change the system settings.



Settings – System

The System screen will appear with the “General” tab pre-selected, as shown below:



Settings - System - "General" tab

The System screen has the following tabs:

- [General](#);
- [License](#);
- [Update](#);
- [Backups](#);
- [Storages](#);
- [High Availability](#);
- [Certificates](#);
- [Custom Branding](#).

We will describe the features below.

# System - "General" tab

This tab has the main function of making changes to the general settings of Blockbit GSM:

Sistema

Geral Licença Updates Backups Armazenamentos Alta Disponibilidade Certificados

Configurações

Nome do Host  
gsmanual

Domínio  
blockbit.com

Fuso horário  
America/Sao\_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS)

\* Idioma  
Português

Sessões

\* Tempo limite inativo (minutos)  
300

\* Tentativas de Login  
3

\* Timeout do bloqueio (minutos)  
1

Certificados

Certificate Authority  
Certificate Authority

Enabled Authentication

Termo de responsabilidade

☐ Habilitar

Tipo  
Pre Login

Mensagem - Português Brasileiro

Mensagem - Inglês

Mensagem - Espanhol

Serviços

\* HTTP  
80

\* SSH  
22

\* HTTPS  
443

\* DEPLOY  
444

System Settings – General

It consists of the panels:

- [Settings](#);
- [Login Disclaimer](#);
- [Sessions](#);
- [Services](#).

Next, we will analyze each one of them.

## Settings

In the settings panel we can configure the following options:

Settings

Hostname

gsm

Domain

blockbit.com

Timezone

America/Sao\_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS) ▾

\* Language

English ▾

General - Settings

- **Hostname:** The chosen name. It can be anyone as long as it complies with the FQDN - Fully Qualified Domain Name standard. Ex.: GSM;
- **Domain:** Network domain. Ex.: [blockbit.com](http://blockbit.com);
- **Timezone:** Select the time zone in which your business is located. Ex.: America/Sao\_Paulo;
- **Language:** Select the desired language. Ex.: *English*;

After making the desired changes, click on the “Save” button, located in the upper right corner of the screen.



“Save” button

Your changes will have been successfully saved.

Next, we'll review the Disclaimer panel.

## Login Disclaimer

GSM allows you to enable a Disclaimer message that is displayed on the login page of the Administration Interface. It can be configured to appear, when entering the system or after logging in. In this message it is possible to add the company's usage and system compliance policies.

In the Disclaimer panel, we have the following options:

### Disclaimer

☒ **Enable**

**Type**

Pre Login

**\* Message - Brazilian portuguese**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut rhoncus, leo in lacinia sodales, odio augue gravida mauris, sed pretium risus erat cursus nisi. Etiam libero arcu, interdum a aliquet ac, malesuada vitae lorem. Proin at erat pharetra, dignissim enim porta, gravida

**\* Message - English**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut rhoncus, leo in lacinia sodales, odio augue gravida mauris, sed pretium risus erat cursus nisi. Etiam libero arcu, interdum a aliquet ac, malesuada vitae lorem. Proin at erat pharetra, dignissim enim porta, gravida

General - Disclaimer

- **Enable:** By checking this checkbox the display of the disclaimer will be enabled;
- **Type:** Defines how the message will be displayed. Being able to select from the following options:
  - **Pre Login:** The Disclaimer message will be displayed as soon as you access the system, before logging in. *If the system detects the language pack "portuguese" installed in the browser, the displayed Disclaimer will be the one written in the Message - Brazilian portuguese field, otherwise, by default the disclaimer registered in Message - English will be used;*
  - **Post Login:** The Disclaimer message will be displayed to the user after logging in.
- **Message - Brazilian portuguese:** In this field it is possible to write the message that will be displayed if the selected language is Portuguese;
- **Message - English:** In this field it is possible to write the message that will be displayed if the selected language is English.



The Message - Brazilian portuguese and Message - English fields accept only plain (pure) text, it is not possible to use formatting.

After making the desired changes, click on the "Save" button, located in the upper right corner of the screen.



"Save" button

Your changes will have been successfully saved.

The Disclaimer message will be displayed as configured, an example follows:



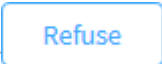
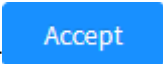
Login Disclaimer

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras vel placerat ipsum, sit amet sollicitudin tellus. Fusce feugiat vehicula lectus sit amet hendrerit. Proin et arcu ut quam molestie maximus. Phasellus ut feugiat justo. Morbi elementum vitae diam non aliquam. Etiam ut ultrices dui. Sed varius, urna in commodo facilisis, magna massa volutpat quam, id interdum lorem lacus id augue. Fusce ipsum lorem, malesuada eu nulla convallis, vestibulum finibus nibh. Nullam id urna sit amet justo pretium scelerisque et commodo ante. Aliquam velit metus, convallis tempor quam at, viverra convallis metus. Curabitur sollicitudin ipsum elit, ac congue tellus consectetur at. Fusce tincidunt leo non tincidunt pellentesque.

Refuse

Accept

Login Disclaimer

If the user clicks the  button he will not be able to access the system. However, when you click  it will access normally.



This concludes the customization of the Disclaimer message.

## Sessions

In this screen it is possible to configure authentication parameters and view the session of the administrators logged into the Blockbit GSM, in addition to ending their sessions.

- To configure the authentication parameters, just change the fields with the desired values:

Sessions

\* Idle Timeout (minutes)

300

\* Login Attempts

3


\* Lock Timeout (minutes)

1

System Settings – Sessions



- **Idle timeout:** Idle time before the session expires, the value is in minutes. Ex.: 30;
- **Login attempts:** Number of maximum failed Login attempts before blocking access, the value is in minutes. Ex.: 3;
- **Lock timeout:** Time that the user will be blocked when making the maximum number of wrong attempts at login, the value is in minutes. Ex.: 3.




Click **save** [  ] located in the upper right corner of the screen to save the changes made to the settings.




2. To view the active sessions of the logged in administrators, click on the **Active Sessions** [  ] button located in the upper right corner of the screen:

Active Sessions <span>×</span>				
Start	Name	Address	Status	Action
2019-10-04 13:19:14	admin	172.16.100.144	✓	
2019-10-04 14:18:34	admin	172.16.100.144	✓	
				<button>Close</button>


Active sessions

- **Start:** Date and time the administrator logged in or logged into the BLOCKBIT GSM. Ex.: 2017-04-21 19:42:42;
- **Name:** Admin name. Ex.: admin;
- **Address:** Administrator IP address. Ex.: 192.168.111.14;
- **Status:** Login status. Ex.: *Active*;
- **Action:** Allows you to remove the administrator session. By clicking on the **Remove** [  ] button, the administrator will be removed from the session and the login screen will be displayed to whoever has been removed.



Click the [  ] button to close the screen.



Click **save** [  ] located in the upper right corner of the screen to save the changes made to the settings.

Next, let's look at the Services panel.

## Services

In this screen it is possible to change the communication and administration ports of the Blockbit GSM:



If the ports are changed on Blockbit GSM, they must also be changed on other managed Blockbit devices.



If the HTTP and / or HTTPS ports are changed, access to the Web Interface must be done with the new configured ports.

Services

\* HTTP

80

\* SSH

22

\* HTTPS

443


\* DEPLOY

444

System Settings – Services

- **HTTP:** Blockbit GSM Web Interface access port. Ex.: 80;
- **HTTPS:** Blockbit GSM Web Interface access port. Ex.: 443;
- **SSH:** Access port to the CLI console of Blockbit GSM and communication with managed devices. Ex.: 22;
- **DEPLOY:** Communication port with managed devices. Ex.: 444.



Click **save** [  ] located in the upper right corner of the screen to save the changes made to the settings.

## Certificates

In this panel, you can enable the use of certificates to access the administration interface.

After enabling, select the accessing host digital certificate or the C.A. “Certificate Authority” and C.S. “Certificate Service”.

Certificates

Certificate Authority


Select ▼

Service Certificate

Select ▼

☐ Enabled Authentication

Settings - Administration - Certificates

- **Enabled Authentication** : Enables access by authentication through X.509 v3 certificate.



Click on **save** in the upper right corner to save any change.

Next, we will analyze the contents of the [License](#) tab.

# System - "License" tab

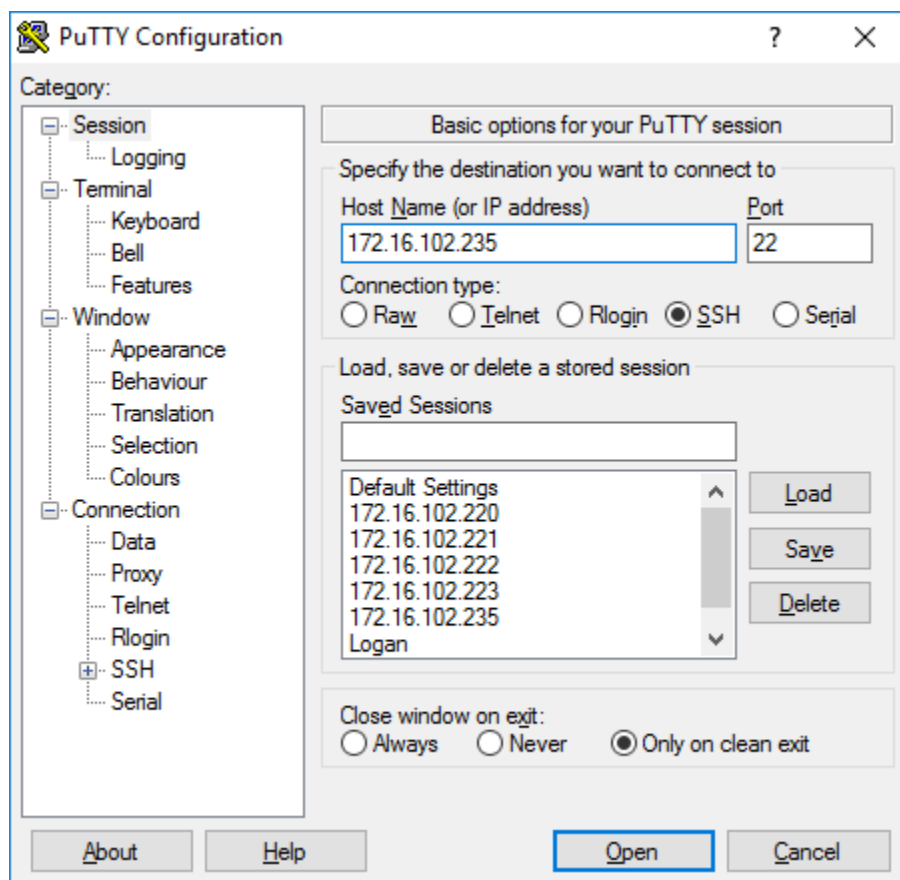
In this screen it is possible to apply or renew the activation license of Blockbit GSM. To carry out the licensing, it is necessary to provide the UUID (Blockbit GSM Universal Unique Indicator) for your service channel, which will provide you with the license number.



Before licensing, check if the Blockbit GSM is connected to the internet.

In the following, we will introduce you step by step to license your Blockbit GSM:

1. Check that the access device has a recommended SSH client already installed. Let's exemplify the process using the "PUTTY" application;
2. Access the SSH console. Fill in the fields:
  - **Host Name (or IP Address):** Enter the IP address of the Blockbit GSM. Ex.: 172.16.102.235;



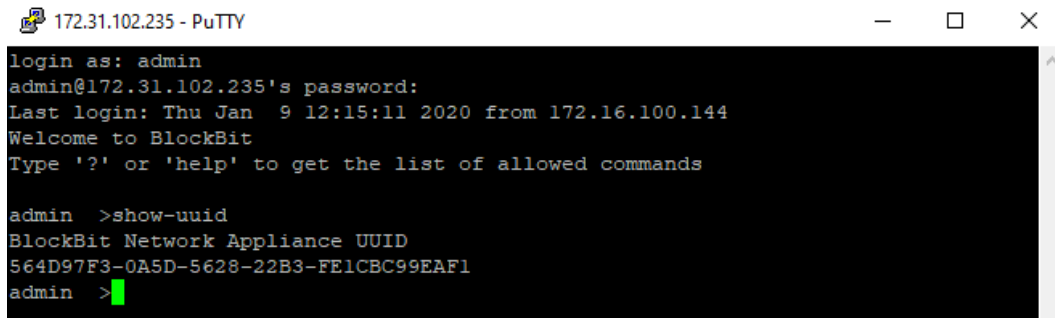
Licensing - PuTTY

- Click on the "Open" button.

3. The console will be displayed prompting for username and password;

In "login as:" type the user "admin" and press "Enter".  
After "password:" enter the password "admin" and press "Enter".

4. Run the show-uuid command;



```
172.31.102.235 - PuTTY
login as: admin
admin@172.31.102.235's password:
Last login: Thu Jan  9 12:15:11 2020 from 172.16.100.144
Welcome to BlockBit
Type '?' or 'help' to get the list of allowed commands

admin >show-uuid
BlockBit Network Appliance UUID
564D97F3-0A5D-5628-22B3-FE1CBC99EAF1
admin >
```

Comando *show-uuid*

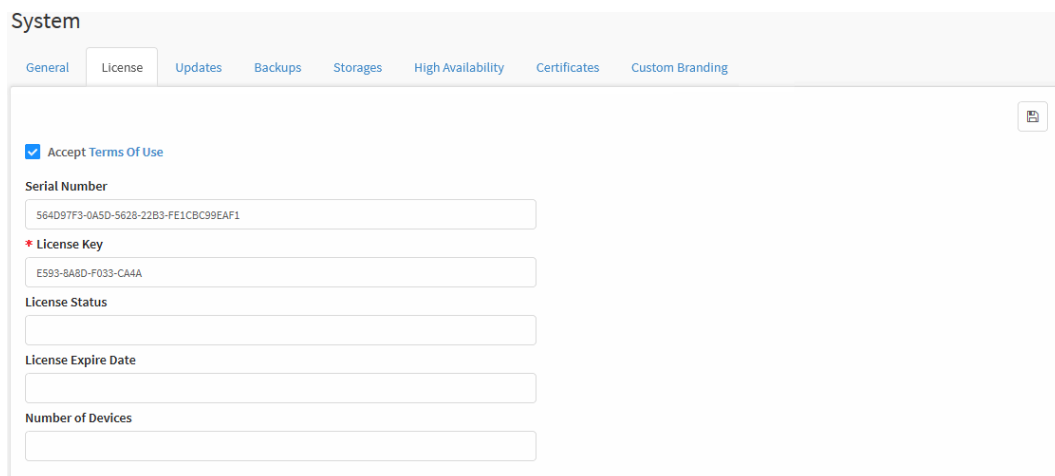
5. Send the code "Blockbit Network Appliance UUID" to your Blockbit customer service channel for the license release. Ex.: 564D97F3-0A5D-5628-22B3-FE1CBC99EAF1;

6. You will receive the License number code, from your service channel. Ex.: 8FD0-D18D-DA6C-D70C;

7. Return to the Blockbit GSM Web Interface on the License screen;

8. Make sure the "Accept Terms of Use" checkbox is checked, if unchecked, click to select it;

9. In the text box "License Key" enter your license number, as shown in the image below;



System

General License Updates Backups Storages High Availability Certificates Custom Branding

☒ Accept Terms Of Use

Serial Number  
564D97F3-0A5D-5628-22B3-FE1CBC99EAF1

\* License Key  
E593-BA8D-F033-CA4A


License Status  
[Empty field]

License Expire Date  
[Empty field]

Number of Devices  
[Empty field]

License key

10. After making the desired changes, click on the [  ] button, located in the upper right corner of the screen;

 Settings successfully changed!

*Settings successfully changed!*

11. The information on the screen will be updated and will display the following information: "Serial Number", "License Key", "License Status", "License Expiration Date" and "Number of Devices", however, with their data representing the current state of the system.

System

General

License

Updates

Backups

Storages

High Availability

Certificates

Custom Branding

☒ Accept Terms Of Use

Serial Number

S64D97F3-0A5D-562B-22B3-FE1CBC99EAF1

\* License Key

8FD0-D18D-DA6C-D70C

License Status

true

License Expire Date

3000-12-31

Number of Devices

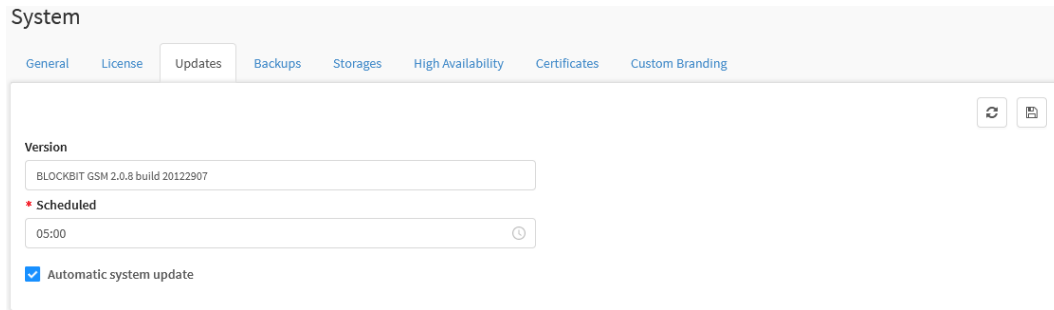
0

*System Settings – License*

*Next, we will analyze the content of the [Update](#) tab.*

# System - "Updates" tab

This screen has the function of updating your GSM. This panel consists of three options: "Version", "Scheduled" and "Automatic System Update".




System Settings – Updates


- **Version:** Displays the current version and build of your Blockbit GSM. Ex.: *Blockbit* GSM 1.3.0 build 19092518;
- **Scheduled:** By clicking on the text box a menu will appear, it is possible to change the scheduled time to execute the desired update, for that just click on the arrows to change the hours and minutes, done that, click outside the menu in order to finish the selection. Ex.: 14:41;
- **Automatic System Update:** This check box allows the automatic system update to be performed. If it is selected, the update will take place at the time scheduled in the option above "Scheduled".

1. In the upper right corner of the screen it is possible to find two contextual buttons: "Update Now" and the "Save" button (whose function is self-explanatory);



2. When clicking on the **update now** [  ] button, the system will be updated immediately instead of waiting for the schedule mentioned in "scheduled".




Click **save**[  ] located in the upper right corner of the screen to save the changes made to the settings.


Next, we will analyze the contents of the [Backups](#) tab.

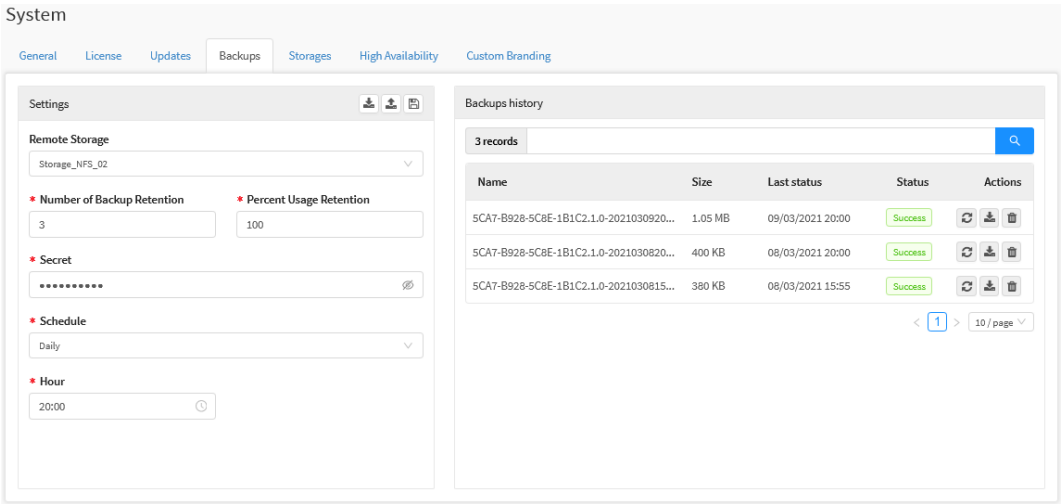


# System - "Backups" tab

Through the options available on this tab, the administrator can configure an automatic backup routine of the system settings, in addition, it is possible to view a record of the status of the implementation of the backups in the right panel with the possibility of performing a new implementation, downloading the backup file, remove or interrupt a backup being performed.

 For more information on how to configure backup on UTM's administered by GSM, see this [page](#).  
If you want to know more about creating storage devices, see this [page](#).

 It is possible to consult the logs with more information regarding the backup procedure using the [\[debug-backup\]](#) command.



System - Backups

This tab is composed of the panels:

- [Settings](#);
- [Backups History](#).

Next, we'll look at each one starting with the [Settings](#) panel.

# System - Backups - Settings

In this panel it is possible to configure the automatic backup service, guaranteeing a complete copy of the system and guaranteeing its restoration in a much faster and more efficient way, for this it is necessary to define the storage location, which must be previously registered in [Storages](#).



When making a backup, GSM creates a complete "image" of the system, the generated file will have the extension ".conf" and will be included in it:

- The Operating System;
- The configuration database.

Next, we will analyze the content of this panel:

*Backups - Settings*

- **Remote Storage:** Defines the location where the backups will be stored. The items that appear in this box are created in the [Storages](#) tab. Ex.: *Storage\_NFS\_02*;
- **Number of Backup Retention:** Determines how many backups will be stored in the directory. At the end of this limit, the oldest backup is deleted. For example, if you choose "3", only the last 3 backups will be kept, so when a new backup is generated the routine will be executed to delete the oldest one, always respecting the value added in this field. Ex.: 3;
- **Percent usage retention:** Defines the percentage of usage that the directory created within the storage will use when saving the backup. If the limit is reached, backup rotation is performed, removing the oldest one in order to always keep the most recent backups. If a directory has 1000 GB and 30% retention is chosen, when the records occupy 30 GB the rotation will be activated, otherwise the retention number will be verified. Ex.: 100%;



The system acts first by checking if the usage percentage has been reached and then checking the number of backups retained. Consequently:

1. If you still have free space, the system will check the number of backups retained.
2. If the maximum retention amount has not been reached, the backup storage will continue to function normally without deleting previous records.

Analyzing the opposite scenario, the performance of the system will be as explained below:


1. If the space limit is reached, rotation will be activated to keep only the most recent backups;
2. If disk space still exists, but the number of backups retained exceeds the limit set by the administrator, the oldest records will be removed, respecting the value defined in the field, so that the directory always has the most recent backups.



If the administrator does not want the percentage to be considered, simply add the value "100" so that the space is fully used before activating the rotation. In this way, only the number of backups retained will be considered.

- **Secret:** Insert the secure key, it must contain at least eight characters with uppercase and lowercase letters, numbers and special characters. Without this key, it is not possible to restore the backup. Ex.: q1Q!q1Q!;
- **Schedule:** Defines the period that the system backup will be performed, it can be:
  - **Disabled:** Disables automatic backup;
  - **Daily:** Defines that the backup will be performed daily;
  - **Weekly:** Defines that the backup will be performed weekly;
  - **Monthly:** Defines that the backup will be performed monthly.
- **Hour:** Defines the time to be backed up. Ex.: 20:00;



You can still download a backup file by clicking the [  ] button located at the top of the panel.

System Backup

X

\* Key

\* Confirm Key

Cancel


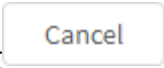
Save

Backups - System Backup


- **Key:** Register a secure key for the backup file. Ex.: q1Q!q1Q!;
- **Confirm Key:** Confirm the key by typing it again.

Save

Cancel

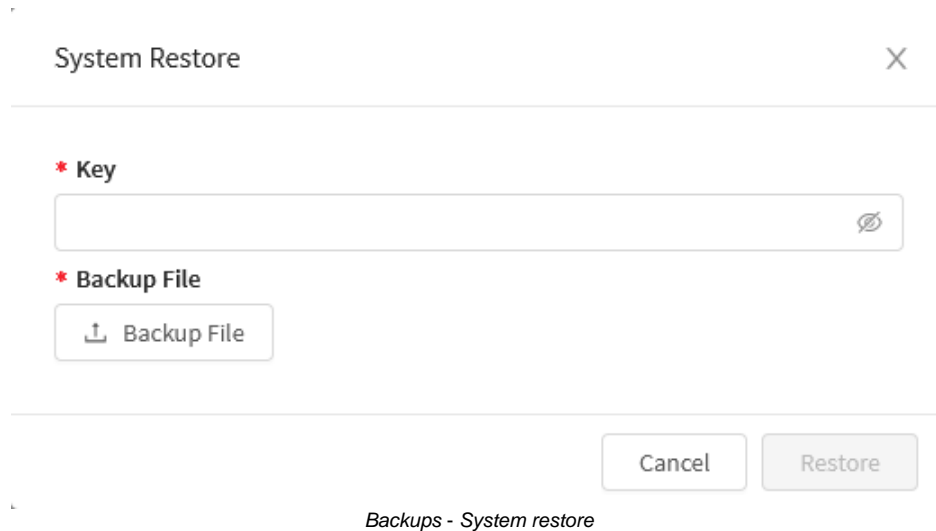
Click [  ] to save and download the backup file or [  ] to close this window.





To restore a backup file from Manager, just click on [  ], the window below will be displayed:





If the environment is in H.A., it is recommended to restore the Backup Manager through the IP of the physical interface and not the virtual IP.



- **Key:** Enter the key that was added when creating the backup file;
- **Backup File:** Select the backup file to be restored.

Click [  ] to restore the backup file or [  ] to close this window.










Finally, to save the backup settings for this panel, click the [  ] button.

 **Backup saved successfully**  
*Backup saved successfully*






Next, we will analyze the [Backups History](#) panel.

# System - Backups - Backups History

In this area the system registers in a list the implementation of the backups configured in the [Settings](#) panel, with the possibility of performing some actions such as reimplementation of completed backup routines, download of the backup file, removal of backups, etc. Next, we will analyze the features of this panel:



Backups history				
3 records <span>🔍</span>				
Name	Size	Last status	Status	Actions
5CA7-B928-5C8E-1B1C2.1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030820...	400 KB	08/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030815...	380 KB	08/03/2021 15:55	Success	  
< 1 > 10 / page ▾				

## Backups - Backups

- **Name:** Backup identification, shows the name of the snapshot taken. Ex.: 4B4F-BB06-3B2D-D3BB-UTM-2.0.4-140820.snap;
- **Size:** Displays the size of the backup file. Ex.: 1.05 MB
- **Date:** In this column, displays the system date and time at the time of the backup;
- **Status:** Displays the current status of the Backup routine execution, which can be:
  -  **Running**: The backup routine is currently running;
  -  **Error**: Something went wrong that caused the backup routine to fail;
  -  **Waiting**: Routine is in waiting time. This can occur when the system detects a process that may interfere with the backup that is currently running (for example, another backup routine);
  -  **Success**: The backup was successful.
- **Actions:** The "Actions" menu consists of buttons:
  -  **Restore**: This button is used to perform the backup procedure on the Device again. For that, it is necessary to add the key created in the Secret field in the [Settings](#) panel. If a backup is removed from the directory, it will remain recorded in the history, but this option will be disabled;



If the environment is in H.A., it is recommended to restore the Backup Manager through the IP of the physical interface and not the virtual IP.

-  **Download**: This button is not displayed if the backup type is "System". By clicking on it, you can download the snapshot.
-  **Delete**: When you click this button, the backup is removed from the history.

For more information on backups, see this [page](#).

Next we will analyze the *Storages* tab.

# Example - Backup Manager

This section will present the step-by-step for configuring Manager Backups.



For more information on Backups, see this [page](#).

The steps we will take in this demonstration will be:


- [Inclusion of Storage](#);
- [Backup Routine Creation](#);
- [Settings Validation](#).

We will start the demo by configuring a [Storage](#).

# Example - Backup Manager - Inclusion of Storage

After [adding the devices](#), in this step we will perform the following steps:

- [Object Creation](#);
- [Storage configuration](#);

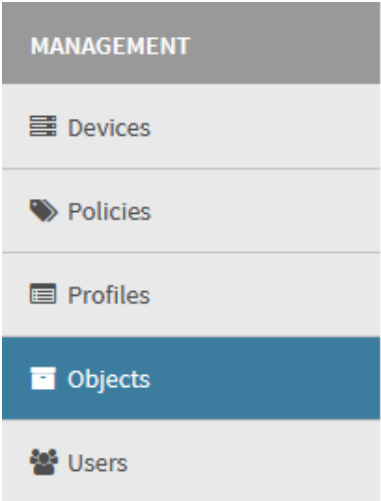


This example will assume that the storage that will be used by the administrator is installed and configured correctly. For more information about Blockbit GSM compatibility with remote storage see this [page](#).

Initially we will generate the IPs that will be used by the Storages.

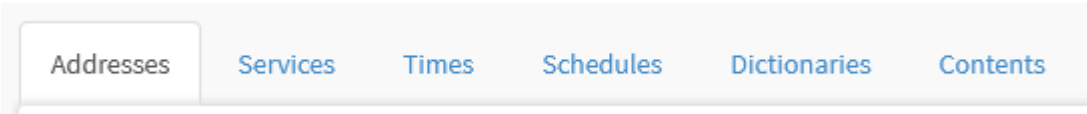
## Object Creation

First we will create the single IP objects that will be used to connect to the Remote Storage, so access the Management menu and click on the Objects option:



Management - Objects

Click on the Addresses tab:



Addresses tab

Click on the **Actions Menu** [] icon and select the “Create Object” option;



Inventory - Create Device

We will add the IP object "Storage\_NFS\_02", complete the form as shown below:

Create Addresses Object

X

\* Name

Storage\_NFS\_02

\* Type

IPv4 Address

Unique

\* Address

Mask

172.31.160.30

255.255.255.255

+

-

Description

Cancel

Import Address

Save

Adresses Object - Create Adresses Object

- **Name:** We will use the name "Storage\_NFS\_02";
- **Type:** Select the "IPv4 Address" option;
- **Unique** ☒: This will be an object of a unique type, so be sure to check this checkbox;
- **Address:** The Storage address is "172.31.160.30";
- **Mask:** The mask can remain the default;
- **Description:** In this example, we will not add a description.

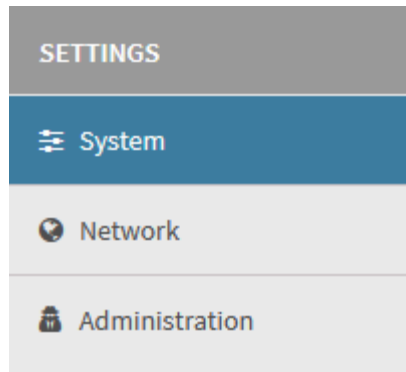
Save

Click [ ] to save the settings.

After creating the address objects, we will create the Storages.

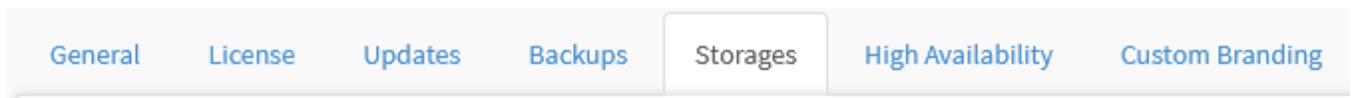
## Configuration of Storages

Access the Settings menu and click on the option System:



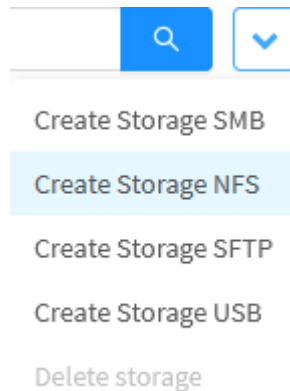
Settings - System

Access the Storages tab:



Storages tab

Click on the **Actions Menu** [ ] icon and select the "Create Storage NFS" option;



Storages - Create Storages NFS

We will add Storage\_NFS\_02, complete the form as shown below:

Create Storage NFS

X

\* Description

Storage\_NFS\_02

\* IP

Storage\_NFS\_02

\* Directory

/bkp-blockbit-nfs/user/nfs-200.30

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

☐ Protocol TCP

☐ Disable locking

☐ Enable posix

Operation Mode

☒ Hard ☐ Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

☐ Only Logger

Cancel


Save

Storages - Create Storage NFS

In this window we will just configure the following fields:

- **Description:** In this example we will name the storage "Storage\_NFS\_02";
- **IP:** Select the IP address of the NFS server configured in the previous step, in this case we will use the object "Storage\_NFS\_02";
- **Directory:** We will use the "/bkp-blockbit-nfs/user/nfs-200.30" directory.

The other fields can be kept with the default configuration.

Click  to save the settings.

After finishing all the configurations, the storage will have been successfully configured:

System

General

License

Updates

Backups

Storages

High Availability

Custom Branding

4 records

Description

Type

Size

Actions

☐

Storage\_NFS\_01

NFS

52%

☐

Storage\_NFS\_02

NFS

45%

☐

Storage\_SFTP\_02

SFTP

45%

<

1

>

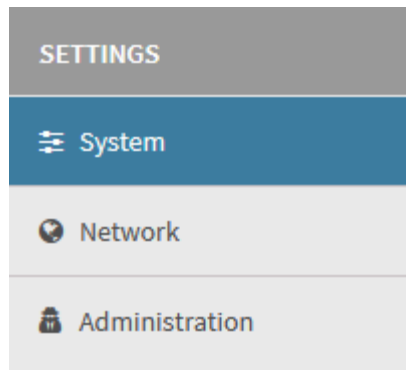
10 / page

System - Storages

In the next step, we will create the [Backups routines](#).

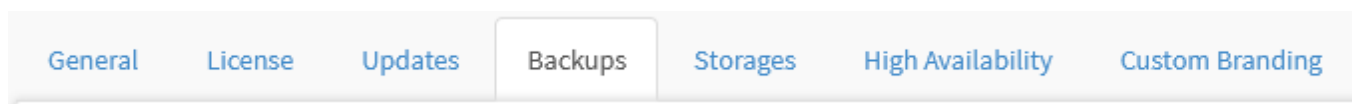
# Example - Backup Manager - Creation of the Backup Routine

After creating the [storage](#), just create the backup routine, initially, access the Settings menu and click on the System option:



*Settings - System*




Click on the "Backups" tab:



System - Backups Tab

We will create a daily backup routine:

Settings

Remote Storage

Storage\_NFS\_02

\* Number of Backup Retention


3

\* Percent Usage Retention

100

\* Secret

.....




\* Schedule

Daily


\* Hour

20:00



Backups - Create Backup

- **Remote Storage:** We will select "Storage\_NFS\_02";
- **Number of Backup Retention:** In this case we will configure so that there is retention of 3 backup;
- **Percent usage retention:** We will use 100% of the directory space, so that there is no limitation;
- **Secret:** Enter the desired secret key;
- **Schedule:** The schedule will be daily, so we will select the option "Daily";
- **Hour:** Finally, select the time when it will be done, in this example, it will be at 20:00.

Click [  ] to save the settings.

When finishing all the configurations, the screen will be as shown below:

System

General

License

Updates

Backups

Storages

High Availability

Custom Branding

Settings

Remote Storage

Storage\_NFS\_02

Number of Backup Retention

3

Percent Usage Retention

100

Secret

\*\*\*\*\*

Schedule
















Daily

Hour

20:00

Backups history

5 records

Name	Size	Last status	Status	Actions
5CA7-B928-5C8E-1B1C2.1.0-2021031120...	1.05 MB	11/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021031020...	1.05 MB	10/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030820...	400 KB	08/03/2021 20:00	Success	  
5CA7-B928-5C8E-1B1C2.1.0-2021030815...	380 KB	08/03/2021 15:55	Success	  

< 1 > 10 / page

Devices - Backups

Finally, we will discuss the [validation](#) of the settings we have made.

# Example - Backup Manager - Configuration Validation

To validate the correct functioning of the backup settings, it is possible to force the manual backup using the *Run System Backup Now*  button.

System Backup

\* Key

.....


\* Confirm Key

.....

Cancel

Save

Backups - System Backups

After adding the secret key, just click  and check the status and progress of the backups in the interface where they were created, an example follows:

System

General

License

Updates

Backups

Storages

High Availability

Custom Branding

Settings

Remote Storage

Storage\_NFS\_02

\* Number of Backup Retention

3

\* Percent Usage Retention

100

\* Secret

.....

\* Schedule

Daily

\* Hour

20:00

Backups history

5 records

Name	Size	Last status	Status	Actions
5CA7-B928-5C8E-1B1C2.1.0-2021031120...	1.05 MB	11/03/2021 20:00	Success	<div></div> <div></div> <div></div>
5CA7-B928-5C8E-1B1C2.1.0-2021031020...	1.05 MB	10/03/2021 20:00	Success	<div></div> <div></div> <div></div>
5CA7-B928-5C8E-1B1C2.1.0-2021030920...	1.05 MB	09/03/2021 20:00	Success	<div></div> <div></div> <div></div>
5CA7-B928-5C8E-1B1C2.1.0-2021030820...	400 KB	08/03/2021 20:00	Success	<div></div> <div></div> <div></div>
5CA7-B928-5C8E-1B1C2.1.0-2021030815...	380 KB	08/03/2021 15:55	Success	<div></div> <div></div> <div></div>


<

1

>

10 / page

Devices - Backups

 For more information on the components of this screen, see this [page](#).

In addition, the operations performed by the backups generate audit logs, as shown in the image below:

772



## Administration

[Administrators](#) [Users Profiles](#) [Auth Servers](#) [Identity Provider](#) [Audit Log](#)

142 records

Date	User	Interface	Activity	IP	Actions
2021-03-10 20:58:57	Administrator	backups	Delete	192.168.200.2	
2021-03-10 20:58:03	Administrator	backups	Edit	192.168.200.2	
2021-03-10 20:16:21	Administrator	device-backups	Edit	192.168.200.2	
2021-03-10 19:12:49	Administrator	device-backups	Save	172.31.200.253	
2021-03-10 18:53:51	Administrator	device-backups	Delete	172.31.200.253	
2021-03-10 18:00:23	Administrator	backups	Edit	172.31.200.253	
2021-03-10 16:10:58	Administrator	device-backups	Edit	192.168.111.85	
2021-03-10 16:01:42	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:13	Administrator	device-backups	Save	192.168.112.21	
2021-03-10 16:01:01	Administrator	device-backups	Save	192.168.112.21	

< 1 2 3 4 5 ... 15 > 10 / page

### Administration - Audit Log

Click on for more information regarding registration:

Audit View ×

```
"Audit Information" : {  
  "settings_system-download-file" : "5CA7-B928-5C8E-1B1C2.1.0-202103121619.conf"  
  "settings_system-download-size" : "1.05 MB"  
}
```

Close

### Devices - Backups - Audit View



For more information on audit reports, see this [page](#).

Finally, during the backup process, it is also possible to check more details in the CLI using the [\[debug-backup\]](#) command.


```
admin >debug-backup  
date="2021-03-12 16:23:02" backup_id="4" device_type="manager" action="backup" storage_name="Storage_NFS_02" storage_type="nfs" backup_type="conf" status="running" status_message="" service="backup_manager"  
date="2021-3-12 16:23" backup_id="4" device_type="manager" action="backup" storage_name="Storage_NFS_02" storage_type="nfs" backup_type="Conf" status="Done" service="backup_manager"
```

### CLI - debug-backup

For more information on device backups, see this [page](#).

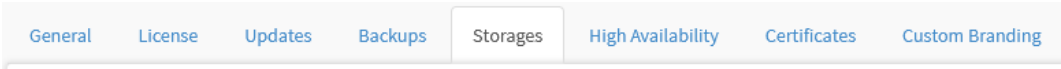
# System - "Storages" tab

In this tab are located the resources that allow the administration of the GSM storage interfaces. This panel allows the administrator to register the storage devices that will be used by the backup services.













The storage devices created in this tab are used mainly in the [backup service of the GSM](#) and in the [backups of UTMs](#) managed by the system.

To access the Storage management interface, click on the "Storages" tab:




Storages tab

The screen will appear, as shown by the image below:

4 records					
<input type="checkbox"/>	Description	Type	Size	Actions	
<input type="checkbox"/>	SFTP Storage	SFTP	<div><div></div></div> 0%		
<input type="checkbox"/>	SMB Storage	SMB	<div><div></div></div> 20%		
<input type="checkbox"/>	USB Storage 1	USB	<div><div></div></div> 99%		
<input type="checkbox"/>	USB Storage 2	USB	<div><div></div></div> 0%		
				< 1 >	10 / page

System - Backup Storages



**ATTENTION:** Regardless of which directory category has been created by the administrator, each GSM needs to have its own directory.

In this section we will expose the types of storage supported by the system and its applications:

- [SMB](#);
- [NFS](#);
- [SFTP](#);
- [USB](#).

This section will demonstrate:

- [Register each type of Storages](#);
- [Delete Storages](#);
- [Column components of this screen](#).


Next, we'll review the [Create Storage](#) button.

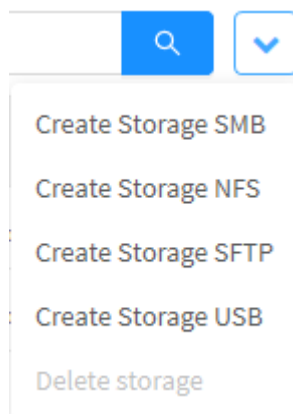
# Storages - Actions Menu

The actions menu contains options for the creation of storage units in GSM, and these will be used in the creation of Backups (check this [page](#) for more information).

And you also have the option to remove them.



Click [  ], the following window will be displayed:



*Storages - Create Storage*


The available options are:

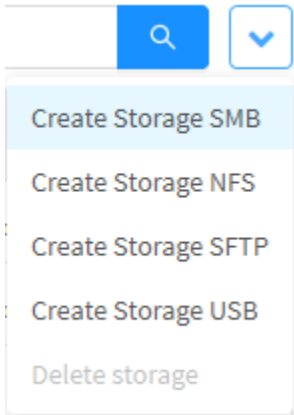
- [Create Storage SMB](#);
- [Create Storage NFS](#);
- [Create Storage SFTP](#);
- [Create Storage USB](#);
- [Delete Storage](#).

Next we will explain each option in this menu.

# Create Storage - SMB

"Server Message Block" storage is commonly used for folder sharing by Windows. This storage model is made available by the system for "Backup / Restore" applications.

To add an SMB storage, click on [  ] and select the "Create Storage SMB" option as shown below:



Create Storage SMB

The window below will appear, configure the form according to the specifications for connection to the respective SMB server:

Create Storage SMB

X

\* Description

\* IP

Select

Login

Password

\* Share

\* Simultaneous transfers

5

☐ Only Logger

Cancel

Save

Storage - Add SMB storage

- **Description:** Storage name. Ex.: *SMB Storage*;
- **IP:** Select the IP address of the file server. This field will display the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage that will be used. Ex.: 172.16.102.52;
- **Login:** File server user. Ex.: blockbit1;
- **Password:** File server user password;
- **Share:** Name of the folder that was shared on the file server. Ex.: *storage*;
- **Simultaneous transfers:** Defines the limit of simultaneous transfers that the System can make using this particular storage. Ex.: 5;
- **Only Logger** ☐: If this check box is enabled, the unit will be used exclusively to store the loggers.




For more information on how to create a single IP Object, see this [page](#).

Save

Cancel


After filling in all fields click [  ] to finish or click [  ] to close the window without making any changes;

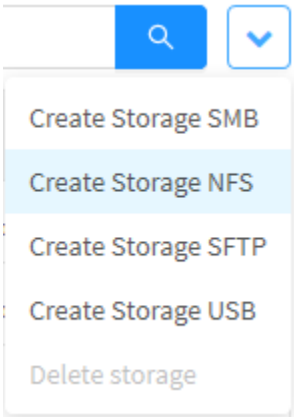
After saving, for the settings to take effect, it will be necessary to access the **command queue** [  ] and apply the changes made. For more information on the command queue access the page: [UTM - Command Queue](#).

Next we'll look at how to create an [NFS](#) storage.

# Create Storage - NFS

The "Network File System" is commonly used to share folders on UNIX servers. This storage model is made available by the system for "Backup / Restore" applications.

To add an NFS storage, click [  ] and select the "Create Storage NFS" option, as shown:



Create Storage NFS

The window below will be displayed, configure the form specifying the fields "Description", "IP" and "Directory" of the NFS server for the storage of the backup / restore feature.

Create Storage NFS

Description

IP

Select

Directory

Reading Bytes

4096

Writing Bytes

4096

Port

2049

Block sizes Bytes

Protocol TCP

Disable locking

Enable posix

Operation Mode

Hard

Soft

Extra Options

opt=n, opt2=m

Simultaneous transfers

5

Only Logger

Cancel

Save

Storage - Add NFS storage

- **Description:** NFS store name. Ex.: NFS Backup;

- **IP:** Select the IP address of the NFS server. This field will display the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage that will be used. Ex.: 172.16.102.53;
- **Directory:** Storage directory on the NFS server. Ex.: /storage/backup;
- **Reading Bytes:** Sets the read speed of the server bytes;
- **Writing Bytes:** Sets the writing speed of the server bytes;
- **Port:** Defines the port used by the server;
- **Block sizes Bytes:** Determines the size of NFS storage blocks;
- **Protocol TCP** ☐: If this check box is enabled, the TCP protocol will be used by the NFS server;
- **Disable locking** ☐: If this check box is enabled, stored files cannot be blocked;
- **Enable posix** ☐: When activating this check box, this storage will be enabled to be accessed by systems that use POSIX requirements (Portable Operating System Interface);
- **Operation Mode:** Defines the Storage NFS operation mode, which can be:
  - **Hard;**
  - **Soft.**
- **Extra Options:** The configuration of this item can be configured based on the configurations and specifications of the NFS server;
- **Only Logger** ☐: If this check box is enabled, the unit will be used exclusively to store the loggers.



For more information on how to create a single IP Object, see this [page](#).




If the administrator does not know the details of the configuration of the NFS server, he can keep the default values of the interface configuration.

Save

Cancel

After filling in all fields click [  ] to finish or click [  ] to close the window without making any changes;

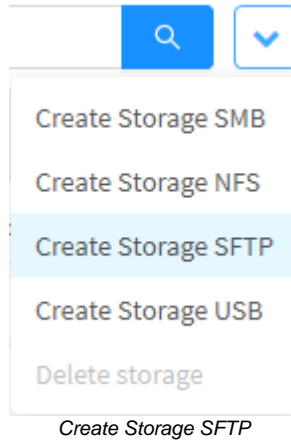
After saving, for the settings to take effect, it will be necessary to access the **command queue** [  ] and apply the changes made. For more information about the command queue visit the page: [UTM - Command queue](#).

Next, we'll look at how to create [SFTP](#) storage.

## Create Storage - SFTP

The "Secure Shell" is a cryptographic network protocol commonly used to connect network services securely, the "SSH File Transfer Protocol" uses these features for data transfer and management. This storage model is made available by the system for "Backup/Restore" applications;

To add an SFTP storage, click [  ] and select the "Create Storage SFTP" option, as shown:



Configure the SFTP server form to store the backup / restore feature.

Create Storage SFTP

X

\* Description

\* User

\* IP

Select

▼

\* Port

Select

▼

\* Directory

Ex./mnt/sftp/

\* Simultaneous transfers

5

☐ Compression

☐ Only Logger

Cancel

Save

### Storage - Add SFTP storage



- **Description:** SFTP store name. Ex.: SFTP *Backup*;
- **User:** User responsible for the SFTP connection. Ex: *user1*;
- **IP:** SFTP server IP address. This field will display the existing IP objects, so it is recommended to create a unique IPv4 address object for the storage that will be used. Ex.: *Storage\_SFTP*;
- **Port:** SFTP service port. Ex.: 22;
- **Directory:** Storage directory on the SFTP server. Ex.: */home/user1/backup*;
- **Simultaneous transfers:** Defines the limit of simultaneous transfers that the System can make using this particular storage. Ex.: 5;
- **Compression** ☐: By activating this checkbox the data from this storage will be compressed;
- **Only Logger** ☐: If this check box is enabled, the unit will be used exclusively to store the loggers.




For more information on how to create a single IP Object, see this [page](#).

Save

Cancel

After filling in all fields click [  ] to finish or click [  ] to close the window without making any changes;

After saving, for the settings to take effect, it will be necessary to access the **command queue** [  ] and apply the changes made. For more information about the command queue visit the page: [UTM - Command queue](#).

After that, we will edit the "SFTP" storage by clicking on the [  ] button in the Action column, the screen below will be displayed.

Edit Storage SFTP

X

\* Description

Backup SSH

\* User

root

\* IP

Storage\_SFTP\_IP

\* Port

SSH

\* Directory

/home/user1/backup

\* Simultaneous transfers

5

☐ Compression

☐ Only Logger


Public Key

ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDcYlgoUdjFAadl3b3QqssJE7bDkth5mi6jfrjHPw  
Tp7wX3CJCRxLLc+i8J6B9I+Qrr9Z9fyf6ztg8O8UwxHXKYcggUfuZS586ecXf8vowUJ7Kjgn

Cancel

Save

SSH - Edit storage SSH

The system will generate a public key to be exported to the SSH server, by clicking on the  icon, after copying the key we will go to the remote server where the SSH will be configured.

In the user's .ssh directory where the backup will be stored, for example: "/home/user1/.ssh", the key that was copied to the authorized\_keys directory will be saved, as shown in the image below.

```
[root@nfsfw .ssh]# pwd
/home/user1/.ssh
[root@nfsfw .ssh]# ls -alh
total 20K
drwx-----. 2 user1 user1 4,0K Dez 22 15:09 .
drwx-----. 5 user1 user1 4,0K Set 14 11:00 ..
-rw-r--r--. 1 user1 user1 1,2K Set 14 11:05 authorized_keys
-rw-----. 1 user1 user1 1,7K Jun 12 2017 id_rsa
-rw-r--r--. 1 user1 user1 394 Jun 12 2017 id_rsa.pub
[root@nfsfw .ssh]#
```

SSH - SSH authorized\_keys

When editing the file we will paste the key and save the changes.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDMyvBeB0Z5idhze48LDCM0w9aN/T81wWUZYwK1W29fLnrApcOvBAH4vaNR1CgmKF71WC1L+ngYARZ8HUxeYgPy2a33nz2BBey80zPVSVOB/2nPxRu0hR0j1NUx0Vwx  
VwSVsb7wPSFY68mt0b0InF/SrdcJzFi4PjhPaDMnTQ0V6NmPXrBwKq+cK3mULw+EjHyysqs6YLX2rojSLC9tAKW5pN5RhjyyavcdLIPg5xe4QEDYpR5d8qQ26FB03RLJ8kOTT/7309SLudplj9iR/FBpeaUEoHg0h+T91bQ  
tKJMTS+N7D5EV0E0LpnKd/QMz44d3UwkM8M2j521/*NLhh root@utm.blockbit.com
```

*SSH - Edit SSH authorized\_keys*

This completes the Device Storage SFTP settings.

Next, we'll look at how to create [USB](#) storage.

# Create Storage - USB

It is a physical data storage device. Type devices (USB-HDD; USB-SSD) are supported. This "Storage" model is made available by the system for "Backup / Restore" applications.

In order to identify a "USB" type device, it will be necessary to make sure that it is connected, and to make some configurations in the CLI so that the assembly, recognition of the device type and configuration of the access unit according to its identification will be done.

To prepare the device so that it is recognized by the system, follow the steps below:

## *Configuration of USB Storage in the CLI*

Initially make sure that the device is connected and that there is no important data stored on it.



**ATTENTION:** Following this step by step, in some configuration steps some commands will clear all data from the storage device.

Make sure that you are using a clean device or that the data inside it is not needed.

Access the Blockbit UTM console via [Terminal](#), login using the admin user and the personalized password.



The default password is:

Login: admin

Password: admin



It is highly recommended to change the default password for the console "admin" user. To change the default password, it is necessary to create a secure password. This password must contain at least 8 characters with uppercase and lowercase letters, numbers and special characters. To change the password, use the CLI command "passwd", check this [page](#) for more information.

Access to the terminal is restricted, to list the available commands, type: ? or **help**.

```

admin >help
arp                               ip                               reset-admin-sessions  uptime
arping                           ipcalc                          reset-logs            vmstat
date                             less                            restore-logger-backup whois
debug-backup                     logger-backup                  rewizard
debug-deployer                  logger-certificate-sync        route
debug-ha                        logger-config                  sar
debug-rotation                  logger-config-sync             set-network-dns
debug-sync                      logger-connect                set-network-gateway
delete-logger-backup            logger-devices-add             set-network-hostname
disable-snm                      logger-devices-list            set-network-interface
enable-root                     logger-disable                 set-network-timezone
enable-snm                      logger-enable                  show-devices
ethtool                         logger-key                     show-license
exit                            logger-storage                 show-logger-backups
fdisk                           logger-update-schedule         show-uuid
free                            lscpu                         show-version
fsck                             mkfs                           shutdown
grep                             more                           snapshot
ha-failover                     netstat                       tcpdump
ha-up                            ntpdate                       tcptop
help                             passwd                         telnet
history                         ping                           tracepath
hostname                        reboot                         traceroute
ifconfig                        reset                          update-gsm
ifstat                         reset-admin-block             update-license
iotest                         reset-admin-password           upgrade-kernel
admin >

```

*Terminal*

1. To list the new disk, type: **fdisk -l**

```

admin > fdisk -l
Disk /dev/sda: 320.1 GB, 320072933376 bytes, 625142448 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x000b93f6

Dispositivo Boot      Start          End      Blocks   Id  System
/dev/sda1  *           2048       1026047       512000   83   Linux
/dev/sda2             1026048   625141759   312057856   8e   Linux LVM

Disk /dev/mapper/root: 21.5 GB, 21474836480 bytes, 41943040 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/swap: 4177 MB, 4177526784 bytes, 8159232 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/data: 293.9 GB, 293890686976 bytes, 574005248 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/sdb: 8000 MB, 8000110592 bytes, 15625216 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >

```

Before formatting the disk, it may be necessary to proceed with partitioning the disk.

Partitioning the disk, run the command: ex.: **fdisk /dev/sdb**

```
admin >fdisk /dev/sdb
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Command (m for help):
```

Type “m” to list the parameter / command base of the “fdisk” utility for disk partitioning.

```
Command (m for help): m
Command action
  a   toggle a bootable flag
  b   edit bsd disklabel
  c   toggle the dos compatibility flag
  d   delete a partition
  g   create a new empty GPT partition table
  G   create an IRIX (SGI) partition table
  l   list known partition types
  m   print this menu
  n   add a new partition
  o   create a new empty DOS partition table
  p   print the partition table
  q   quit without saving changes
  s   create a new empty Sun disklabel
  t   change a partition's system id
  u   change display/entry units
  v   verify the partition table
  w   write table to disk and exit
  x   extra functionality (experts only)

Command (m for help):
```

Delete the current partition. “d – delete a partition”

```
Command (m for help): d
Selected partition 1
Partition 1 is deleted

Command (m for help):
```

Add a new partition. “n – add new partition”

```
Command (m for help): n
Partition type:
  p   primary (0 primary, 0 extended, 4 free)
  e   extended
```

```
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-31299583, default 2048): 2048
Last sector, +sectors or +size{K,M,G} (2048-31299583, default 31299583):
Using default value 31299583
Partition 1 of type Linux and of size 14.9 GiB is set

Command (m for help):
```

Save the new partition table to disk. **“w – write table to disk and exit”**

```
Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```



The system requires that “Disk” devices be formatted according to the EXT4 log file system.


To format the identified disk already partitioned, type: **mkfs -t ext4 /dev/sdb1**

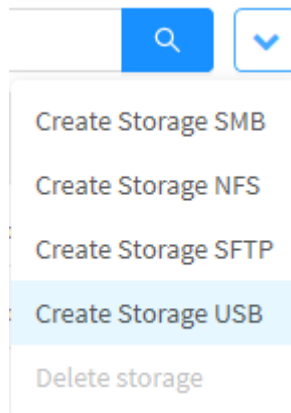
```
admin >mkfs -t ext4 /dev/sdb1
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
979200 inodes, 3912192 blocks
195609 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
120 block groups
32768 blocks per group, 32768 fragments per group
8160 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Once connected to the server and formatted to the EXT4 standard, the device is ready to be listed. For that, we will need to add the storage device in the graphic interface of GSM.

## *Configuration of USB Storage on the Interface*

Click on [  ] and select the "Create Storage USB" option.

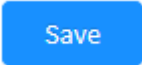
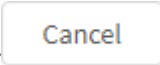



Create Storage USB

The form below will be displayed:

Storage - Add SMB storage

- **Description:** Enter the name of the connection. Ex.: *SMB*;
- **USB Device:** Select the USB storage device to be used, if the list does not display anything, see the steps described [above](#);
- **Simultaneous transfers:** Defines the limit of simultaneous transfers that the System can make using this particular storage. Ex.: 5.

After filling in all fields click [  ] to finish or click [  ] to close the window without making any changes;


After saving, for the settings to take effect, it will be necessary to access the **command queue** [  ] and apply the changes made. For more information about the command queue visit the page: [UTM - Command queue](#).

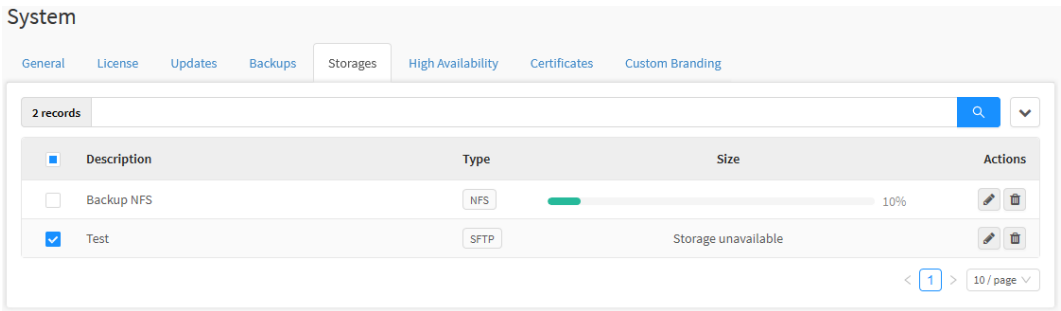
Next, we will detail how to [delete storages](#).



# Storages - Delete Storages

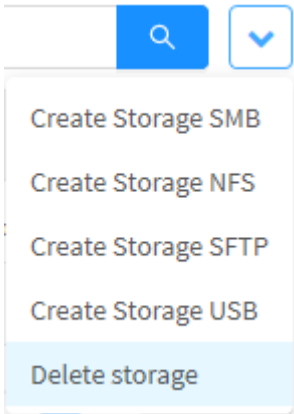
Through the button "Delete Storages" it is possible to delete the selected Storages. To delete from the Actions menu, follow these steps:

- 1. Select which Storage Device (s) you want to delete. To select, just click with the mouse on the checkbox that is located next to the Name. On selected storage devices the checkbox will change from gray to blue [  ]. Ex.: Test;



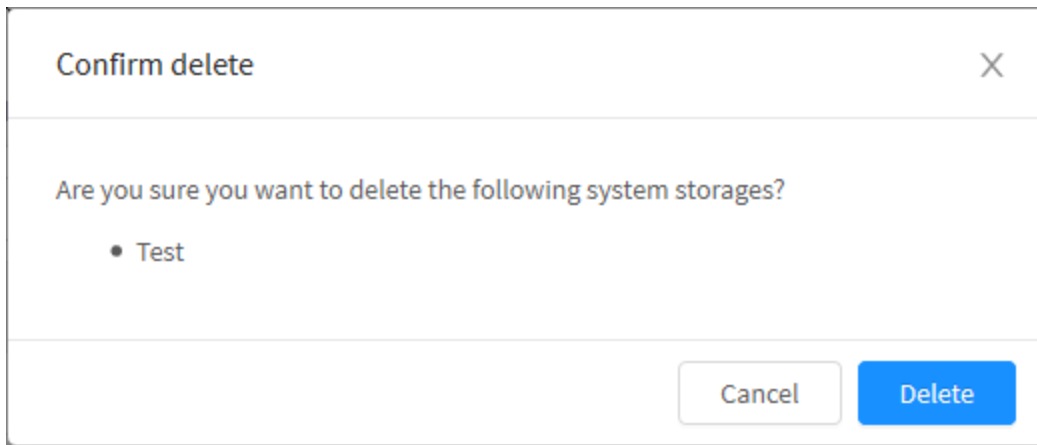
Storages – Selection of Storage Devices to delete

- 2. Enter the **actions menu** [  ] and click on the option "Delete Profile".




Storages – Delete Storage

- 3. The notification message will appear asking if you really want to delete the selected Profiles:



*Storages – Storages deletion message*

If you wish to cancel, click on the [  ] button. To finish, click the [  ] button.

 **System storage deleted successfully!**

*System storage deleted successfully!*

After performing these procedures, the profiles will have been successfully deleted.

Next, we will detail the components of the [columns](#).

# Storages - Columns

Below we will explain the content of each column of the Storages tab:

4 records

<input type="checkbox"/>	Description	Type	Size	Actions
<input type="checkbox"/>	SFTP Storage	SFTP	0%	
<input type="checkbox"/>	SMB Storage	SMB	20%	
<input type="checkbox"/>	USB Storage	USB	99%	
<input type="checkbox"/>	NFS Storage	NFS	52%	
<input type="checkbox"/>	SMB Storage (Logger)	SMB	This Storage is mounted on the logger	

< 1 > 10 / page

Profiles – Storages

Below we will explain each column:

- **Checkbox** : By clicking on this check box, the Storage Device is selected to perform other operations;
- **Description**: Displays the description of the registered Storage Device;
- **Type**: Displays the type of storage, the possible options to be displayed are:
  - [SMB](#);
  - [NFS](#);
  - [SFTP](#);
  - [USB](#).
- **Size**: Displays the percentage of storage usage for the device in question or indicates that the Storage is being used specifically for logger;
- **Actions**: The “Actions” column is made up of buttons:
  - **Edit** : It allows to edit the settings of the Storage Device added in the option of the [actions menu](#);
  - **Delete** : Deletes the profile, it is equivalent to the [Delete Storage](#) option of the actions menu.

For more information on device arrays, see this [page](#).

If you want more information about the High Availability tab, visit this [page](#).


# System - "High Availability" tab

The "High Availability" tab allows the administrator to configure an active primary GSM management server and a secondary passive (standby) server to be used in case of failure. This feature ensures that the system is more resilient by considerably reducing its unavailability and ensuring its normal operation regardless of whether the primary server components are not operational.

The secondary server acts in redundancy of the primary, being activated and assuming the operational functions in case of any type of failure in the primary server, during this event, the main server will be in standby until the situation has been normalized. When the connection returns to normal, the primary server will return to active and the secondary server will be on standby again for any eventual failures that may occur.

The synchronization of the H.A. is resilient, it acts by synchronizing all data in a temporary environment, performs a data integrity validation and then in fact replicates it on the server itself. In addition, all deploys that were not completed thanks to a server failure event, will be restarted and the packages reapplied ensuring that no data or process is corrupted thanks to any event with the clusters.

By default, the server is installed in Standalone mode, that is, the High Availability feature is disabled. If you want to enable it, change the Operation Mode checkbox in Cluster Settings according to which appliance you are configuring, if you want to configure the primary appliance, select the "Primary" option, otherwise choose "Secondary" in order to configure the appliance that will be on standby.

**ATTENTION:** To configure the H.A. the following requirements must be met:

It is mandatory that the two servers have the same computational capacities (Memory, Processor, Storage, etc.), the same models and the same versions, regardless of whether it is a physical or virtual appliance.

The H.A. functionality in the Manager settings can only be enabled when there is no integrated Local Logger. Standalone logger is mandatory.

The primary server must be properly licensed and the license must be linked to the two appliances that will be used.

To configure this feature, click on the "High Availability" tab:



High Availability Tab

The following screen will appear, as shown by the image below:

Cluster Settings

Operation Mode

Primary

Secret Key

\*\*\*\*\*

Local Key

53616c7465645f5fad68ed344d2d0420424e14f09d1515f2db9579f2ca5d2f749d9b2682ad815e5e48346154220f52f54a317cde20d3ef460073067ba72790ac3331f24e0799c5dbb23b3bb6ea17068ed50c0db7099d3f43b5a575541a672dcf57408ed06558e9ca3b2b5ae040dd0a9a3732

Peer Interface #1

eth1

Peer IP #1

10.10.10.2

Peer Interface #2

eth2

Peer IP #2

10.10.10.3

Peer Key

53616c7465645f5f73b43c788731114cd2f196aa697549c02e3a195d7b9830ed762fa599a5bd00533af2d7b5277d63e4648f3ef93a5945a6ec4bf48d5d2fbadce396bd52b0720940a30e0282b7db27681dd7078b0d51c2f2469effac8ca48954aa003182285fc5c9ff44ade56fab437187530

Heartbeat Interval (seconds)

5

Sync Interval (minutes)

5

Fallover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

Auto Activation

☒

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.83	255.255.0.0	
<input type="checkbox"/> ETH1		Select	
<input checked="" type="checkbox"/> ETH2	172.31.207.84	255.255.0.0	

Cluster Status

Local State

PRIMARY ACTIVE

Active Uptime

03:11:14

Peer Connection

UP

Peer State

SECONDARY STANDBY

Synchronization Date

08/01/2021 17:03

Synchronization Status

DONE

## System - High Availability

This screen is composed of the panels:

- [Cluster Settings](#);
- [Cluster Interfaces](#);
- [Cluster Status](#).

In addition, we will also exemplify [how to configure appliances with the H.A..](#)

Next, we will analyze the [Cluster Settings](#) panel.

# High Availability - Cluster Settings

In this panel we can find all the basic configurations of the Cluster used by the High Availability features of the GSM, next we will delve into how to configure each field.

Cluster Settings

\* Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Interface #3

Select

Peer IP #3

Peer Key

\* Heartbeat Interval (seconds)

3

\* Sync Interval (minutes)

5

\* Failover Threshold



5

E-mail Notifications

☐ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** By default, the High Availability feature is disabled (Standalone), to enable it, change this check box according to which appliance you are configuring. The available options are:
  - **Standalone:** This is the default option, if you have already made another configuration, when selecting "Standalone" again the H.A. will be disabled and the system will operate without a secondary server in redundancy;
  - **Primary:** Select this option if you want to configure the main cluster;
  - **Secondary:** Select this option if you want to configure the appliance that will be on standby.

- **Secret Key:** Sets the security key for the high availability cluster. The definition of this password is mandatory, in order to guarantee that unauthorized synchronism will not occur in the clusters, guaranteeing the trust relationship between both devices. This field is required. Both clusters must have the same secret key;
- **Local Key:** Defines the tunnel key, it is a local key that will be used to make the monitoring connection and to synchronize data with the remote server. This field is required. The key is automatically generated by the system and it must be inserted in the peer key at the other end. This field has the buttons:
  - **Copy** : Its function is to copy the secret key, in order to avoid typing errors in the configuration of the clusters;
  - **Change Key** : This button allows the automatic creation of a random secret key.
- **Peer IP #1:** In this field, the IP address of a redundant server is defined with the function of monitoring the heartbeat and performing data synchronism. It is a mandatory field;
- **Peer IP #2:** As in the field above, a redundant IP address for monitoring and synchronization is optionally configured. Peer IP # 2 is activated in case of Peer IP # 1 failures. This field is optional;
- **Peer IP #3:** Just as the previous ones, it is set as a redundant IP for monitoring and synchronism. It is activated in case Peers #1 and #2 fail. Essentially, it's an optional field.



It is possible to configure 1 or 2 heartbeat servers on the Peer IP options.

On the primary server, one must point the Peer IP of the secondary cluster.

On the secondary server, the primary cluster's Peer IP must be pointed.




To configure the Peer IP # 1 and # 2 fields, you will need to configure the interfaces previously in the network settings, see this [page](#).

- **Peer Key:** In this field you must add the "Local Key" of the secondary server (or the primary one, if you are configuring the secondary server). It is used to authorize the connection between devices. It is a mandatory field;
- **Heartbeat Interval:** Determines the monitoring interval, defining when the connection and synchronism tests between the Heartbeat interfaces of the servers will be performed. The value in this field is defined in seconds. This field is required;
- **Sync Interval:** Sets the sync interval for all settings from the primary to the secondary server. This field is determined in minutes. This field is required;
- **Failover Threshold:** Determines the limit of failures in Heartbeat tests, if the maximum value of errors generated by Heartbeat tests is reached, the secondary server will be activated and the primary server will go into standby automatically failing over. This field is determined in seconds. *This field is required;*
- **E-mail Notifications:** In this field, the administrator can register an address to receive notification emails, messages will be sent in real time in failover and synchronism events. In order for notifications to be sent, it is necessary to configure the e-mail tab in Network, for more information, see this [page](#);
- **Auto Activation** ☐: If this option is enabled, automatic activation between the Secondary device and the Primary device will be performed. Therefore, if the primary machine is disabled and this option is checked, it will activate the secondary machine.

Next, we will detail the content of the [Cluster Interfaces](#) panel.

# High Availability - Cluster Interfaces

Este painel exibe todas as interfaces de rede redundantes em um Cluster de alta disponibilidade. À seguir vamos detalhar os componentes deste painel:




The configuration of the interfaces used by the high availability service cluster supports only IPv4 networks.

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual MAC
<input type="checkbox"/> ETH1			
<input type="checkbox"/> ETH2			
<input type="checkbox"/> ETH3			

High Availability - Cluster Interfaces

- **Eth** ☐: When you enable this check box, the fields for configuring the interface are enabled and the interface is activated for use by the Cluster;
- **Virtual IP**: This is the IP that UTMs use to communicate with the manager. Defines the virtual IP address that will be dynamically started on the active device. This field is required;




The virtual IP is the address to which the UTMs will communicate with the Manager, and it is also the IP that is used by the cluster that has priority, this means that:

If the primary server stops working, the secondary server will assume the virtual IP that has been configured in this field.

Likewise, if the secondary server is no longer needed, the primary will activate and assume the configured virtual IP.

- **Netmask**: Determines the netmask that will be used by the virtual IP address. This field is required;
- **Virtual MAC**: Sets the MAC address of the virtual IP. This field is not mandatory, however, if it is left blank, the MAC address of the appliance itself will be used, being susceptible to conflicts with the ARP table.



It is recommended to add a Virtual MAC, this configuration is important to avoid conflicts on the network or with the arp table.

Next, we will detail the [Cluster Status](#) panel.



# High Availability - Cluster Status

The features displayed on this panel make it possible to access the current state of the Cluster, in addition to allowing synchronization and manual activation of the secondary server. Next, we will detail the features available on this screen:

Cluster Status

Local State

SECONDARY ACTIVE

Active Uptime

22:49:56

Peer Connection

DOWN

Peer State

PRIMARY STANDBY

Synchronization Date



09/01/2021 15:30

Synchronization Status

DONE

High Availability - Cluster Status

At the top of this panel we have the following options:

- **Sync Now** [  ]: This button has the function of executing the synchronism manually;
- **Active Now** [  ]: This button performs the manual failover of the clusters, in a normal scenario, for example, when clicking on this button the secondary interface will be activated and the primary will be in standby.

In addition, this panel is composed of the fields:

- **Local State:** Displays the current state of the local device and can be:
  - **Primary Active:** Demonstrates that the primary Cluster is active;
  - **Primary Standby:** Demonstrates that the primary Cluster is in Standby;
  - **Secondary Active:** Demonstrates that the secondary Cluster is active;
  - **Secondary Standby:** Demonstrates that the secondary Cluster is in Standby;
- **Active Uptime:** Displays how long the Cluster changed its status from Active. This field will not display any information if the cluster enters Standby. Ex.: 10 days -21:42:07;



Note that the Active Uptime field does not refer to how long the server has been on, but when the status was changed to "Active".


- **Peer Connection:** Displays the status of the tunnel connection to the remote device, which can be:
  - **Up:** Demonstrates that the connection is working normally;

- **Down:** Demonstrates that the connection has dropped.
- **Peer State:** Displays the current status of the remote device and can be:
  - **Primary Active:** Demonstrates that the primary Cluster is active;
  - **Primary Standby:** Demonstrates that the primary Cluster is in Standby;
  - **Secondary Active:** Demonstrates that the secondary Cluster is active;
  - **Secondary Standby:** Demonstrates that the secondary Cluster is in Standby.
- **Synchronization Date:** Displays the date of the last sync. Ex.: 04/12/2020 -21:42:07;
- **Synchronization Status:** Displays if the status of the last synchronism, which can be:
  - **Success:** Demonstrates that the sync was successful;
  - **Error:** Demonstrates that there was an error in the timing.
- **Error Message:** In case of any error, this field displays a message specifying what happened, which can be:
  - **Connection:** In this case, the message shows that there was an error in the connection between the clusters;
  - **Integrity:** This message demonstrates a failure in the integrity of one of the clusters.

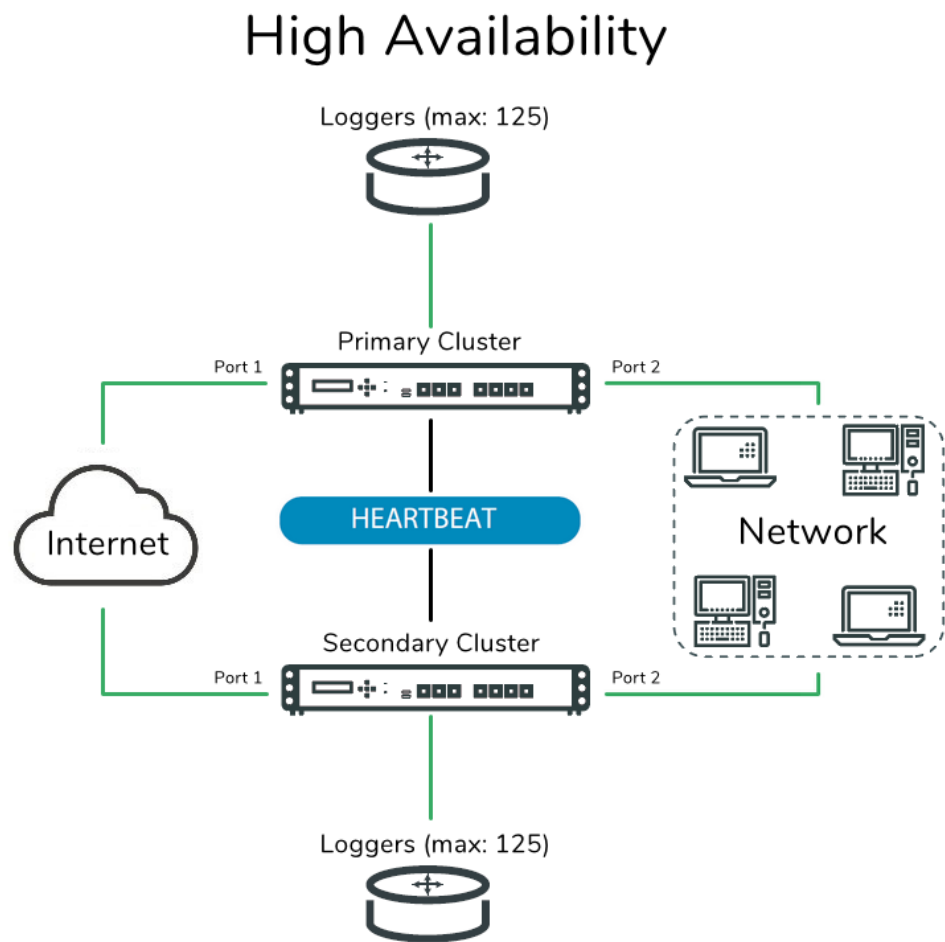
Next we will analyze a [demonstration of how to configure the H.A. in GSM](#).

# High Availability - Example

This section will walk you through setting up a primary and secondary H.A. server.

 For more information about H.A. see this [page](#).

This demonstration will take into account the following structure:



High Availability - Structure

The following IPs will be used in this example:

High Availability - IP Addressing

Name	IP address	IP Virtual
Primary Cluster	172.31.207.81	172.31.207.80
Secondary Cluster	172.31.207.82	

The steps we will take in this demonstration will be:

1. [Primary Cluster Configuration](#);
2. [Secondary Cluster Configuration](#);
3. [Validation of H.A. Settings](#)

We will start the demo by configuring the [Primary Cluster](#) interfaces.

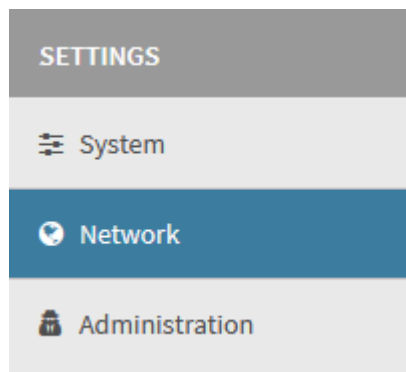
# High Availability - Primary Cluster Configuration

In this example we will make the following settings:

- Configuration of the heartbeat interfaces as the communication with the secondary cluster's IP needs to be functional for the heartbeat to be effective;
- Primary cluster configuration.

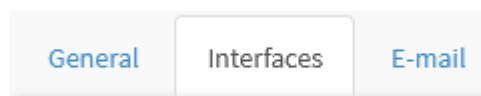
## Interface Configuration

Initially, access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab



Some details of the interfaces tab will not be considered in this example, if you want more information, see this [page](#).

Configure your network as needed, in this example we will use eth0:

Add Edit Interface
✕

---

**\* IP Address**

**\* Mask Address**

☒ Enable

Cancel

Save

Eth0 settings

- **IP Address:** The IP address used by the interface. Following the topology, the IP will be 172.31.207.81;
- **Mask Address:** The mask used by this IP address;
- **Enable** ☒: Select this check box to enable the interface.

Save

Click [ ] to finish the settings:

In addition, we will configure eth1 to use in heartbeat with the secondary Cluster.

Add Edit Interface
✕

---

**\* IP Address**

**\* Mask Address**

☒ Enable

Cancel

Save

Eth1 settings

- **IP Address:** The IP address used by the interface, in this case we will use IP 10.10.10.1;
- **Mask Address:** The mask used by this IP address;
- **Enable** ☒: Select this check box to enable the interface.

Save

Click [ ] to finish the settings:

The screenshot below shows the Primary Cluster interfaces already configured and enabled correctly:

Network Settings

General

Interfaces

E-mail

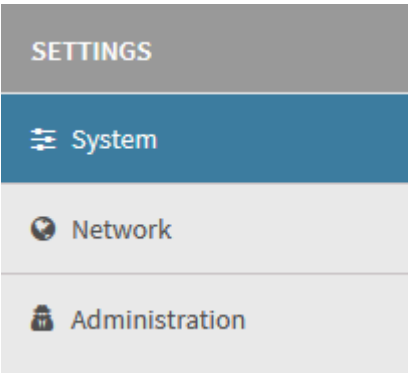
Name	Address	Mask	Status	Actions
eth0	172.31.207.81	255.255.0.0		
eth1	10.10.10.1	255.255.255.252		
eth2	20.20.20.1	255.255.255.252		
eth3	30.30.30.1	255.255.255.0		
eth4				
eth5				

Network Settings - Interfaces

Next, we'll cover the cluster's H.A. settings:

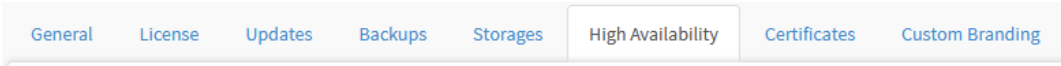
## H.A. Settings

Access the Settings menu and click on the option System:



Settings - System

Click on the High Availability tab:



High Availability Tab

The following screen will be displayed:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

Operation Mode
Standalone

Secret Key

Local Key

Peer Interface #1
Peer IP #1

Peer Interface #2
Peer IP #2

Peer Key

Heartbeat Interval (seconds)
3

Sync Interval (seconds)
5

Failover Threshold (seconds)
5

E-mail Notifications
Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input type="checkbox"/> ETH0		Select	
<input type="checkbox"/> ETH1		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

Next we will detail the panels that we will need to configure.

## Cluster Settings

Complete the form as shown below:



## Cluster Settings

### \* Operation Mode

### Primary

\* Secret Key

.....

\* Local Key

53616c7465645f5f8c2f55ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19  
008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cf  
dbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29dbd8e73

\* Peer Interface #1

eth1

## \* Peer IP #1

### 10.10.10.2

### Peer Interface #2

Select

## Peer IP #2

## \* Peer Key

53616c7465645f5f63fbfe70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6  
fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef  
23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

- \* Failover Threshold (seconds)


5

## E-mail Notifications

admin@blockbit.com

☒ Auto Activation

## High Availability - Cluster Settings

- **Operation Mode:** As this will be the primary Cluster, select the "Primary" option;
- **Secret Key:** Defines the security key for the trust relationship between the clusters, they will need to use the same key. Ex.: q1Q!q1Q!;
- **Local Key:** To generate a certificate for data synchronization, click the  button;
- **Peer Interface #1:** In this field is added the interface that will be used to perform the heartbeat with Secondary Cluster, in which case we will use eth1;
- **Peer IP #1:** In this field the IP of the interface that will perform heartbeat with the Secondary Cluster is added, for that, we will use the IP of eth1 of the Secondary Cluster: 10.10.10.2;
- **Peer Key:** In this field you must paste the "Local Key" of the Secondary Cluster;
- **Heartbeat Interval:** We will set the heartbeat interval to 3 seconds;
- **Sync Interval:** We'll set the sync interval to 5 minutes;
- **Failover threshold:** We will set the limit to 5 failures;
- **E-mail Notifications:** Add the email that will be used to receive notifications from the H.A. service, in which case we will use: [admin@blockbit.com](mailto:admin@blockbit.com);

- **Auto Activation** ☒: Finally, we will enable auto-activation so that the cluster is automatically activated in case of failure.

Next, we will configure the virtual IPs.

## Cluster Interfaces

Complete the form as shown below:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
<input type="checkbox"/> ETH1		Select ▼	
<input type="checkbox"/> ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: In this example we will only use the ETH0 interface, so enable it by checking the checkbox;
- **Virtual IP**: Add to the virtual IP that the cluster will assume when they have priority, in the example we will use the IP: 172.31.207.80;
- **Netmask**: Add the IP address mask, in case: 255.255.0.0;
- **Virtual Mac**: The Virtual Mac is optional, in which case we will use it to avoid conflicts in the ARP table. In the example we will use the MAC: 00:0c:29:f4:f1:ff.

When finishing all the configurations, the screen will be as shown below:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

\* Operation Mode

Primary

\* Secret Key

\*\*\*\*\*

\* Local Key

53618c7465645f5f8fc2755ad99bb7121080b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119cc298f2fe02c039dc55f7295c675acae96fd7b7305bd685cfdbb06f104a4ea0f5cb54d2e43725de74c7e9e322951c829db4539ab1381210733c29db8e73

\* Peer Interface #1

eth1

\* Peer IP #1

10.10.10.2

Peer Interface #2

Select

Peer IP #2

\* Peer Key

53618c7465645f5f8fc2755ad99bb7121080b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119cc298f2fe02c039dc55f7295c675acae96fd7b7305bd685cfdbb06f104a4ea0f5cb54d2e43725de74c7e9e322951c829db4539ab1381210733c29db8e73

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

\* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0	00:0c:29:f4:f1:ff
<input type="checkbox"/> ETH1		Select	
<input type="checkbox"/> ETH2		Select	

Cluster Status

Local State

Active Uptime


Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Primary Cluster

To save, click [  ].

This finalizes the configuration of the primary cluster, next we will [configure the secondary cluster](#).

807

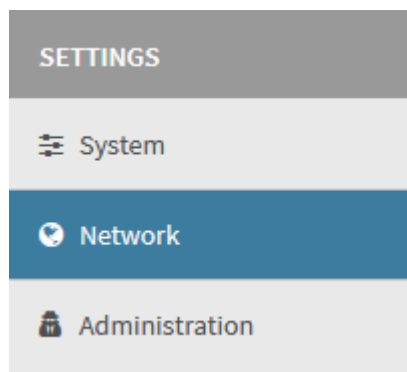
# High Availability - Secondary Cluster Configuration

After having made the configurations in the [Primary Cluster](#), we will make the following configurations in the Secondary:

- It is necessary to perform the Installation Wizard of the secondary machine, according to the guidelines on this [page](#).
- Configuration of the heartbeat interfaces as the communication with the IP of the primary cluster needs to be functional for the heartbeat to be effective;
- Secondary cluster configuration.

## Interface Configuration

Access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab



Some details of the interfaces tab will not be considered in this example, if you want more information, see this [page](#).

Configure your network as needed, in this example we will use eth0:

Add Edit Interface

\* IP Address

172.31.207.82

\* Mask Address

255.255.0.0


☒ Enable

Cancel

Save

Eth0 settings

- **IP Address:** The IP address used by the interface. Following the topology, the IP will be 172.31.207.82;
- **Mask Address:** The mask used by this IP address;
- **Enable** ☒: Select this check box to enable the interface.

Click  to finish the settings:

In addition, we will configure eth1 to use in heartbeat with the Primary Cluster.

Add Edit Interface

\* IP Address

10.10.10.2

\* Mask Address

255.255.255.252

☒ Enable

Cancel

Save

Eth1 settings

- **IP Address:** The IP address used by the interface, in this case we will use IP 10.10.10.2;
- **Mask Address:** The mask used by this IP address;
- **Enable** ☒: Select this check box to enable the interface.

Save

Click [ ] to finish the settings:

The screenshot below shows the Primary Cluster interfaces already configured and enabled correctly:

Network Settings

General Interfaces E-mail

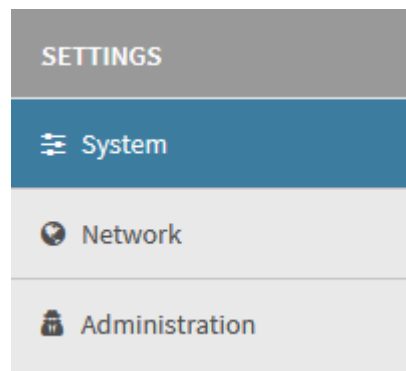
Name	Address	Mask	Status	Actions
eth0	172.31.207.82	255.255.0.0	✓	
eth0	172.31.207.82	255.255.0.0	✓	
eth1	10.10.10.2	255.255.255.252	✓	
eth2	20.20.20.2	255.255.255.252	✓	
eth3	30.30.30.2	255.255.255.0	✓	
eth4			✗	
eth5			✗	

Network Settings - Interfaces

Next, we'll cover the cluster's H.A. settings:

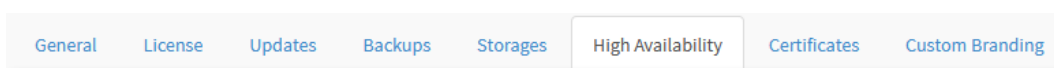
## H.A. Settings

Access the Settings menu and click on the option System:



Settings - System

Click on the High Availability tab:



High Availability Tab

The following screen will be displayed:

System

General

License

Updates

Backups

Storages

High Availability

Certificates

Custom Branding

Cluster Settings

Operation Mode

Standalone

Secret Key

Local Key

Peer Interface #1

Select

Peer IP #1

Peer Interface #2

Select

Peer IP #2

Peer Key

Heartbeat Interval (seconds)

3

Sync Interval (seconds)

5

Failover Threshold (seconds)

5

E-mail Notifications

Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input type="checkbox"/> ETH0		Select	
<input type="checkbox"/> ETH1		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

Next we will detail the panels that we will need to configure.

## Cluster Settings

Complete the form as shown below:

## Cluster Settings

### \* Operation Mode

## Secondary

\* Secret Key

●●●●●●●●

\* Local Key

53616c7465645f5f63fb1e70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

### \* Peer Interface #1

eth1

\* Peer IP #1

### 10.10.10.1

## Peer Interface #2

Select

## Peer IP #2

## \* Peer Key

53616c7465645f58fc2755ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19  
008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cf  
dbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29db8e73

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

\* Failover Threshold (seconds)


5

## E-mail Notifications

admin@blockbit.com

☒ Auto Activation

## High Availability - Cluster Settings

- **Operation Mode:** As this will be the Secondary Cluster, select the "Secondary" option;
- **Secret Key:** Defines the security key for the trust relationship between the clusters, they will need to use the same key. Ex.: q1Q!q1Q!;
- **Local Key:** To generate a certificate for data synchronization, click on the button ;
- **Peer Interface #1:** In this field, the interface that will be used to perform the heartbeat with Primary Cluster is added, in which case we will use eth1;
- **Peer IP #1:** In this field is added the IP of the interface that will perform heartbeat with the Primary Cluster, for that, we will use the IP of the eth1 of the Primary cluster: 10.10.10.1;
- **Peer Key:** In this field you must paste the "Local Key" of the Primary Cluster;
- **Heartbeat Interval:** We will set the heartbeat interval to 3 seconds;
- **Sync Interval:** We'll set the sync interval to 5 minutes;
- **Failover threshold:** We will set the limit to 5 failures;
- **E-mail Notifications:** Add the email that will be used to receive notifications from the H.A. service, in which case we will use: [admin@blockbit.com](mailto:admin@blockbit.com);



- **Auto Activation** ☒: Finally, we will enable auto-activation so that the cluster is automatically activated in case of failure.

Next, we will configure the virtual IPs.

## Cluster Interfaces

Complete the form as shown below:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
<input type="checkbox"/> ETH1		Select ▼	
<input type="checkbox"/> ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: In this example we will only use the ETH0 interface, so enable it by checking the checkbox;
- **Virtual IP**: Add to the virtual IP that the cluster will assume when they have priority, in the example we will use the IP: 172.31.207.80;
- **Netmask**: Add the IP address mask, in case: 255.255.0.0;
- **Virtual Mac**: The Virtual Mac is optional, in which case we will use it to avoid conflicts in the ARP table. In the example we will use the MAC: 00:0c:29:f4:f1:ff.

When finishing all the configurations, the screen will be as shown below:

System

General
License
Updates
Backups
Storages
High Availability
Certificates

Cluster Settings

\* Operation Mode

Secondary

\* Secret Key

\* Local Key

53616c7465645f5f63fb70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c8ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cd82852fec1008c62b518354b112c4a017

\* Peer Interface #1

eth1

\* Peer IP #1

10.10.10.1

Peer Interface #2

Select

Peer IP #2

\* Peer Key

53616c7465645f5f63fb70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c8ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cd82852fec1008c62b518354b112c4a017

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

\* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0	00:0c:29:f4:f1:ff
<input type="checkbox"/> ETH1		Select	
<input type="checkbox"/> ETH2		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Secondary Cluster

To save, click [  ].

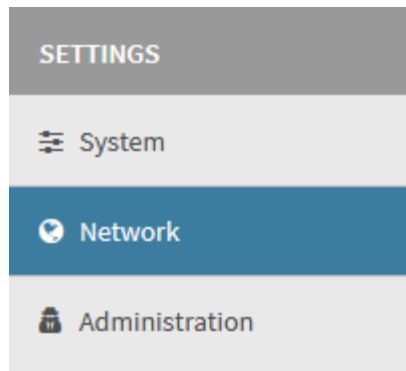
This finalizes the configuration on the secondary cluster, then we will [validate the settings](#).

After having made the configurations in the [Primary Cluster](#), we will make the following configurations in the Secondary:

- Configuration of the heartbeat interfaces as the communication with the IP of the primary cluster needs to be functional for the heartbeat to be effective;
- Secondary cluster configuration.

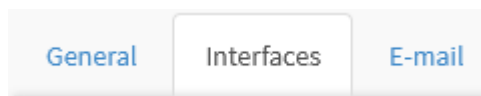
## Interface Configuration

Access the Settings menu and click on Network:



Settings - Network

Click on the Interfaces tab:



Interfaces tab



Some details of the interfaces tab will not be considered in this example, if you want more information, see this [page](#).

Configure your network as needed, in this example we will use eth0:

Add Edit Interface

\* IP Address

172.31.207.82

\* Mask Address

255.255.0.0

☒ Enable

Cancel

Save

Eth0 settings

- **IP Address:** The IP address used by the interface. Following the topology, the IP will be 172.31.207.82;
- **Mask Address:** The mask used by this IP address;

- **Enable** ☒: Select this check box to enable the interface.

Click  to finish the settings:

In addition, we will configure eth1 to use in heartbeat with the Primary Cluster.

Add Edit Interface

\* IP Address

10.10.10.2

\* Mask Address

255.255.255.252

☒ Enable

Cancel

Save

Eth1 settings

- **IP Address:** The IP address used by the interface, in this case we will use IP 10.10.10.2;
- **Mask Address:** The mask used by this IP address;
- **Enable** ☒: Select this check box to enable the interface.

Click  to finish the settings:

The screenshot below shows the Primary Cluster interfaces already configured and enabled correctly:

Network Settings

General

Interfaces

E-mail

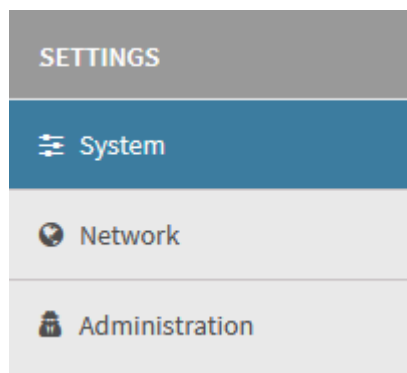
Name	Address	Mask	Status	Actions
eth0	172.31.207.82	255.255.0.0		
eth0	172.31.207.82	255.255.0.0		
eth1	10.10.10.2	255.255.255.252		
eth2	20.20.20.2	255.255.255.252		
eth3	30.30.30.2	255.255.255.0		
eth4				
eth5				

Network Settings - Interfaces

Next, we'll cover the cluster's H.A. settings:

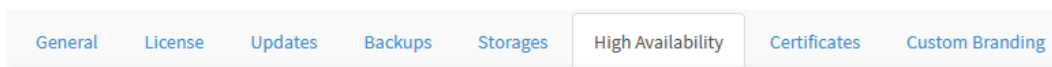
## H.A. Settings

Access the Settings menu and click on the option System:



*Settings - System*

Click on the High Availability tab:



High Availability Tab

The following screen will be displayed:

System
General
License
Updates
Backups
Storages
High Availability
Certificates
Custom Branding

Cluster Settings

Operation Mode
Standalone

Secret Key

Local Key

Peer Interface #1
Peer IP #1

Peer Interface #2
Peer IP #2

Peer Key

Heartbeat Interval (seconds)
3

Sync Interval (seconds)
5

Failover Threshold (seconds)
5

E-mail Notifications
Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input type="checkbox"/> ETH0		Select	
<input type="checkbox"/> ETH1		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

System - High Availability

Next we will detail the panels that we will need to configure.

## Cluster Settings

Complete the form as shown below:

Cluster Settings

\* Operation Mode

Secondary

\* Secret Key

.....

\* Local Key

53616c7465645f5f63fbfe70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c6ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460cdb2852fac1008c62b518354b112c4a017

\* Peer Interface #1

eth1

\* Peer IP #1

10.10.10.1

Peer Interface #2

Select

Peer IP #2

\* Peer Key

53616c7465645f5f8fc2755ad99bb7121060b3c0610ffa71b73be4c6a5d9221b4ebc744432e19008a620832b53b3c5bd3c42f119ce296f2fe02c039dc55f7295c675acae96f1d7b7305bd685cfdbb06f104a4ea6f5cb54d2e43725de74c7e3e322951c829dbc4539ab1381210733c29db8e73

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

\* Failover Threshold (seconds)


5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

High Availability - Cluster Settings

- **Operation Mode:** As this will be the Secondary Cluster, select the "Secondary" option;
- **Secret Key:** Defines the security key for the trust relationship between the clusters, they will need to use the same key. Ex.: q1Q!q1Q!;
- **Local Key:** To generate a certificate for data synchronization, click the  button;
- **Peer Interface #1:** In this field, the interface that will be used to perform the heartbeat with Primary Cluster is added, in which case we will use eth1;
- **Peer IP #1:** In this field is added the IP of the interface that will perform heartbeat with the Primary Cluster, for that, we will use the IP of the eth1 of the Primary cluster: 10.10.10.1;
- **Peer Key:** In this field you must paste the "Local Key" of the Primary Cluster;
- **Heartbeat Interval:** We will set the heartbeat interval to 3 minutes;
- **Sync Interval:** We'll set the sync interval to 5 seconds;
- **Failover threshold:** We will set the limit to 5 failures;
- **E-mail Notifications:** Add the email that will be used to receive notifications from the H.A. service, in which case we will use: [admin@blockbit.com](mailto:admin@blockbit.com);

- **Auto Activation** ☒: Finally, we will enable auto-activation so that the cluster is automatically activated in case of failure.

Next, we will configure the virtual IPs.

## Cluster Interfaces

Complete the form as shown below:

Cluster Interfaces			
Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0 ▼	00:0c:29:f4:f1:ff
<input type="checkbox"/> ETH1		Select ▼	
<input type="checkbox"/> ETH2		Select ▼	

High Availability - Cluster Interfaces

- **ETH0** ☒: In this example we will only use the ETH0 interface, so enable it by checking the checkbox;
- **Virtual IP**: Add to the virtual IP that the cluster will assume when they have priority, in the example we will use the IP: 172.31.207.80;
- **Netmask**: Add the IP address mask, in case: 255.255.0.0;
- **Virtual Mac**: The Virtual Mac is optional, in which case we will use it to avoid conflicts in the ARP table. In the example we will use the MAC: 00:0c:29:f4:f1:ff.

When finishing all the configurations, the screen will be as shown below:



System

General
License
Updates
Backups
Storages
High Availability
Certificates

Cluster Settings

\* Operation Mode

Secondary

\* Secret Key

\* Local Key

53616c7465645f5f63fb70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c8ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460c8b2852fac1008c62b518354b112c4a017

\* Peer Interface #1

eth1

\* Peer IP #1

10.10.10.1

Peer Interface #2

Select

Peer IP #2

\* Peer Key

53616c7465645f5f63fb70e19299bbcb1338592a632daa14dba80ba136d49c23a1700b3db6fc492f8767052c8ecb172a0ed5e22ecba3e4ba334a643a2db3c0814512b8857711e9412bc7ef23449eb775980bcef656a1faf191997c30282674460c8b2852fac1008c62b518354b112c4a017

\* Heartbeat Interval (seconds)

3

\* Sync Interval (seconds)

5

\* Failover Threshold (seconds)

5

E-mail Notifications

admin@blockbit.com

☒ Auto Activation

Cluster Interfaces

Interface	Virtual IP	Netmask	Virtual Mac
<input checked="" type="checkbox"/> ETH0	172.31.207.80	255.255.0.0	00:0c:29:44:f1:ff
<input type="checkbox"/> ETH1		Select	
<input type="checkbox"/> ETH2		Select	

Cluster Status

Local State

Active Uptime

Peer Connection

Peer State

Synchronization Date

Synchronization Status

High Availability - Secondary Cluster

To save, click [  ].

This finalizes the configuration on the secondary cluster, then we will [validate the settings](#).

# High Availability - Configuration Validation

To perform the validation, we will access the CLI of the Primary Cluster and run some commands, in case you need more information about it, consult this [page](#).

One of the simplest tests to validate the functioning of the H.A. is to [ping](#) the Primary Cluster (172.31.207.81) to the Secondary Cluster (172.31.207.82) and check for an answer, as shown in the image below:

```
admin >ping 172.31.207.82
PING 172.31.207.82 (172.31.207.82) 56(84) bytes of data.
64 bytes from 172.31.207.82: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 172.31.207.82: icmp_seq=2 ttl=64 time=0.257 ms
64 bytes from 172.31.207.82: icmp_seq=3 ttl=64 time=0.173 ms
64 bytes from 172.31.207.82: icmp_seq=4 ttl=64 time=0.169 ms
64 bytes from 172.31.207.82: icmp_seq=5 ttl=64 time=0.109 ms

--- 172.31.207.82 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4107ms
rtt min/avg/max/mdev = 0.109/0.177/0.257/0.048 ms
admin >
```

CLI - Validation of communication from the Primary to the Secondary Cluster

It is also possible to carry out these same steps at the other end, following a demonstration using the [ping](#) command to verify the communication from the Secondary Cluster (172.31.207.82) to the Primary (172.31.207.81):

```
admin >ping 172.31.207.81
PING 172.31.207.81 (172.31.207.81) 56(84) bytes of data.
64 bytes from 172.31.207.81: icmp_seq=1 ttl=64 time=0.233 ms
64 bytes from 172.31.207.81: icmp_seq=2 ttl=64 time=0.211 ms
64 bytes from 172.31.207.81: icmp_seq=3 ttl=64 time=0.246 ms
64 bytes from 172.31.207.81: icmp_seq=4 ttl=64 time=0.182 ms
64 bytes from 172.31.207.81: icmp_seq=5 ttl=64 time=0.267 ms
64 bytes from 172.31.207.81: icmp_seq=6 ttl=64 time=0.305 ms

--- 172.31.207.81 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5123ms
rtt min/avg/max/mdev = 0.182/0.240/0.305/0.043 ms
admin >
```

CLI - Secondary Cluster to Primary communication validation using the Ping command

In addition, after making the configuration, the interface itself displays the current status of both Clusters, in Local State the current state of the machine that is currently logged is displayed and Peer State displays the state of the machine at the other end. In the example below we are looking at the Primary Cluster panel that is active, while the Secondary Cluster is in Standby:

Cluster Status

Local State

PRIMARY ACTIVE

Active Uptime

00:43:13

Peer Connection

UP

Peer State

SECONDARY STANDBY

Synchronization Date

13/01/2021 15:59

Synchronization Status

DONE

Cluster Primary Cluster Status

The same panel follows, but observed at the tip of the secondary Cluster:

Cluster Status

Local State

SECONDARY STANDBY

Active Uptime

01:09:53

Peer Connection

UP

Peer State

PRIMARY ACTIVE

Synchronization Date

13/01/2021 17:05

## Cluster Secondary Cluster Status

Finally, to ensure that the H.A. is functioning correctly, we can shut down the Primary Cluster, for that we will issue the command `[shutdown]` in the CLI of the primary Cluster. Thanks to the fact that it is no longer available, the secondary will take priority and will rise to the IP 172.31.207.80 previously defined in the cluster interfaces. The status panel will reflect these changes, as shown below:

Cluster Status

Local State

SECONDARY ACTIVE

Active Uptime

Peer Connection

DOWN

Peer State

PRIMARY STANDBY

Synchronization Date

13/01/2021 17:35

Synchronization Status

DONE

Cluster Secondary Cluster Status after the Primary has been shut down


This concludes the demo, for more information regarding High Availability, see this [page](#).

For more information on the status of High Availability, see this [page](#).

# System - "Certificates" tab

The resources on this tab, allow the administrator to configure his own certification authority, which is a simple and practical way of obtaining the certificate that will be used to ensure reliability in accessing the solution's resources.

The purpose of a certification authority is to confirm the ownership of the certificates, confirming that the certificate received when accessing a particular website or address really belongs to the entity that is providing it. This is what ensures that you are even securely accessing SSL / HTTPS websites and addresses.

 It is necessary to configure a CA in this tab to be able to create a SAML identity provider, for more information see this [page](#).

To access the certificate management interface, access the Certificates tab.



Certificates tab

System

General License Updates Backups Storages High Availability Certificates Custom Branding

Certificates

\* Country

US

\* State

New York

\* City

New York

\* Organization

Blockbit

\* E-mail

admin@blockbit.com

\* Organizational Unit

QA

\* Expires in (years)

10

\* Hostname

gsm.blockbit.com


\* Key Size

1028

System - Backups

Next we will detail the fields on this form.

- **Country:** Determines the country. Ex.: *US*;
- **State:** Sets the state. Ex.: *New York*;
- **City:** Determines the city. Ex.: *New York*;
- **Organization:** Defines the company name. Ex.: *Blockbit*;
- **E-mail:** Determines the administrator's email. Ex.: *admin@blockbit.com*;
- **Organizational Unit:** Defines the department. Ex.: *QA*;
- **Expires (years):** Determines the validity time of the certificate. Ex.: *10 anos*;
- **Hostname:** Defines the CA Hostname. Ex.: *admin@blockbit.com*;
- **Keysize:** Defines the size that the CA key will have. Ex.: *2048*.

When finishing the configuration, click [  ] to save.





Saving a CA requires the server to generate a new certification body. *This action requires reinstallation of the new CA on all devices on the network.*



If you want to recreate the CA, you must also re-create the Server Certificate, this procedure requires the installation of the new CA on all devices on the network. *Download the CA and reinstall on all workstations. Remembering that to validate the new CA you must RESTART the server.*

This completes the configuration of the certificates tab.

Next we will analyze the [Custom Branding](#) tab.

# System - "Custom Branding" tab

In this tab, the GSM can be customized, being possible to change the product title, icon, background image, menu colors etc. Using these options it is possible to customize the GSM according to the visual identity used by the user's company.


The customization of appliances is controlled through a license, therefore, this option will only be available if the user has a valid active customization license. If the GSM license allows customization, the custom branding tab will be available.

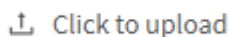






For more information on how to customize UTMs, see this [page](#).

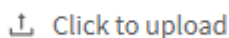


System Settings - Custom Branding


- **Page title:** Defines the name that will be displayed in the title bar in the system window. Ex.: UTM;
- **Section:** This option customizes the color of the GSM sections (where "Management", "Analytics" and "Settings" appear), this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #89968e;
- **Section Font:** In this option, the font color of the GSM sections is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Selected:** In this option, the color of the selected menus and the top bar of the GSM is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #466452;
- **Selected Font:** In this option, the font color of the selected menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #f9f9f9;
- **Menu:** In this option, the color of the menus is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #81d47a;
- **Menu Font:** In this option, the color of the menu fonts is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #000000;
- **Base:** In this option, the base color of the panel where the menus are located is customized, this field accepts the HEX color code, in addition it is possible to click on the box beside and select the desired color in a color picker with RGBA field. Ex.: #b4daaa;




 Click to upload

- **Favicon:** Clicking the  button allows you to upload the page's favicon. If you want to view the added image, click , to download click , to delete, click . The format needs to be PNG or ICO, the minimum dimensions are 24x24, there is no maximum size, it is only necessary that the image has the same height and width (must be squared shaped);

 Click to upload

- **Logo:** Clicking the  button allows you to upload the logo used at the top of the menus. If you want to view the added image, click , to delete, click . The format needs to be SVG of dimensions 300x65. There is no maximum size, it is only necessary that the image has different height and width (be rectangular);

 Click to upload

- **Background:** Clicking the [  ] button allows you to upload an image that is used as a background on the initial login screen. If you want to view the added image, click [  ], to delete, click [  ]. The format needs to be PNG or JPG of dimensions 1920x1080;
- **Preview:** Demonstrates the changes that were made to the options above in a preview for checking before actually applying them.

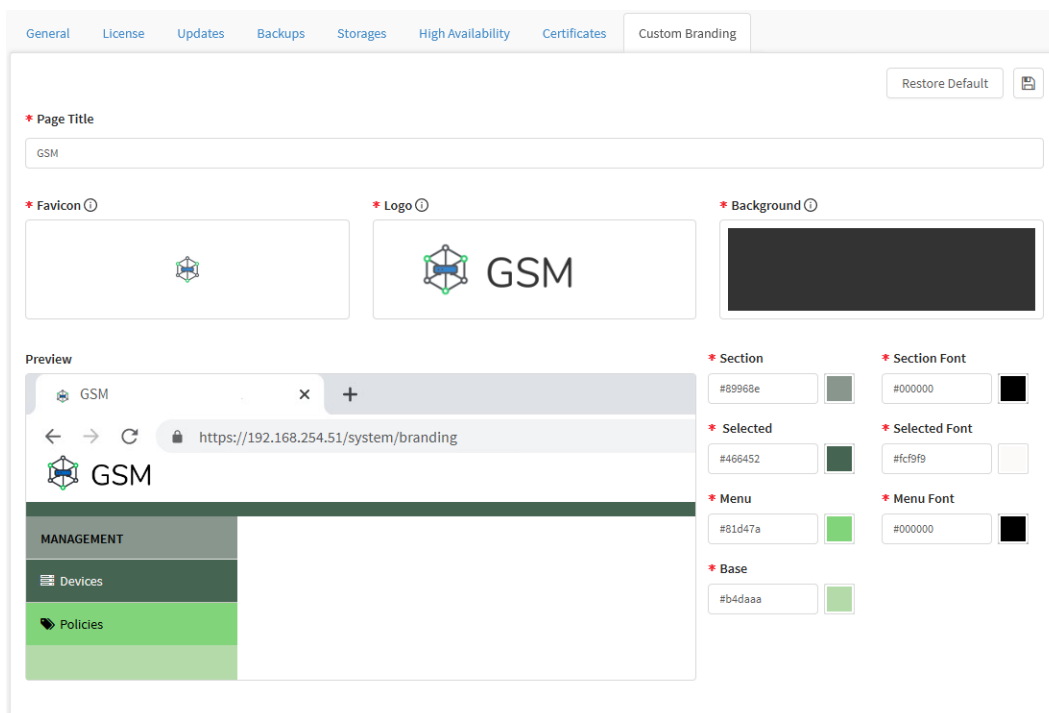


To assist in defining colors:

It is possible to create or consult a color palette on the website <https://coolers.co/generate> that provides coloring information at: *Color Name, HEX, RGB, HSB, HSL, CMYK, LAB, RAL, HKS, Copic and Prismacolor.*

If it is necessary to convert from Pantone to RGB, CMYK or HEX, see the converter on the official website at this link: <https://www.pantone.com/color-finder>.

Here is an example of a template with customization already applied:

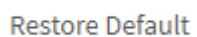


Config Template - Custom Branding - Edited template



When applying custom branding on UTM it may be necessary to clear the browser cache to view the changes.

To access the cache deletion window just use the command "ctrl + shift + del".

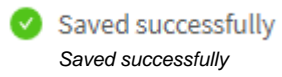


If you are not satisfied with the changes made, click [  ] to restore the default settings.



To save changes, click [  ].






After performing these procedures, the firewall customization was successful.

For more information on the tabs in System, see this [page](#).

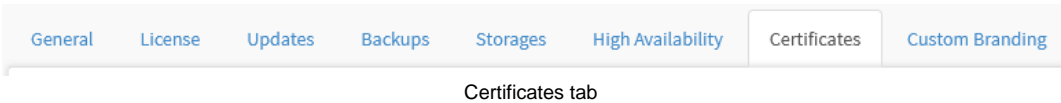
# System - Certificates tab

The resources on this tab, allow the administrator to configure his own certification authority, which is a simple and practical way of obtaining the certificate that will be used to ensure reliability in accessing the solution's resources.

The purpose of a certification authority is to confirm the ownership of the certificates, confirming that the certificate received when accessing a particular website or address really belongs to the entity that is providing it. This is what ensures that you are even securely accessing SSL / HTTPS websites and addresses.

 It is necessary to configure a CA in this tab to be able to create a SAML identity provider, for more information see this [page](#).

To access the certificate management interface, access the Certificates tab.



## System

GeneralLicenseUpdatesBackupsStoragesHigh AvailabilityCertificatesCustom Branding

Certificates

\* Country

US

\* City

New York

\* E-mail

admin@blockbit.com

\* Expires in (years)

10

\* Key Size

1028

\* State

New York

\* Organization

Blockbit

\* Organizational Unit

QA

\* Hostname


gsm.blockbit.com

System - Backups

Next we will detail the fields on this form.

- **Country:** Determines the country. Ex.: *US*;
- **State:** Sets the state. Ex.: *New York*;
- **City:** Determines the city. Ex.: *New York*;
- **Organization:** Defines the company name. Ex.:*Blockbit*;
- **E-mail:** Determines the administrator's email. Ex.: *admin@blockbit.com*;
- **Organizational Unit:** Defines the department. Ex.: *QA*;
- **Expires (years):** Determines the validity time of the certificate. Ex.: *10 years*;
- **Hostname:** Defines the CA Hostname. Ex.: *admin@blockbit.com*;
- **Keysize:** Defines the size that the CA key will have. Ex.: *2048*.



When finishing the configuration, click [  ] to save.



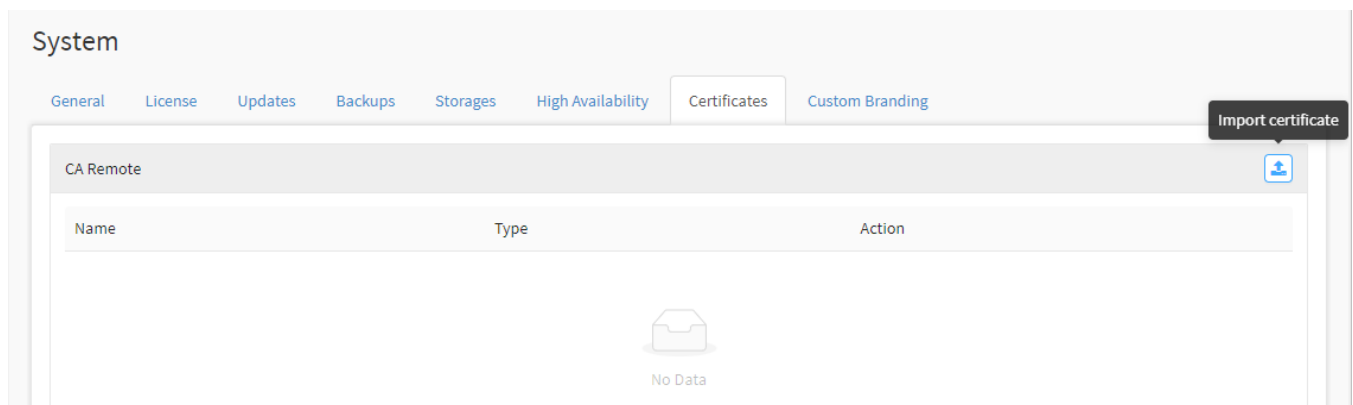
Saving a CA requires the server to generate a new certification body. *This action requires reinstallation of the new CA on all devices on the network.*



If you want to recreate the CA, you must also re-create the Server Certificate, this procedure requires the installation of the new CA on all devices on the network. *Download the CA and reinstall on all workstations. Remembering that to validate the new CA you must RESTART the server.*

## Import Certificates

This option allows the upload of .CRT or .PEM format certificates:



### Certificates - Import Certificate

When clicking *Import Certificate*, the upload screen will appear:

☒ .pem ☐ .crt

\* Name

Upload .pem

\* Certificate

\* Private Key

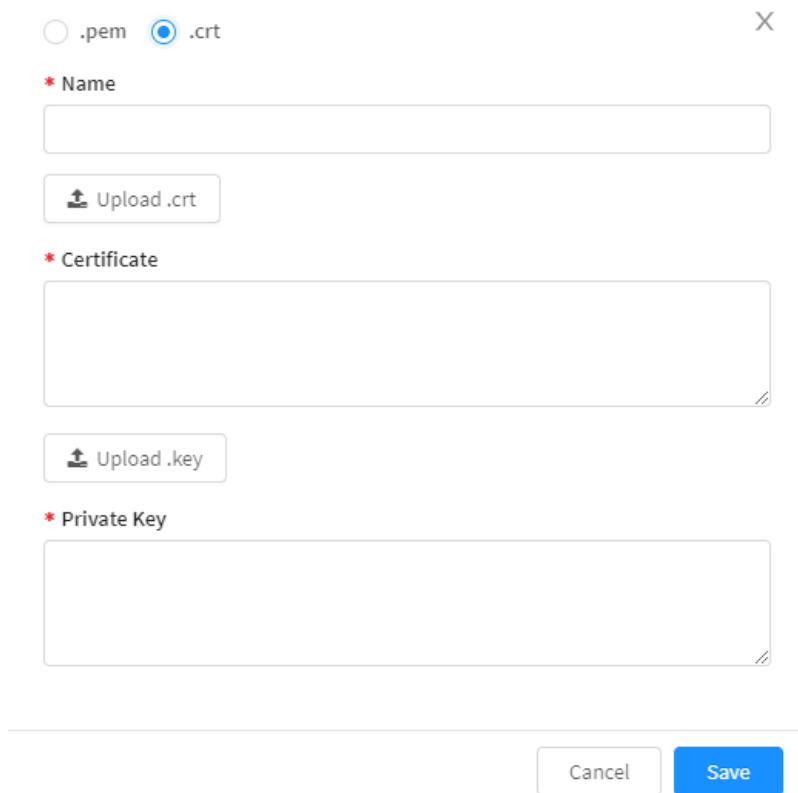
Cancel

Save

#### Import certificates - .PEM files

- **Name:** Insert a customized name for the certificate;
- **Upload .PEM:** Select the .PEM certificate to be used;
- **Certificate:** Insert the certificate's name;
- **Private Key:** Field for the insertion of the certificate's validation key.

When selecting the .CRT option, the "upload key" field will be displayed:



The form is titled "Import certificates - .PEM files" and has a close button (X) in the top right corner. It contains three main sections, each with a red asterisk indicating a required field:

- Name:** A text input field.
- Upload .crt:** A button with an upload icon and the text "Upload .crt".
- Certificate:** A large text area for entering the certificate's name.
- Upload .key:** A button with an upload icon and the text "Upload .key".
- Private Key:** A large text area for entering the certificate's validation key.

At the bottom right, there are two buttons: "Cancel" and "Save".

#### Import Certificates - .CRT files

- **Name:** Insert a customized name for the certificate;
- **Upload .CRT:** Select the .CRT certificate to be used;
- **Certificate:** Insert the certificate's name;
- **Upload .KEY:** Field used to select the .KEY file;
- **Private Key:** Field for the insertion of the certificate's validation key.

## Revocation

This option allows the upload of .CRT format certificates:

## System

[General](#) [License](#) [Updates](#) [Backups](#) [Storages](#) [High Availability](#) [Certificates](#)

CA Remote

Name	Type	Action
<div><div></div><div>No Data</div></div>		

Revocation

Ativo

Servidor LDAP

☒

LDAP

Ativo

URL

☒

blockbit.com

### *Certificates - Revocation Certificate*

The revoked certificates list can be updated by these methods:

- Importing a Revoked Certificates List, normally a ".crl" file;
- Through a LDAP server;
- Through a web server.

This completes the configuration of the certificates tab.

Next we will analyze the [Custom Branding](#) tab.

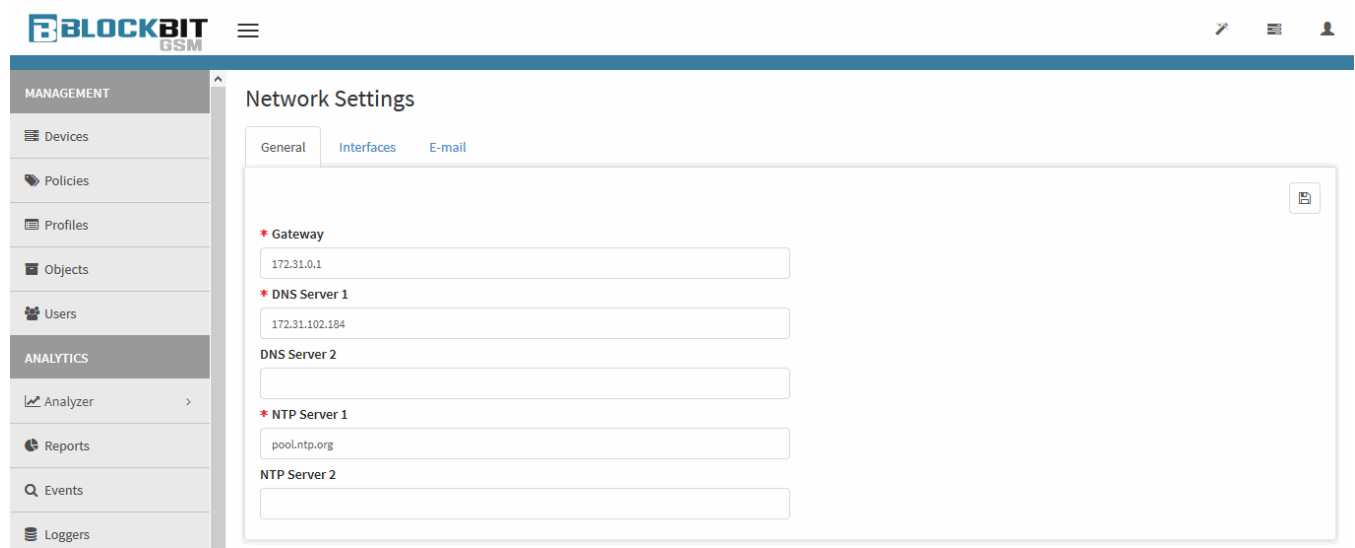
# Network

Through the "Network" button it is possible to change the network settings.



Settings – Network

The System screen will appear with the "General" tab pre-selected, as shown below:



Settings - Network - "General" tab

The Network Settings screen has the following tabs:


- [General](#);
- [Interfaces](#);
- [E-mail](#).

We will describe the features below.

# Network - "General" tab

This screen allows you to change the server settings:

GeneralInterfacesE-mail



\* Gateway

172.23.0.1

\* DNS Server 1

8.8.8.8

DNS Server 2

1.1.1.1

\* NTP Server 1

pool.ntp.br

NTP Server 2

a.ntp.br

Key ID

Server Key

Type Key


MD5

☐

Enable auth

Network Settings

- **Gateway:** Default network route address. Ex.: 172.16.102.1;
- **DNS Server 1:** Set the network or internet DNS server. Ex.: 176.16.102.161;
- **DNS Server 2:** Set the secondary DNS for your network or the internet. Ex.: Secondary Google DNS 8.8.4.4;
- **NTP Server 1:** Set the clock synchronization server. Ex.: [a.ntp.br](#);
- **NTP Server 2:** Set the secondary clock synchronization server. Ex.: [b.ntp.br](#).
  - **Enable Auth:** Enables PEERS/Server authentication support;
  - **Key ID:** Enter Peer key;
  - **Server Key:** Enter Sever key;
  - **Type Key:** Select key type (MD5, SHA1 or SHA256).

Click the [] button located in the upper right corner of the screen to save the changes made to the settings.

# Network - "Interfaces" tab

This screen allows you to change the network interface settings.

General

Interfaces

E-mail

Name	Address	Mask	Status	Actions
eth0	172.31.240.245	255.255.0.0		
eth1				
eth2				
eth3				

Network Interfaces

- **Name:** The name of the network interfaces. Ex.: eth0;
- **Address:** Blockbit GSM IP address. Ex.: 172.16.102.235;
- **Mask:** Define the Net mask. Ex.: 255.255.254.0;
- **Status:** Determines whether the network interface is **enabled** or **disabled** , to activate the status, edit the interface;
- **Action:** By clicking on the button, you can edit the network settings;
- **Reload Interfaces button:** Clicking on the *refresh* button updates the number of network interfaces in Blockbit GSM.

To edit an interface's network settings follow the steps below:

1. In the Action column, click the button. Fill in the data you want to edit:
- **Address:** Blockbit GSM IP address. Ex.: 10.0.0.1;
  - **Mask:** Define the Net mask. Ex.: 255.255.255.0.



Add Edit Interface

\* IP Address

172.31.240.245

\* Mask Address

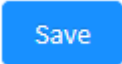
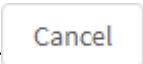
255.255.0.0


☒ Enable

Cancel

Save

*Edit Interface.*

2. To save changes, click [  ], otherwise click [  ] to close the window.

Click on the synchronize [  ] button located in the upper right corner of the screen to save the changes made to the settings.

# Network - "E-mail" tab

This screen allows you to change the settings for sending and receiving notifications via e-mail.

General

Interfaces

E-mail

\* Server

smtp.blockbit.com

\* Port

587

User

user@blockbit.com

Password

.....


\* Security


SSL

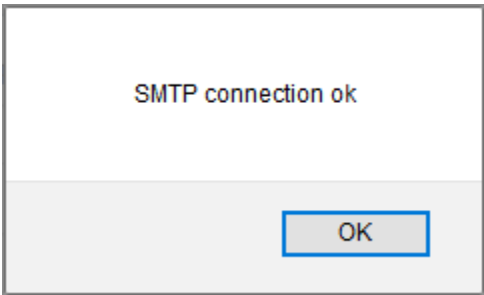
E-mail

Below we will analyze each field of the form:

- **Server:** Determines the email server. Ex.: [smtp.blockbit.com](#);
- **Port:** Determines the port to be used. Ex.: 587;
- **User:** The user's email. Ex.: [user@blockbit.com](#);
- **Password:** The password to be used;
- **Security:** The type of encryption having three options: "SSL", "TLS" and "none" (no encryption).

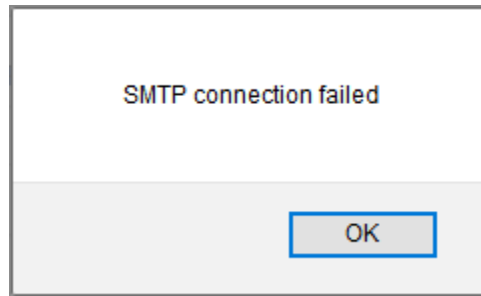
After completing the fields, it is recommended to perform a check by clicking the **configurations**[] button, then we will analyze this procedure:

- **Settings button:** When clicking on the **configurations**[] button a check is made on the server to detect if it is working correctly. A validation on the access credentials is performed and, finally, a check is performed on the door service, being able to display three messages:
  - **SMTP connection ok:** If the settings are working correctly, as shown in the image below;



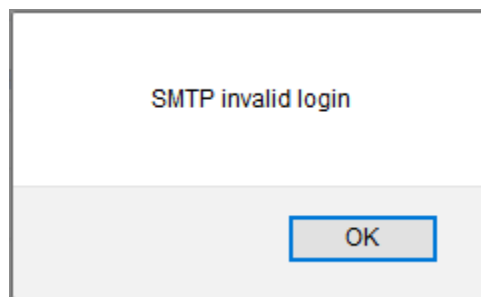
SMTP connection ok

- **SMTP connection failed:** If there is an error in the server settings, as exemplified by the image below;




*SMTP connection failed*

- **SMTP invalid login:** If the credentials are incorrect, as shown in the image below.



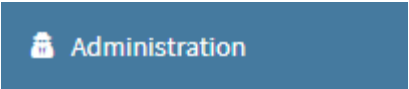
*SMTP invalid login*

Click **save** [  ] located in the upper right corner of the screen to save the changes made to the settings.

# Administration

Through the “Administration” button it is possible to change the GSM administrative settings.

To do so, click on the appropriate option as shown below:



Settings – Administration

The Administration screen will appear with the “Users” tab pre-selected, as shown below:

## Administration

AdministratorsUsers ProfilesMFAAuth ServersIdentity ProviderAudit LogAccess Control

2 records

☐

Name

☐

admin

☐

admin 2

☐

E-mail

☐

admin@blockbit.com

☐

admin2@blockbit.com

☐

Profile

☐

Read-Write

☐

Read-Only

☐

Type

☐

Local

☐

Local

☐

Auditor

☐

☐

Actions

☐

<

1

>

10 / page

Settings – Administration

The Administration screen has the following tabs:

- [Administrators](#);
- [Users Profiles](#);
- [Auth Servers](#);
- [Identity Provider](#);
- [Audit Log](#);
- [Access Control](#).

We will describe below all the features of this screen.

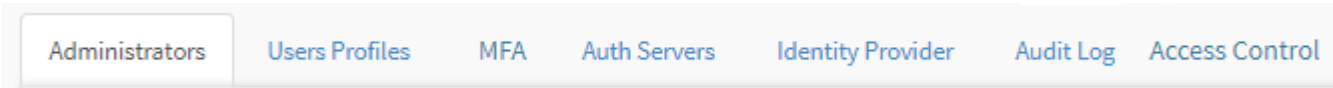
# Administration - "Administrators" tab

In the "Administrators" tab it is possible to register users with an administrative profile in Blockbit GSM.

Blockbit GSM allows two or more administrator profile users simultaneously.

The "Administrators" tab consists of six columns: "Name", "E-mail", "Profile", "Type", "Auditor", "Actions" and the search bar, which is located at the top of the screen, as well as the action menu.

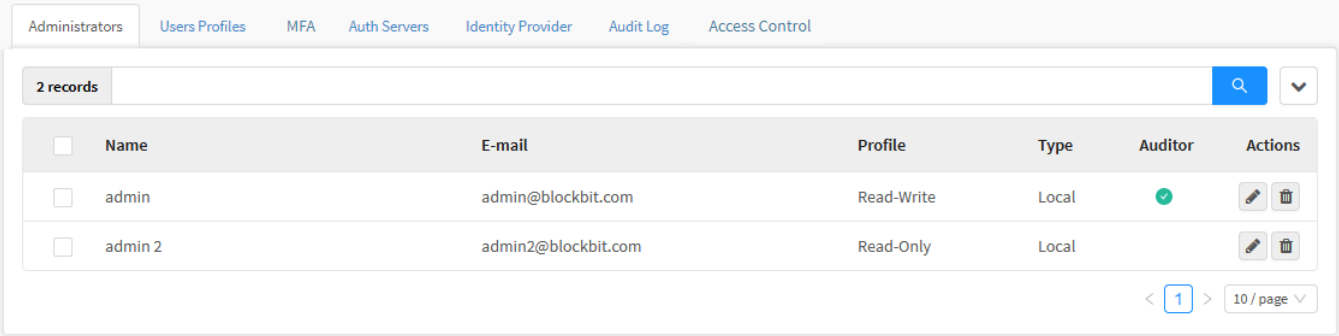
If it is not already selected, click on the "Administrators" tab.



Administrators tab

The screen shown by the image below will appear:

## Administration



Administration - Administrators

This section will cover the [Registration](#), Editing and [Removal](#) of administrator users

Next, we'll look at each component of this panel.

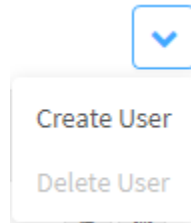
# Administration - Administrators - Actions Menu

At the top right of the screen we have the actions menu:



Users - Actions menu button

By clicking on this button the menu below is displayed:



Users - Actions menu

The menu consists of the following options:

- [Create User](#);
- [Delete User](#).

Next, each option in the action menu will be detailed.

# Administrators - Actions Menu - Create User



When accessing the **actions menu** [ ] and clicking the "Create User" button, the "Create Admin User" form will appear, as illustrated by the image below.

The image shows a web form titled "Create Admin User" with a close button (X) in the top right corner. The form contains several fields, each with a red asterisk indicating it is required:

- Name**: A text input field.
- E-mail**: A text input field.
- Profile**: A dropdown menu with a downward arrow.
- Type**: A dropdown menu with "Local" selected and a downward arrow.
- Password**: A text input field with a toggle icon (an eye with a slash) on the right.
- Confirm Password**: A text input field with a toggle icon (an eye with a slash) on the right.
- Auditor**: A checkbox.

At the bottom right of the form are two buttons: "Cancel" and "Save".

Administration – Create Admin User.

In this form it is possible to create a new user with their respective access profile, according to the fields below:

- **Name**: Defines the Username. Ex.: "Admin";
- **E-mail**: The user's access email. Ex.: "admin@[blockbit.com](mailto:admin@blockbit.com)";
- **Profile**: In this session it is possible to determine the access profile of the user being registered. Select the profile previously registered in the "Profiles" tab in the drop-down list. Ex.: "WebFilter - Admins";
- **Type**: Defines whether the administrator user will log in locally or perform remote access to the system. If you selected "Remote" the form will display the field for selecting the type of server instead of the password and confirmation of the same. See the image below for more information;
- **Server**: If in "Type" the option "Remote" has been selected, this field will be displayed instead of "Password" and "Confirm Password". Select the remote server to be used for remote authentication, the items present in this checkbox are added to the [Server](#) tab;
- **Password**: If in "Type" the option "Local" has been selected, this field will be displayed instead of "Server". Enter user password;
- **Confirm Password**: Just like "Password", this field is only available in local access, its function is to confirm the password security, type it again;
- **Auditor**: This checkbox determines whether the user has access as an "Auditor".

As mentioned earlier, if the "Remote" option is selected in the "Type" field, the "Server" field will be displayed, as shown in the image below:

**Create Admin User** X

\* **Name**

\* **User**

\* **Profile**

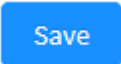
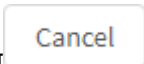

\* **Type**

\* **Server**

☐ **Auditor**

Cancel Save

Administration – Create Admin User

Click the [  ] button to save all changes, otherwise, click [  ] or the [  ] at the top right of the screen to close the window.



# Administrators - Actions Menu - Delete User

The “Delete User” button in the action menu is used to remove users who were previously selected by clicking on the checkbox. As shown below:

Administration

Administrators

Users Profiles

MFA

Auth Servers

Identity Provider

Audit Log

Access Control

2 records

Name

E-mail

Profile

Type

Auditor

Actions

admin

admin@blockbit.com

Read-Write

Local

test

test@blockbit.com

Read-Only

Local

<

1

>

10 / page

Administration - Selection for removal

After selecting this option, a verification message will appear requesting confirmation.

Delete User

X

Are you sure you want to delete the following User ?

• Test

Cancel

Delete

Delete User

When you click [Delete], the selected users will be removed. If you click [Cancel], this verification message will be dismissed without performing any removal.

# Administration - Administrators - Columns

Below we will explain each column of the Administrators tab:

Administração

Administradores Perfis de Usuários MFA Servidores de Autenticação Provedor de Identidade Log de Auditoria Controle de Acesso

7 records

<input type="checkbox"/>	Nome	E-mail	Perfil	Tipo	Auditor	Api	Ações
<input type="checkbox"/>	admin	admin@blockbit.com	Read-Write	Local			
<input type="checkbox"/>	Buenos	william.bueno@gmail.com	Read-Write	Local			
<input type="checkbox"/>	erick	ejsilva@blockbit.com	Read-Write	Local			
<input type="checkbox"/>	Teste de bancada	teste@blockbit.com	Read-Write	Local			
<input type="checkbox"/>	wes1	wes1@gmail.com	Read-Write	Local			
<input type="checkbox"/>	wes2	wes2@gmail.com	Read-Write	Local			
<input type="checkbox"/>	william	wbueno@blockbit.com	Read-Write	Local			

< 1 > 10 / page

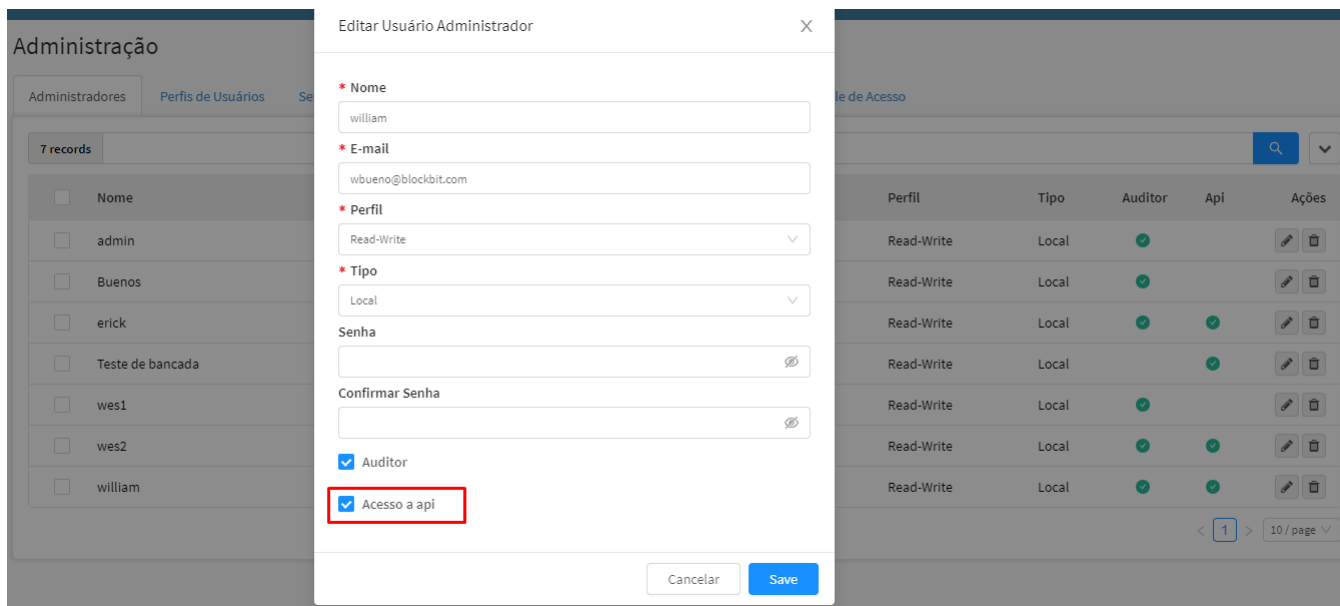
Administration - Users

- **Select** ☐: Allows you to select one or more users;
- **Name**: Displays the name of the Blockbit GSM administrator user;
- **E-mail**: Displays the E-mail of the registered user;
- **Profile**: Determines the user profile, this profile is configured in the [Users Profiles](#) tab;
- **Type**: Displays whether the administrator user will log in locally or perform remote access to the system. This option is configured when [creating the user](#);
- **Auditor**: If the user has an auditor's permission, the icon will be displayed. This option is configured when [creating the user](#);
- **API**: Allows the user to enable the use of the API for collecting individual data from NGFWs (and from Firewall, Policies, IPS, from other devices as well), having as output an external secure platform.
- **Actions**: Provides the following essential functions:
  - **Edit** : Allows you to edit one of the [added](#) users;
  - **Delete** : Allows you to [delete](#) a user.

## API RESTful

The GSM API collects data from other NGFWs in JSON format through a server service. The GSM uses a RESTful API (Representational State Transfer) that consists on a system of architectural communication constrictions which allows the exchange of information between different systems in a safe way through the network. In this document we will analyze the operational details of this function.

In Administration Administrators, we have the "API" column showing the sign for administrator users with the API on. In order to enable it, just edit a preexisting administrator user profile or create one, and mark the "API" option, as we can see on the image below:



Editing an administrator user profile.

- **Name:** Enter the GSM username.
- **E-mail:** Enter the user's e-mail for the login.
- **Profile:** Choose between READ-ONLY and READ-WRITE, to moderate the user permission between just reading, or reading and editing.
- **Type:** Choose between Local or Remote access (Local is used for users created on this very same GSM).
- **Password:** Enter the password.
- **Auditor:** Users with full-fledged administrator access. If limited is selected, any changes done on the system by this user will go through an audit process.
- **API Access:** Mark this option to enable the GSM API, making it possible for NGFWs data to be accessed remotely through the API.

This way, the Firewall, Web Filter and IPS information will be sent to the safe platform out of the GSM. Bellow is some of the information that will be provided by the GSM through the API:

- **Appliance information:** NGFW's name, firmware version, status (up or down), License status (Active/expired).
- **Firewall information:** Number of connections, users, data traffic.
- **Intrusion Prevention System IDS/IPS:** Amount of detected attacks, Total alerts and blocked threats, Top 10 signatures, Top categories, Top risk, Allow filter (6 months, 3 months, 1month, 7 days, 3days, 24 hours, 12 hours), Initial and final hour.
- **Policies application: Consumption by Policy;** total traffic by IP/user, Total services, Ports and consumption; Allow filter (6 months, 3 months, 1month, 7 days, 3days, 24 hours, 12 hours), Initial and final hour.

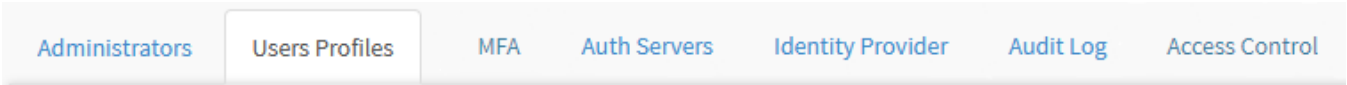
For further detail on the functioning of the GSM API click here and access the [GSM API manual](#).

# Administration - "Users Profiles" tab

In the "Users Profiles" tab, we can see the Profiles of Blockbit GSM administrators, its function is to determine the level of access and restriction that users configured with a certain profile will have within the system. This feature guarantees more specificity in the management of permissions of administrative users.

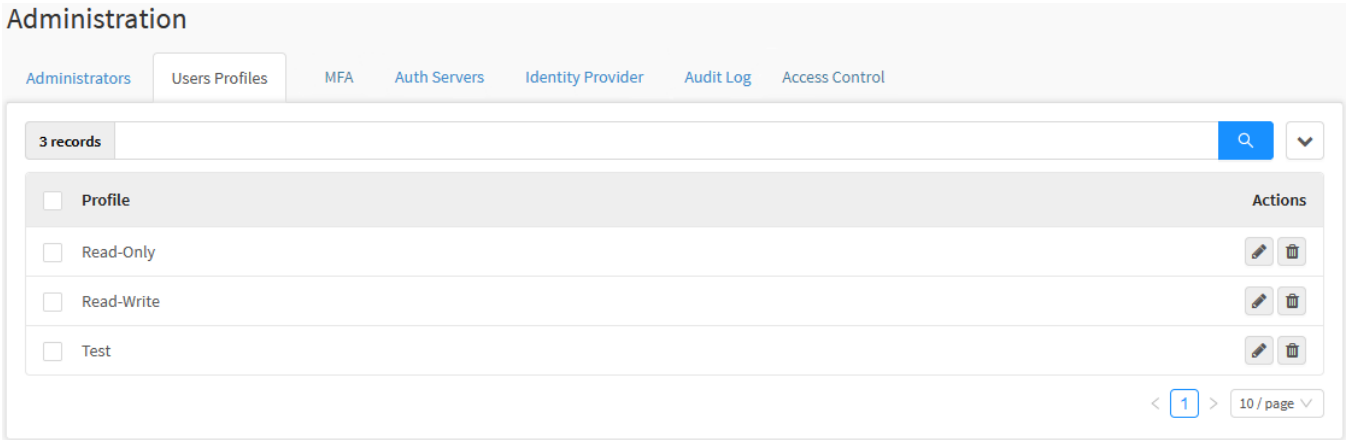
The "Users Profiles" tab consists of the columns: "Profile" and "Actions" and in addition, at the top of the screen are the search bar and the actions menu.

Click on the "Users Profiles" tab.



Users Profiles tab

The screen shown by the image below will appear:



Administration - Users Profiles

This section will cover the [Registration](#), Editing and [Removal](#) of GSM administrator profiles;

Next, we'll look at each component of this panel.

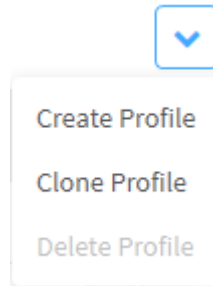
# Administration - Users Profiles - Actions Menu

At the top right of the screen we have the actions menu:



Users - Actions menu button

By clicking on this button the menu below is displayed:



*Administrators - Actions menu*

The menu consists of the following options:

- [Create Profile](#);
- [Clone Profile](#);
- [Delete Profile](#).

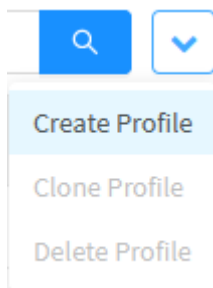
Next, each action menu option will be detailed.

# Users Profiles - Actions Menu - Create Profile

In this option it is possible to create a user profile and configure the access permissions that he will have within the system. When creating a user and linking this profile, all settings made in this session will take effect.



To create a new profile, access the actions menu [ ] and click on the "Create Profile" button.



Menu de Ações - *Create Profile*

The configuration screen for the administration profiles will appear, as shown below:

Create Profile

X

\* Name

Devices

Select

Device Groups

Select

Manager	Read	Write
- Devices	<input type="checkbox"/>	<input type="checkbox"/>
Device Manager	<input type="checkbox"/>	<input type="checkbox"/>
Device Communities	<input type="checkbox"/>	<input type="checkbox"/>
Device Templates	<input type="checkbox"/>	<input type="checkbox"/>
- Policies	<input type="checkbox"/>	<input type="checkbox"/>
Policy Packages	<input type="checkbox"/>	<input type="checkbox"/>
Policy Templates	<input type="checkbox"/>	<input type="checkbox"/>
- Users	<input type="checkbox"/>	<input type="checkbox"/>
Users	<input type="checkbox"/>	<input type="checkbox"/>

Analyzer	Read	Write
- Analysis	<input type="checkbox"/>	<input type="checkbox"/>
Network Traffic	<input type="checkbox"/>	<input type="checkbox"/>
Policy Usage	<input type="checkbox"/>	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>	<input type="checkbox"/>
Application Control	<input type="checkbox"/>	<input type="checkbox"/>
Intrusion Prevention	<input type="checkbox"/>	<input type="checkbox"/>
Threat Protection	<input type="checkbox"/>	<input type="checkbox"/>
User Behavior	<input type="checkbox"/>	<input type="checkbox"/>
- Reports	<input type="checkbox"/>	<input type="checkbox"/>



Cancel

Save

Create Profile

The “Profile” section allows you to define the permissions that the profile will control, next we will detail all the fields on this screen:

- **Name:** Administration profile name. Ex.: “Web Filter - Admins”;
- **Devices:** Allows you to select which devices these options will be applied to;
- **Device Groups:** Allows you to select to which groups of devices the options will be applied. Ex.: “Pool Web Filters”;
- **Manager:** Displays several expansive menus with sets of modules and configurations of the Blockbit GSM Manager, it is possible to control access through the checkboxes, having the following permissions: “None”, “Read Only” and finally, “Read” and “Write”. The options are:
  - **Devices:** Device Manager, Device Communities, and Device Template;
  - **Policies:** Policy Manager and Policy Templates;
  - **Users:** Users and Users Groups;
  - **Objects:** These are object types, Addresses, Services, Times, Schedules, Dictionaries and Content Types;
  - **Settings:** User menu, System, Network and Admin screens;
  - **Deploys:** Deploys Panel screen.
- **Analyzer:** Displays several expansive menus with sets of modules and configurations of the Blockbit GSM Analyzer, it is possible to control access through the checkboxes, having the following permissions: “None”, “Read Only” and finally, “Read” and “Write”. The sets are:
  - **Analysis:** Network Traffic, Policy Usage, Web Filter, Application Control, Intrusion Prevention, Threat Protection and User Behavior;
  - **Reports:** This is the reporting panel, your only option is “Reports”;
  - **Events:** If you refer to the events panel, your only option is “Events”;
  - **Loggers:** Determines access to the “Loggers” panel, which is your only option.

To define the desired permissions, select the item, expand the option using the plus  button (if necessary) and click with the mouse on the selection icon , as shown in the example below:

Create Profile



\* Name

Test

Devices

Select

Device Groups

Select

Manager	Read	Write	Analyzer	Read	Write
<div>-</div> Devices	<input type="checkbox"/>	<input type="checkbox"/>	<div>-</div> Analyzer	<input type="checkbox"/>	<input type="checkbox"/>
Inventory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Network Traffic	<input type="checkbox"/>	<input type="checkbox"/>
Communities	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Web Filter	<input type="checkbox"/>	<input type="checkbox"/>
Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Application Control	<input type="checkbox"/>	<input type="checkbox"/>
Provisioning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion Prevention	<input type="checkbox"/>	<input type="checkbox"/>
Backups	<input type="checkbox"/>	<input type="checkbox"/>	Threat Protection	<input type="checkbox"/>	<input type="checkbox"/>
<div>-</div> Policies	<input type="checkbox"/>	<input type="checkbox"/>	User Behavior	<input type="checkbox"/>	<input type="checkbox"/>
Packages	<input type="checkbox"/>	<input type="checkbox"/>	<div>-</div> Reports	<input type="checkbox"/>	<input type="checkbox"/>
Templates	<input type="checkbox"/>	<input type="checkbox"/>	Reports	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save

Create Profile - Example

Save

Cancel

Click the save [ Save ] button to save the profile, otherwise, click cancel [ Cancel ], or the [ X ] at the top right of the screen, to return to the "Profiles" tab.

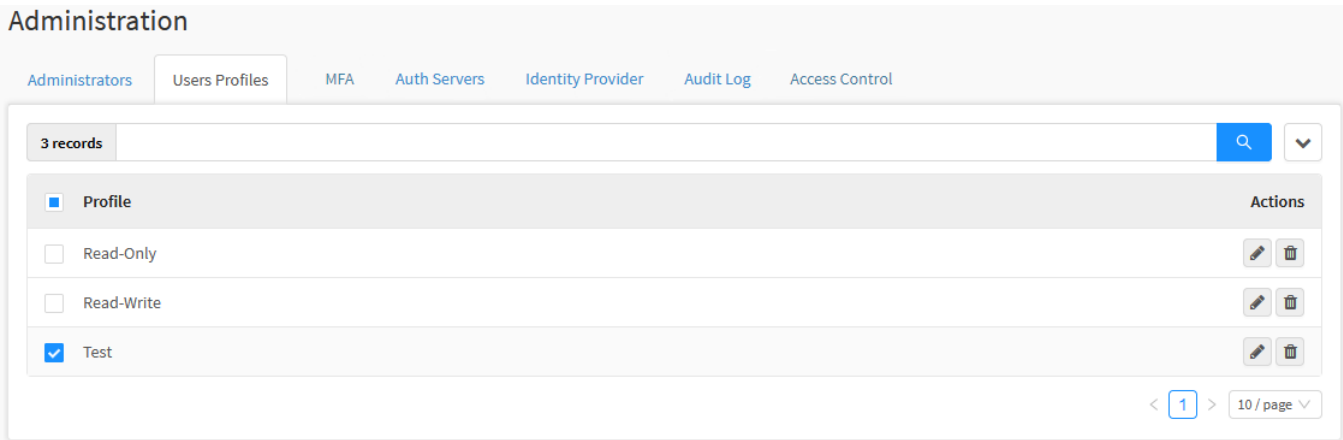
Administration profiles have been successfully created.

After creating this profile, you can link it to a specific user so that your settings are applied, for more information, see this [page](#).




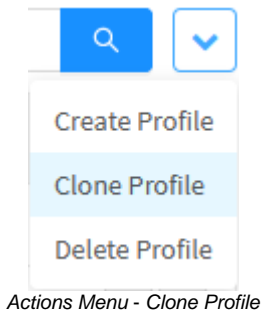
# Users Profiles - Actions Menu - Clone Profile

The “Clone Profile” button on the action menu serves to duplicate profiles that were previously selected by clicking on the checkbox. As shown below:



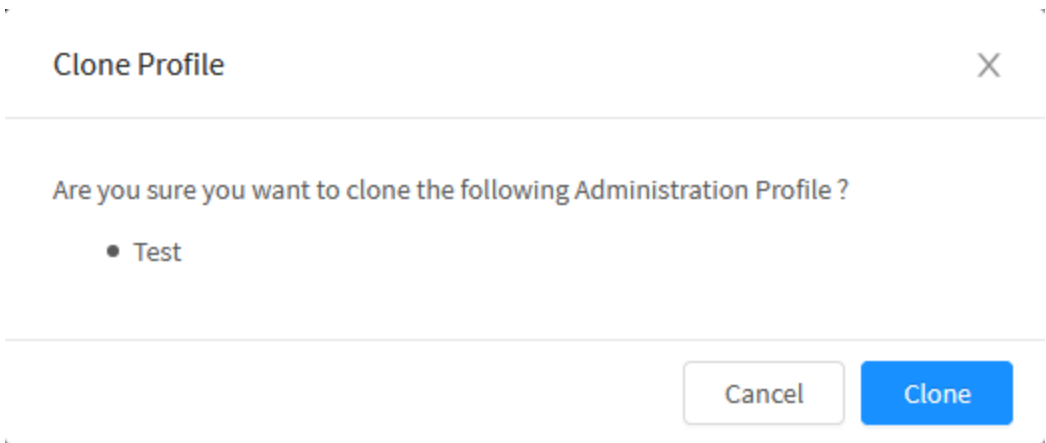
Administration - Users Profiles - Selected item

After selecting the items to be cloned, select the option in the **actions menu** [  ]:



Actions Menu - Clone Profile

A verification message will appear requesting confirmation:



Clone Profile - Cloning confirmation message

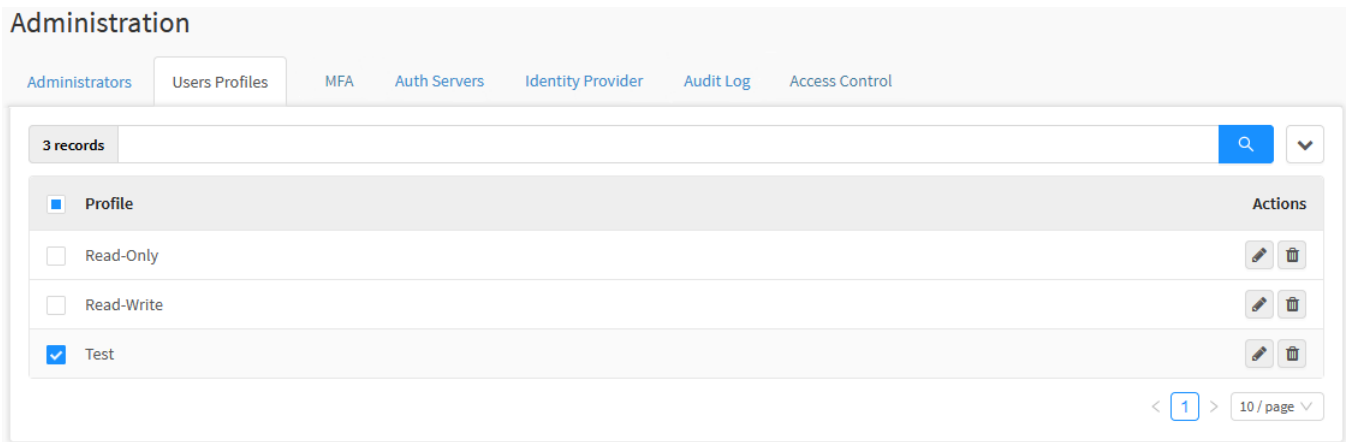
Clone

Cancel


When you click [Clone], the selected profiles will be duplicated. If you click [Cancel], this verification message will be dismissed without performing any removal.

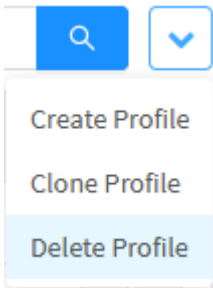
# Users Profiles - Actions Menu - Delete Profile

The “Delete Profile” button in the action menu serves to remove profiles that were previously selected by clicking on the checkbox. As shown below:



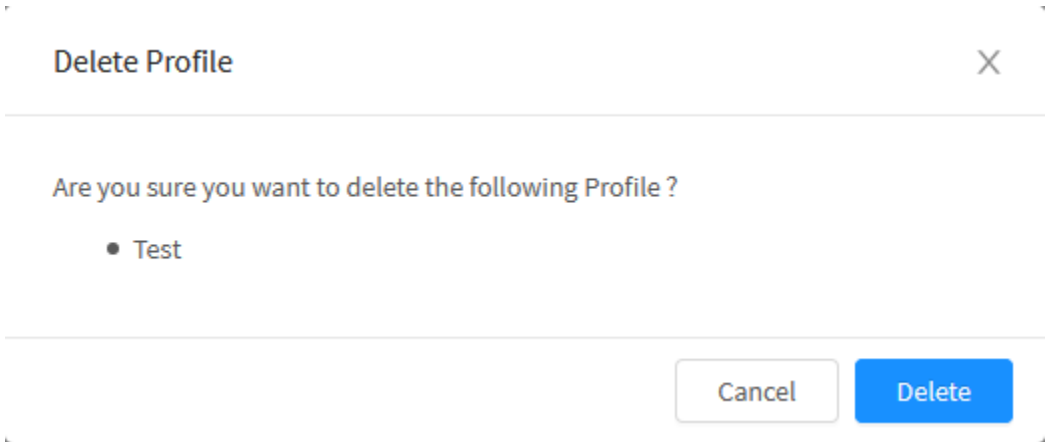
Administration - Users Profiles - Selected item

After selecting the items you want to delete, select the option in the **actions menu** [  ]:

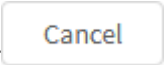


Actions Menu - Delete Profile

A verification message will appear requesting confirmation:



Delete Profile - Deletion confirmation message

A blue rectangular button with rounded corners and the word "Delete" in white text.A light gray rectangular button with rounded corners and a thin border, containing the word "Cancel" in gray text.

When you click [Delete], the selected profiles will be duplicated. If you click [Cancel], this verification message will be dismissed without performing any removal.

# Administration - Users Profiles - Columns

In the following we will explain each column of the Users Profiles tab:

Administration

Administrators

Users Profiles

MFA

Auth Servers

Identity Provider

Audit Log

Access Control

3 records

☐

Profile

Actions

☐

Read-Only

☐

Read-Write




☐

Test

< 1 >

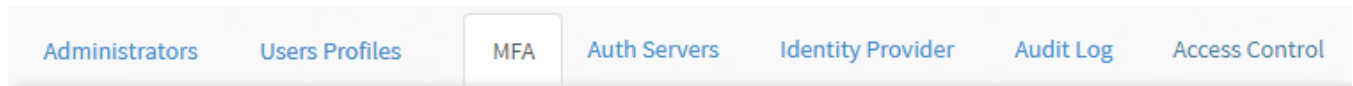
10 / page

Profiles

- **Select**- **Profile**: Displays the name of the administrator profiles created in [Create Profile](#);
- **Actions**: Provides the following essential actions:
  - **Edit**Create Profile option;
  - **Delete**Delete Profile option.

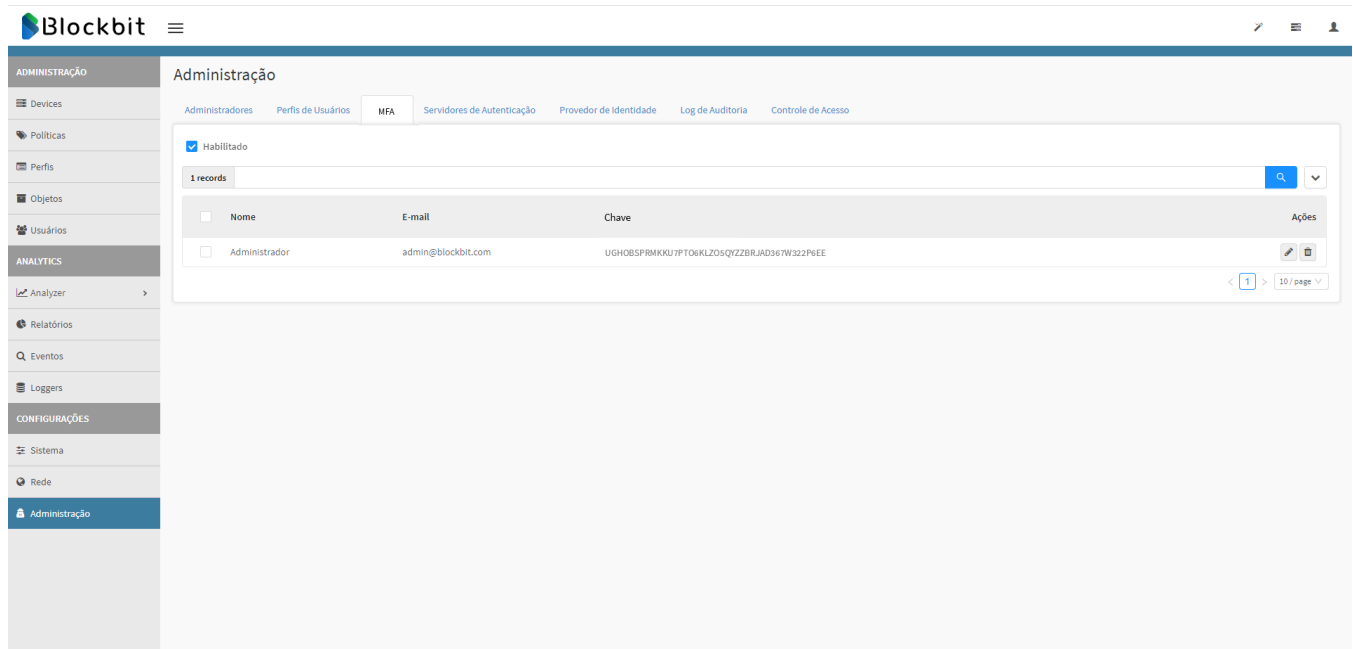
# Administration - "MFA" tab 2.5.0

The *MFA (Multi-factor Authentication)* option allows the generation of a unique key to be utilized along with the *Google Authenticator app*, for the users validation using an MFA token.




MFA (Multi-factor Authentication) tab

The following screen will be displayed:



Administration - MFA

Initially the "Enabled" field, on the upper left corner of the screen, must be marked.

After the activation of the service, a list containing all of the management users will be displayed. By clicking on the "  " button, it will be possible to select a user and generate them a key.

Add user key

Users:

de6ff4e748d@blockbit.com

de6ff4e748d@blockbit.com

fbfb4314115@blockbit.com

75f39920867@blockbit.com

edet@blockbit.com

ahm@blockbit.com



rrea@blockbit.com

Generate key

Validation key generation

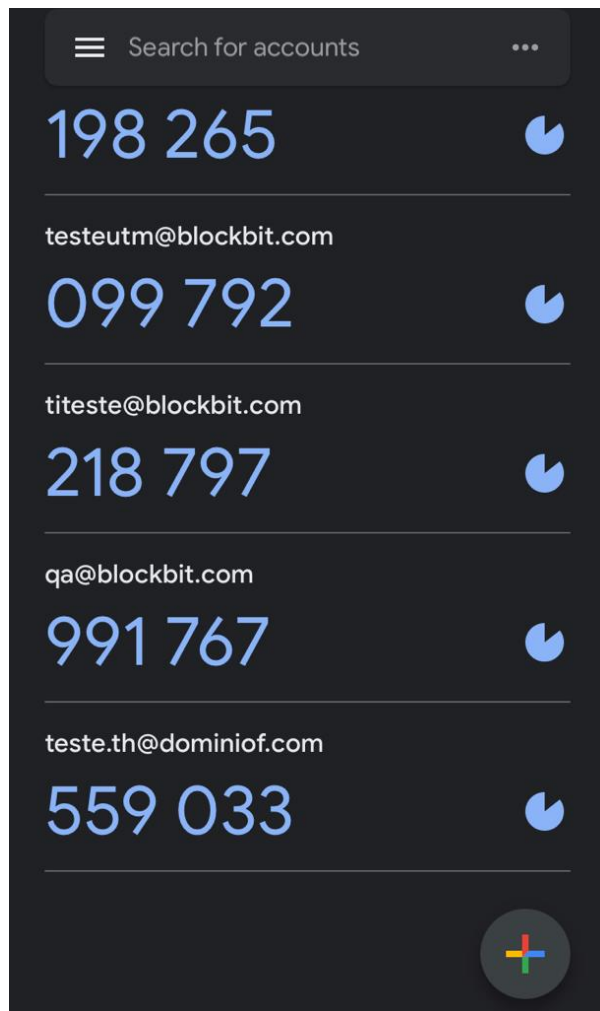
Search by user	3 items	+
Google Authenticator		
testemfa@local.net	TPZWC2G3NNCHIT5RLK03TD3X22NPKR3LIRBFF...	Copy Delete
testemfa2@labblockbit.com	BCI7T3Z6VT24AQVHKYNT2IUAAA3A2XZGCU5IBS5...	Copy Delete
teste.th@dominiof.com	ONVMLPFWMNSZZZGM52AYKZWVDOIQUKPV7VU...	Copy Delete

List of users that have an assigned validation key

By clicking the Copy [  ] or Delete [  ] buttons it's possible to copy or delete a key.

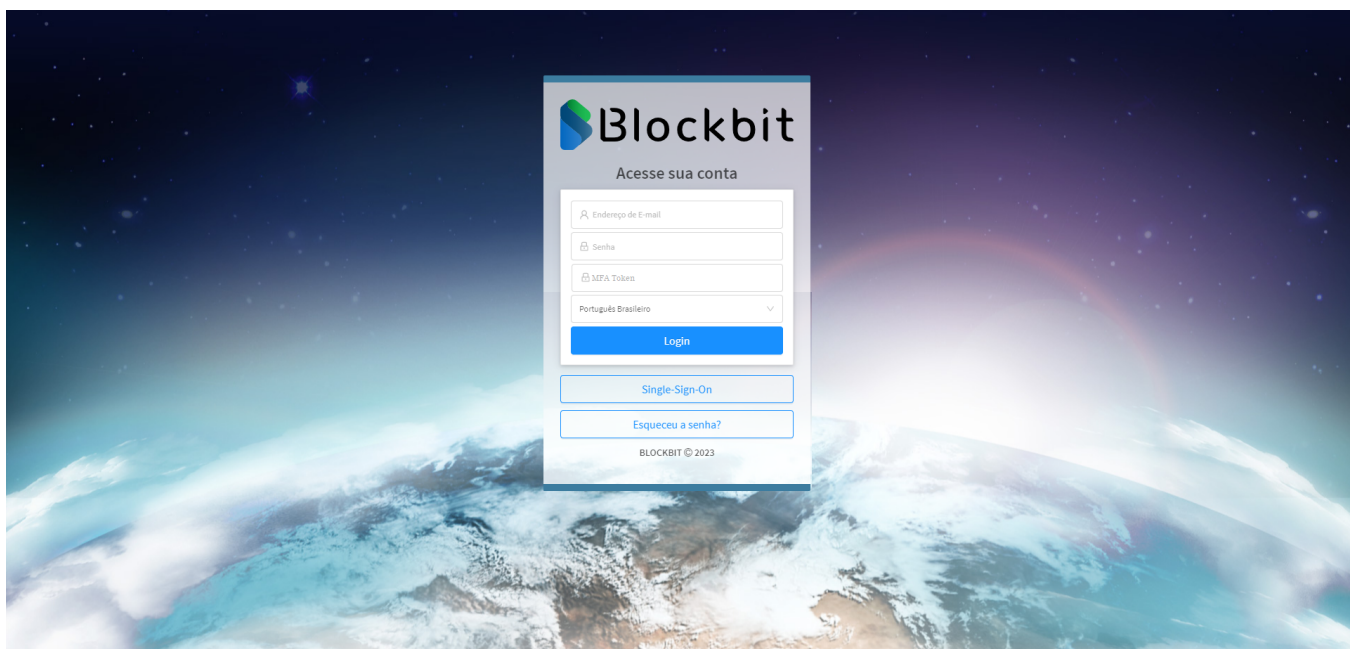
After having generated the key it's necessary to have the "Google Authenticator" app on another device (a smartphone, or notebook). On the App, click the "+" option "Insert validation key" and insert the key generated on the GSM for validation. Select the "time-based key" type.

By doing so, a six-digit validation token will be issued for the user.






Google Authenticator - Access Tokens

After having obtained the token, access the authentication portal and log in:





## Login screen

-  *Login*: Insert the username/e-mail.
-  *Password*: On this field, use the password that's been registered for this user.
-  *MFA Token*: On this field the MFA Token, that was obtained from the google authenticator app, must be inserted.

After filling these fields, click on "Login".

About the *Tokens*:

The *tokens* are meant to be used only once. The user can use up to 3 *tokens*, (the current, the previous and the next ones) upon the attempt to use another *token*, the user becomes invalid. In case the *token* is typed in wrongly thrice, the user becomes invalid for 30 seconds.

It's important to remember that the *token* is changed often, so when logging in, one must consult the token on the *Google Authenticator App*.

Next, we will analyze every component on this panel.

# Administration - "Auth Servers" tab

In the "Auth Servers" tab, it is possible to register servers with the function of allowing authentication of administrator profile users with remote login.

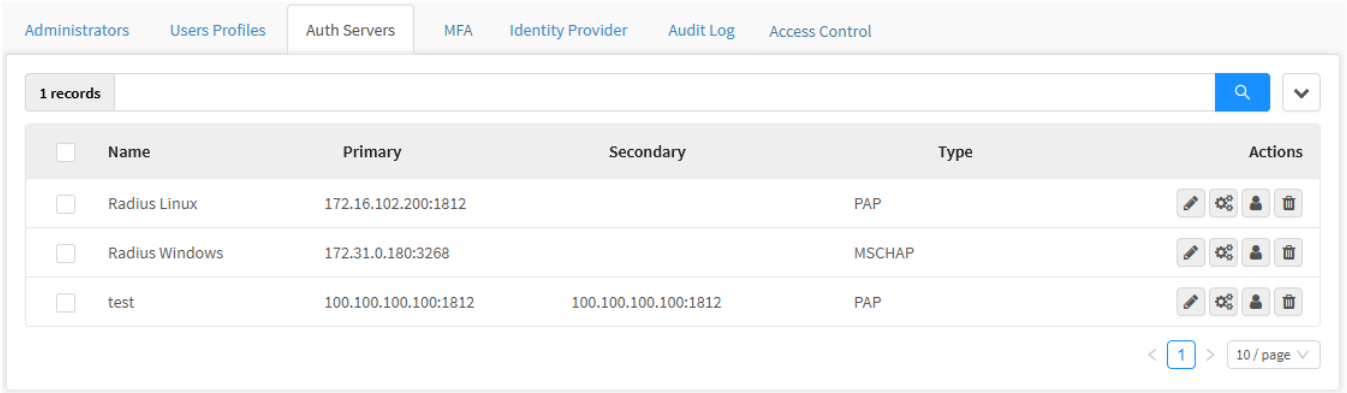
The "Auth Servers" tab consists of five columns: "Server Name", "Primary Server", "Secondary Server", "Authentication Type" and "Actions" and in addition, at the top of the screen are the search bar and the actions menu.

Click on the "Servers" tab.



Auth Servers Tab

The screen shown by the image below will appear:



Administration - Auth Servers Tab

This section will cover:

- Registration and Editing of Radius and Ldap servers;
- Removing the servers;
- How to test that a user's authentication on the server is working.

Next, we'll look at each component of this panel.

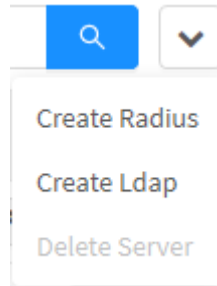
# Administration - Auth Servers - Actions Menu

At the top right of the screen we have the actions menu:



Users - Actions menu button

By clicking on this button the menu below is displayed:



Administration - Actions menu


The menu consists of the following options:


- [Create Radius](#);
- [Create Ldap](#);
- [Delete Server](#).

Next, each action menu option will be detailed.

# Create Radius

In this form it is possible to create a new remote RADIUS server.

 For more in-depth information regarding the characteristics of a RADIUS server, see this UTM manual [page](#).

When accessing the **actions menu** [  ] and clicking on the option "Create Radius", the form "Create Server" will appear, as illustrated by the image below.

Create Server

\* Server Name

Server Name

\* Primary Server

IP

\* Port

Port

\* Secret

Secret

Secondary Server

IP

Port

Port

Secret

Secret

\* Authentication Type

NAS IP Addresses

Select

Cancel




Save

Administration – Create Radius

Next, we will detail each field of this form.:

- **Server Name:** Defines the server name for identification, this name will be displayed in the [columns](#). Ex.: "Radius Server";
- **Primary Server:** Determines the IP address of the primary Radius authentication server;
- **Port:** Defines the port used by the primary server. Ex.: 10;
- **Secret:** Determines the pre-shared key (Pre-Shared Key or PSK). This is the secret shared between the authentication server "Radius" and the account server "Blockbit UTM". Ex.: *blockbit.utm*;
- **Secondary Server:** Sets the IP address of the secondary Radius authentication server;
- **Port:** Determines the port used by the secondary server;
- **Secret:** Defines the pre-shared key (Pre-Shared Key or PSK). Secret shared between the "Radius" authentication server and the "Blockbit UTM" account server. Ex.: *blockbit.utm*;
- **Authentication Type:** Determines which type of authentication protocol will be used, the available options are:
  - MSCHAP;
  - CHAP;
  - PAP.
- **NAS IP Address:** This is the IP address of devices capable of receiving requests from authentication clients and forwarding the request to the network's Radius server: Wireless Routers, Switches or your own UTM Device.

A blue rectangular button with the word "Save" in white text.A light gray rectangular button with the word "Cancel" in blue text.

Click the [  ] button to save all changes, otherwise click [  ] or the [  ] at the top right of the screen to close the window.




Server saved successfully

*Server saved successfully*

Note that despite having created the RADIUS server, there is no self-registration of the administrator users, for that it is necessary to access the administrator user screen and create this user, pointing out which server he belongs to.

## Create LDAP



When accessing the **actions menu** [  ] and clicking on the “Create LDAP” option, the “Create Server LDAP” form will appear, as illustrated by the image below.

Create Server Ldap

X

Settings

User Filter

\* Name

☐ SSL

\* Primary Server

\* Port

\* Login

\* Password

Secondary Server

Port

Login

Password

Cancel

Save

## Administration – Create Server LDAP

This window is made up of the tabs:

- *Settings;*
- *User Filter.*

Next, we will analyze all the components of each of these side flaps.

## Settings

The settings tab is made up of the following fields:

## Settings

## User Filter

## \* Name

Name

☐ SSL

## \* Primary Server

## \* Port

## \* Login

## \* Password

IP

Login

## Secondary Server

## Port

## Login

## Password

IP

Login

Cancel

Save

## Administration – Create Server LDAP

- **Name:** Defines a name for the sync connection, this name will be displayed in the [columns](#). Ex.: *Primary DC*;
- **SSL** ☒: If the service is running on SSL, enable this checkbox;
- **Primary Server:** Sets the primary IP address of the domain controller. Ex.: 172.16.102.191;
- **Port:** Determines the port for connecting to the domain controller. Ex.: 389;
- **Login:** Defines a Windows server user with rights to search the LDAP database, usually a member of the administrators group. Ex: "administrador@dominioc.com"
- **Password:** Determines the user's password;
- **Secondary Server:** Sets the secondary IP address of the domain controller. Ex.: 172.16.102.192;
- **Port:** Determines the port for connecting to the domain controller. Ex.: 389;
- **Login:** Defines a Windows server user with rights to search the LDAP database, usually a member of the administrators group. Ex: "administrador@dominioc.com"
- **Password:** Determines the user's password.

To continue configuring, access the next side tab: [User Filter](#).

## User Filter

In this tab, the fields referring to the user search base and their respective filters in the LDAP base of the Windows AD server are configured.

Create Server Ldap

X

Settings

User Filter

Base

DC=dominiof,DC=com

Filter

(&(objectclass=user)(objectclass=person)(!(objectclass=computer)))

Login Attribute

sAMAccountName

Cancel

Save

Authentication – Add Windows Server – User filter

Configure the "Base", "Filter" and "Login Attribute" fields, according to the LDAP database data of the respective Windows server.



For the configuration of a Windows AD server with LDAP, it is necessary to manually change the fields to have the values below:

- **Filter:** (&(objectclass=user)(objectclass=person)(!(objectclass=computer)))
- **Attribute login:** userPrincipalName

Save

Cancel



Click the [ Save ] button to save all changes, otherwise click [ Cancel ] or the [ X ] at the top right of the screen to close the window.



Server saved successfully

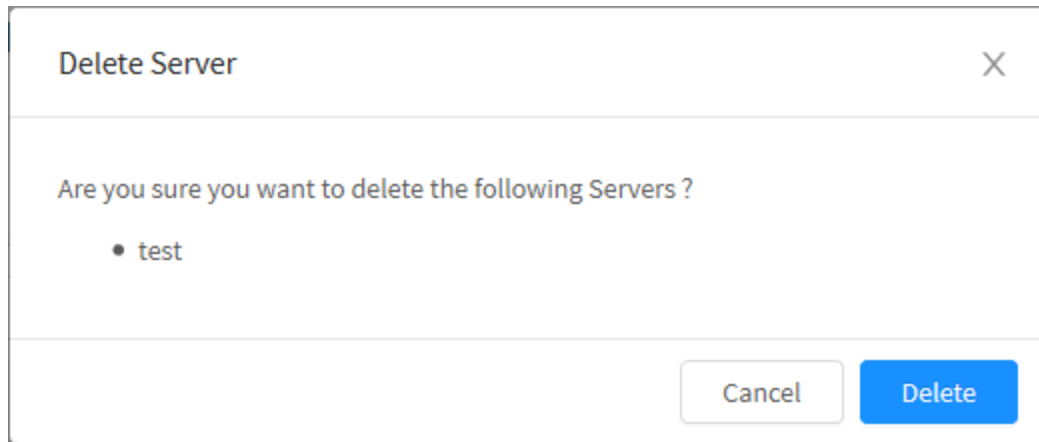
Server successfully saved

Note that despite having created the LDAP server, there is no self-registration of administrator users, for that it is necessary to access [Administration - "Users" tab](#) and create this user, pointing out which server he belongs to.



## Delete Server

The “Delete Server” button in the action menu serves to remove servers that were previously selected by clicking on the checkbox. After selecting this option, a verification message will appear requesting confirmation.



*Delete Server*

















By clicking [  ], the selected servers will be removed. If you click [  ], this verification message will be dismissed without performing any removal.

# Administration - Auth Server - Columns

Below we will detail each column of the Servers tab:






Administrators   Users Profiles   Auth Servers   MFA   Identity Provider   Audit Log   Access Control

1 records

<input type="checkbox"/>	Name	Primary	Secondary	Type	Actions
<input type="checkbox"/>	Server LDAP	172.31.0.180:3268		LDAP	   
<input type="checkbox"/>	Radius Linux	172.16.102.200:1812		RADIUS	   
<input type="checkbox"/>	Radius Windows	172.31.0.180:3268		RADIUS	   
<input type="checkbox"/>	test	100.100.100.100:1812	100.100.100.100:1812	LDAP	   

< 1 > 10 / page

Administration - Auth Servers Tab

- **Select**: Allows you to select one or more servers;
- **Primary**: Sets the IP address of the primary server;
- **Secondary**: Sets the IP address of the secondary server;
- **Type**: Displays the type chosen when creating the server, which can be LDAP or RADIUS;
- **Actions**: Provides the following essential functions:
  - **Edit**: Allows you to edit one of the servers created in the [Create Radius](#) or [Create LDAP](#) option in the actions menu;
  - **Test Connection**: Allows you to test the connectivity of a server;
  - **Test Authentication**: Allows you to test if a user's authentication on the server is occurring correctly, check this [page](#) for more information;
  - **Delete**: Allows you to [delete](#) a server.

# Server - Test Authentication

This screen is for testing whether authentication is working correctly.

When clicking on the **Test Authentication**  button the screen below will be displayed:

Test Authentication

\* User


\* Password

Cancel

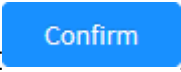
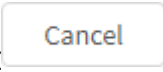
Confirm

Test Authentication

- **User:** Enter the user;
- **Password:** Enter the user's password.



The user that can be used in this panel must have been added in the User tab with the type "Remote", for more information check this [page](#).

To test authentication, click  to test authentication or click  to close the window.

# Administration - "Identity Provider" tab

This tab contains the necessary resources to configure the integration with the SAML identity provider (Security Assertion Markup Language), it is an XML-based opensource authentication protocol for authentication between an identity provider and a service provider (service provider). This feature is a single sign on standard used to integrate multiple web authentication (http) applications with the GSM. It works by allowing the user to enter their login and password for an external identity provider instead of performing the standard login via GSM.

When a user accesses a service provider application (in this case, the GSM), the identity provider requests the user's login and password to confirm his identity, if the credentials are correct, he sends an authentication statement (this being predetermined by SAML) to the service provider so that it can define the access control of the user who made the request.

The identity provider is a trusted third-party application that generates, stores and manages user identification data, it transmits a SAML-based authenticity assertion when this user's credential is validated, in addition, it is able to provide authentication services to multiple service provider, allowing its users to log in to any application that is compatible with this technology.

When enabling this option, the GSM will act as a service provider, allowing the user to use the identity provider to log in and also offering the necessary mechanisms for integration with the selected identity provider.

SAML does not specify which authentication method will be used in the identity provider, and it is possible to use multi-factor authentication, RADIUS, LDAP, Active Directory and etc, according to the selected provider.

The advantages of this feature are:

- Prevents the user from having to remember multiple passwords to access different applications;
- Thanks to the system being outsourced and based on a reliable server, security in the login process is improved;
- Because it depends on less access, it reduces attack vectors where an exploit can be applied.

To access these features, click on the "Identity Provider" tab:



Identity Provider Tab

The following screen will be displayed:

The screenshot shows the 'Identity Provider' configuration page. It has a left sidebar with a 'Service Provider' section and a main content area for the 'Identity Provider'. The 'Service Provider' section includes fields for 'Enabled' (checked), 'Service Name' (blockbit\_saml), 'Service Description' (Blockbit SAML), 'Certificate' (gsmkelvin), 'Base URL' (https://172.31.190.97), 'Base URL Login' (https://172.31.190.97/saml/module.php/saml/sp/metadata.php/saml-sp), 'Base URL Logout' (https://172.31.190.97/saml/module.php/saml/sp/saml2-logout.php/saml-sp), and 'Base URL Metadata' (https://172.31.190.97/saml/module.php/saml/sp/metadata.php/saml-sp). The 'Identity Provider' section includes fields for 'Entity ID' (https://172.31.0.240/simplesaml/saml2/idp/metadata.php), 'Single Sign On Service URL' (https://172.31.0.240/simplesaml/saml2/idp/SSOService.php), 'Single Log Out Service URL' (https://172.31.0.240/simplesaml/saml2/idp/SingleLogoutService.php), 'SSO Binding' (Post, Redirect), 'SLO Binding' (Post, Redirect), 'Certificate' (MIIDJ/CAg4CAQMwDQYJKoZIhvcNAQENBQAwWTELMAkGA1UEBhMCQlxxCzAJBgNVBAGMAINQMqSwCQYDVQQHDAJUDELMAKGA1UECgwCQkxvDQAKBgNVBAQsMAARFjEVENBGA1UEAwwMU0FNTF95T09ULUNBMBA4DTIwMTYyMjE1MDAwDTMv), 'Name ID Format' (nameid-format:emailAddress (1.1)), 'Username Attribute' (name), 'Email Attribute' (mail), 'Profile Attribute' (oiAuthBlock), 'GSM Users' Profiles' (Read-Write), 'Persist User' (checked), and 'Auditor' (checked).

Administration - Identity Provider

This screen is made up of panels:

- *Service Provider;*
- *Identity Provider.*

Next, we will analyze the components of each of these panels.

# Identity Provider - Service Provider

This panel contains the necessary resources to configure GSM as a Service Provider. Next we will detail how to configure this form:

Service Provider

☒ SAML SSO Enabled

\* Service Name

gsm23

\* Service Description

Service Provider GSM23

\* Certificate

gsm23.blockbit.com

\* Base URL

https://172.31.240.23

Base URL Login

https://172.31.240.23/saml/module.php/saml/sp/metadata.php/saml-sp

Base URL Logout

https://172.31.240.23/saml/module.php/saml/sp/saml2-logout.php/saml-sp

Base URL Metadata

https://172.31.240.23/saml/module.php/saml/sp/metadata.php/saml-sp

Identity Provider - Service Provider

- **SAML SSO Enabled** ☒: By selecting this check box, the system enables SAML-based Single Sign On;
- **Service Name**: Defines the name of the Service that will be passed to the Identity Provider;






The service name will be used in requests from the identity provider and will be sent by URL, so it will be necessary to follow the syntax, follow the accepted characters:


ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789-.\_~!/?#[]@!\$&'()\*+,-;=

For more information, see [RFC 3986](#).

- **Service Description**: Determines a description to facilitate identification of the service;

- **Certificate:** This option allows the user to generate a self-signed certificate or import an external certificate from the Identity Provider, which can be public or private. This field contains the following options:
  - **Add Certificate** []: This button allows you to add a new certificate automatically, for more information about the certificate window, see this [page](#);
  - **Import Certificate** []: The button allows certificates generated by the Identity Provider to be imported, for more information on the import window, see this [page](#);
  - **Export Certificate** []: This button allows you to download the certificate.
- **URL Base:** Determines the base URL of the service that will be redirected by the Identity Provider, this field accepts IP or FQDN. When changing the URL base information, all fields below will receive information regarding the service provider;
- **URL Base Login:** In this field, the URL of the Identity Provider Login service is added, it is used to return messages, this URL is automatically generated using the information from the URL Base as a reference;
- **URL Base Logout:** In this field, the URL of the Logout service that the Identity Provider will use to return messages is determined, this URL is automatically generated using the information from the URL Base as a reference;
- **URL Base Metadata:** This field defines the URL of the Metadata service that the Identity Provider will use if it is necessary to import the information from above about the Service Provider, this URL is automatically generated using the information from the URL Base as a reference.



Click on the [] button to export all metadata in XML format, making it possible to impose this file on the Identity Provider interface, this information is necessary to federate the service server (GSM) and close the communication with the Identity Provider.

For more information about the certificate import window, see this [page](#).

For details on configuring the Identity Provider panel, see this [page](#).

# Identity Provider - Service Provider - Add Certificate

The resources in this window allow the administrator to configure his own certification authority, which is a simple and practical way of obtaining the certificate that will be used to ensure reliability in accessing the solution's resources.

The purpose of a certification authority is to confirm the ownership of the certificates, confirming that the certificate received when accessing a particular website or address actually belongs to the entity that is providing it. This is what ensures that you are even securely accessing SSL / HTTPS websites and addresses.



It is necessary to configure a CA in this tab to be able to create a SAML identity provider, for more information see this [page](#).

Add Certificate

X

\* Country

BR

\* State

SP

\* City

Sao Paulo

\* Organization

gsm24 Blockbit

\* E-mail

admin@blockbit.com

\* Organizational Unit

QA Blockbit

\* Expires in (years)

10

\* Hostname

gsm24.blockbit.com

\* Key Size

2048

Cancel

Save

System - Backups

Next we will detail the fields on this form:

- **Country:** Determines the country. Ex.: *US*;
- **State:** Sets the state. Ex.: *New York*;
- **City:** Determines the city. Ex.: *New York*;
- **Organization:** Defines the company name. Ex.: *Blockbit*;
- **E-mail:** Determines the administrator's email. Ex.: [admin@blockbit.com](mailto:admin@blockbit.com);
- **Organizational Unit:** Defines the department. Ex.: *QA*;
- **Expires (years):** Determines the validity time of the certificate. Ex.: *10 years*;
- **Hostname:** Defines the CA Hostname. Ex.: [admin@blockbit.com](mailto:admin@blockbit.com);
- **Keysize:** Defines the size that the CA key will have. Ex.: *2048*.



SaveCancel

When finishing the configuration, click [  ] to save or [  ] to close this window.



Saving a CA requires the server to generate a new certification body. *This action requires reinstallation of the new CA on all devices on the network.*



If you want to recreate the CA, you must also re-do the Server Certificate, this procedure requires the installation of the new CA on all devices on the network. *Download the CA and reinstall on all workstations. Remembering that to validate the new CA you must RESTART the server.*

Next, let's look at the [Import Certificate](#) button.

# Identity Provider - Service Provider - Import Certificate

This window allows the addition of a self-signed certificate, which can be a public or private key, then we will analyze the components of the form:

Add Certificate

\* Certificate Type ☒ (.crt/key) ☐ (.pem)

\* Certificate - Public Key (.crt)

Paste Here

\* Certificate - Private Key (.key)

Paste Here

Cancel OK

Identity Provider - Add Certificate

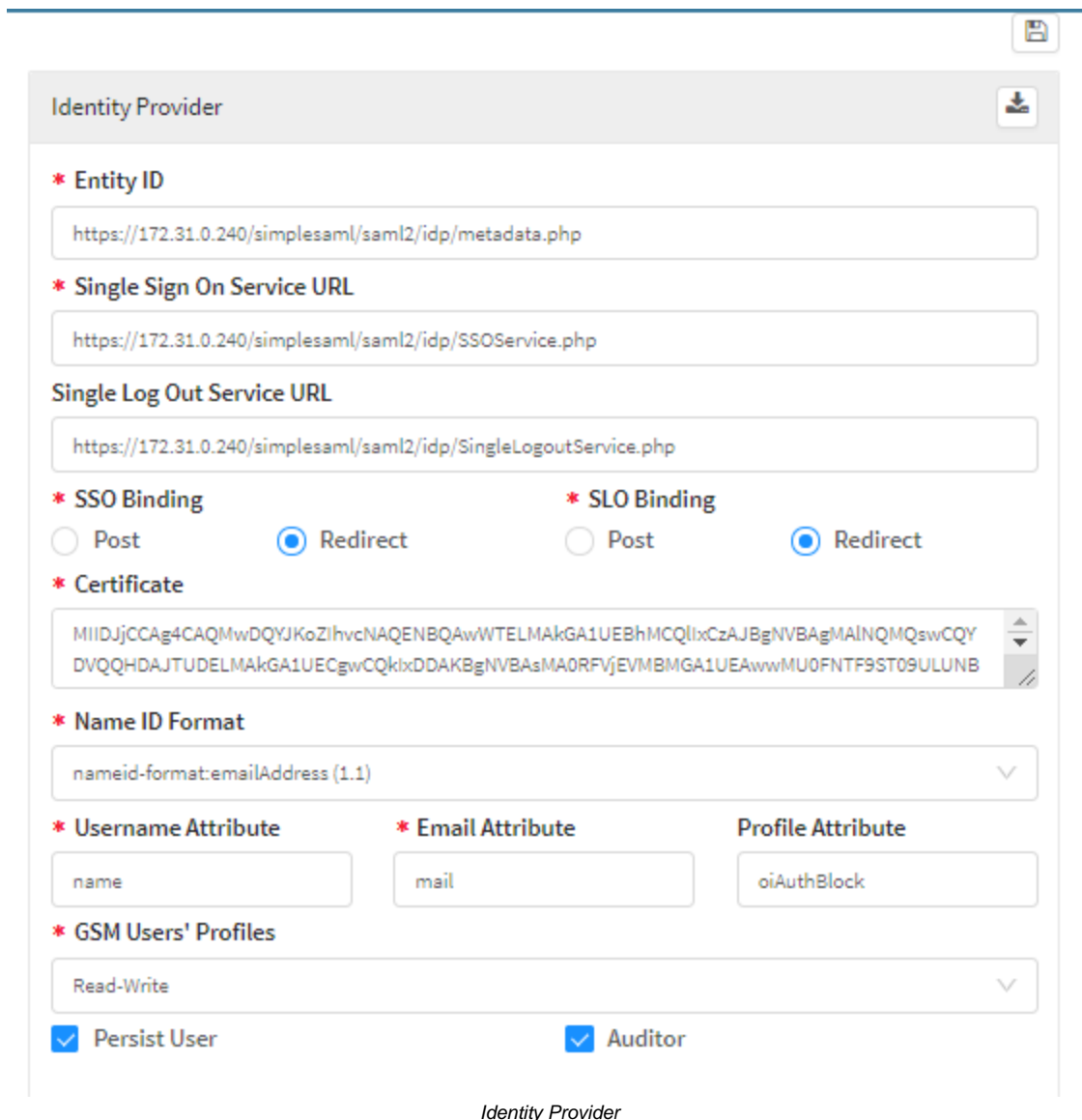
- **Certificate Type:** This option determines the type of certificate that will be used. The selection determines which fields will be displayed on the form, the options are:
  - **(.crt/key)** ☒: In case the (.crt/key) option is enabled the Certificate fields- Public Key (.crt) and Certificate - Private Key (.key) will be displayed;
  - **(.pem)** ☐: If the option (.pem) is enabled, the Certificate field (.pem) will be displayed.
- **Certificate - Public Key (.crt):** This field allows the addition of the public key of the certificate (.crt);
- **Certificate - Private Key (.key):** This field allows the addition of the certificate's private key (.key);
- **Certificate (.pem):** If you have selected the option (.pem), just add the certificate in this field.

For more information on the Service Provider panel form, see this [page](#);

To access information about the Identity Provider panel, see this [page](#).

# Identity Provider - Identity Provider

In this section, you will find the resources needed to setup the GSM synchrony with the *Identity Provider*. Next, we will provide details on how to configure this form:



The screenshot shows a web form titled "Identity Provider" with a download icon in the top right corner. The form contains several fields and options:

- \* Entity ID**: A text input field containing the URL `https://172.31.0.240/simplesaml/saml2/idp/metadata.php`.
- \* Single Sign On Service URL**: A text input field containing the URL `https://172.31.0.240/simplesaml/saml2/idp/SSOService.php`.
- Single Log Out Service URL**: A text input field containing the URL `https://172.31.0.240/simplesaml/saml2/idp/SingleLogoutService.php`.
- \* SSO Binding**: Two radio button options: ☐ Post and ☒ Redirect.
- \* SLO Binding**: Two radio button options: ☐ Post and ☒ Redirect.
- \* Certificate**: A text area containing a long alphanumeric string: `MIIDJjCCAg4CAQMwDQYJKoZIhvcNAQENBQAwWTElMAkGA1UEBhMCQlIx CzAJBgNVBAGMAINQMqswCQYDVQQHDAJUDELMAkGA1UECgwCQklxDDAKBgNVBAAsMA0RFVjEVMBMGA1UEAwwMU0FNTF9ST09ULUNB`.
- \* Name ID Format**: A dropdown menu showing `nameid-format:emailAddress (1.1)`.
- \* Username Attribute**: A text input field containing `name`.
- \* Email Attribute**: A text input field containing `mail`.
- Profile Attribute**: A text input field containing `oiAuthBlock`.
- \* GSM Users' Profiles**: A dropdown menu showing `Read-Write`.
- Persist User**: A checked checkbox.
- Auditor**: A checked checkbox.

Below the form, the text "Identity Provider" is centered.

- **Entity ID**: Defines the URL that will be used to make the communication and set the *Identity Provider* up. This field is mandatory;
- **Single Sign On Service URL**: Determines the Single Sign On URL that will be used in the GSM login by the Identity Provider. *This field is required*;
- **Single Log Out Service URL**: Defines the GSM Single Log Out URL by the Identity Provider. This field is not mandatory. When adding some information in this field, the SLO Binding option is enabled;



Note that some identity providers do not require the configuration of the Logout service.

- **SSO Binding**: Defines which bind method will be used by HTTP requests for the Login service, which can be:
  - **Post** ☒: When selecting this option, the POST method will be used, transferring the Login request through the body of HTTP;
  - **Redirect** ☐: When selecting this option, the GET method will be used, transferring the Login request by URL.
- **SLO Binding**: For this option to be enabled, it is necessary to complete the field Single Log Out Service URL. *This option defines which bind method will be used by HTTP requests for the Logout service, which can be:*

- **Post** [ ☐ ]: When selecting this option, the POST method will be used, transferring the Login request through the body of HTTP;
- **Redirect** [ ☒ ]: When selecting this option, the GET method will be used, transferring the Login request by URL.



**ATTENTION:** The fields regarding Binding must comply with the requirements of the Identity Provider, otherwise the service will not work. For that, analyze the XML that is being imported, to check which Binding method is necessary, if it is not possible to access the Identity Provider, it is advisable to reassess whether the selection in the SSO Binding configuration is correct.


- **Certificate:** In this field, the certificate generated by the Identity Provider must be pasted. Its function is to validate the assertions of the Identity Provider;
- **Named ID Format:** This checkbox defines what will be the formatting of Name ID that will be used by SAML. The Name ID determines which information is a priority in the login process, this is changed according to the XML import, each Identity Provider supports a version of Name ID Format, so select the version indicated for your provider;



**ATTENTION:** The Name ID Format must be in accordance with the requirements of the Identity Provider, otherwise the service will not work. To do so, select the option required by your provider.

- **Username Attribute:** Defines the Attribute of the XML document that will represent the User Name, this data is used to create the user's session in GSM when login via SAML. *This attribute must be copied from the Identity Provider;*
- **Email Attribute:** Determines the Attribute of the XML document that will represent the user's Email, this data is used to create the user's session in GSM when login via SAML. *This attribute must be copied from the Identity Provider;*
- **Profile Attribute:** Determines the Attribute of the XML document that will represent the user's Profile, this data is used to create the user's session in GSM when login via SAML. *This attribute must be copied from the Identity Provider;*
- **GSM Users' Profile :** This field defines which profile of default permissions will be used when the authenticated user accesses GSM, the items in this checkbox are created in the User Profiles tab, for more information, see this [page](#);
- **Persist User** [ ☐ ]: When enabling this option, the user's session persistence in the system will be activated, this option defines if when the user logs out he will be removed from the [Administrators](#) tab, if it is disabled, when logging out the user will also be removed from GSM, in case enabled, the user will continue to be recorded on the GSM even after Logout. By default, this option is disabled;
- **Audit User** [ ☐ ]: If this option is enabled, when authenticating the user will have an auditor's permission, a user with this permission will be able to deploy, otherwise, he will only be able to view them. By default, this option is disabled.



Click on the [  ] button to import the metadata in XML format, making it possible to use the settings provided in the Identity Provider interface. When importing XML via this button, by default the information in the Entity ID, Single Sign On Service URL, Single Log Out Service URL (when supported by Identity Provider), SSO and SLO Binding, Certificate and Name ID fields is auto-completed Format.

For more information about the Service Provider panel form, see this [page](#);

For more information about SAML, see this [page](#).

# Administration - "Audit Log" tab

In the "Audit Log" tab, we see the Activity Audit screen:

AdministratorsUsers ProfilesMFAuth ServersIdentity ProviderAudit LogAccess Control

94 records

Date	User	Interface	Activity	IP	Actions
2019-10-04 13:37:44	admin	settings-system	save	172.16.100.144	<div></div>
2019-10-01 15:46:40	admin	settings-admin	save	172.16.100.144	<div></div>
2019-09-26 14:26:40	admin	policy-templates	delete	172.31.250.11	<div></div>
2019-09-26 14:24:45	admin	policy-templates	delete	172.31.250.11	<div></div>
2019-09-26 14:24:28	admin	policy-templates	update	172.31.250.11	<div></div>
2019-09-26 14:23:44	admin	policy-templates	save	172.31.250.11	<div></div>
2019-09-26 14:23:13	admin	policy-templates	save	172.31.250.11	<div></div>
2019-09-26 14:21:40	admin	policy-templates	update	172.31.250.11	<div></div>
2019-09-26 14:19:07	admin	policy-templates	update	172.31.250.11	<div></div>
2019-09-26 14:13:55	admin	policy-manager	edit	172.31.250.11	<div></div>

<

1

2

3

4

5

...



10

>


10 / page

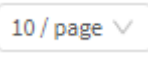
Audit Log

At the top of the screen we have the following fields:

- Search bar:** In this bar it is possible to type keywords and perform a search. To perform a search, click the search button .
- Calendário** : The calendar allows you to make more precise searches taking into account time requirements, the options allowed are: All (Considers all options), By Date (Searches specifically on a date), By Period (Searches specifically between a period), Today, Yesterday (Yesterday), Last 7 Days, Last 30 Days, This Month (Last Month) and Last Month (Last Month). In some options, a calendar will appear allowing the selection of the desired dates;

Below the search fields, the following information is displayed:

- Date:** Demonstrates the date and time when the activities were carried out. Ex.: "08/10/2018 18:22:26";
- User:** Determines which user was responsible for performing the action that will be listed later. Ex.: "admin";
- Interface:** Displays which interface was accessed by the previously mentioned user. Ex.: "Settings-System";
- Activity:** Determines what activity the user performed on the system. Ex.: "update";
- IP:** This is the IP address of the user who performed the registered action; Ex.: "172.16.100.144";
- Actions:** It is the record of what activity was performed on the previously mentioned interface. When clicking on the **Audit View**  button, more information about the actions taken by the user is displayed, see this [page](#) for more information.

At the bottom of the screen, the **Results display**  button: Allows you to determine how many results will be displayed per page, the possibilities are: 10, 20, 30, 40, 50, 100, 500;


It's important to notice that with the Virtual Domains on, the displayed information will be only regarding one's own domain, with no further access to other Virtual Domains.

For more information on (VDOMs), please access this [page](#).

Next, we will analyze the *Audit View*  button.

# Audit View

This screen has the function of showing all the actions taken by the user.

When clicking on the **Audit View**  button, the following screen will be displayed:



To exit this window, just click on , or on the  at the top right of the screen to return to the previous window.

# Administration - "Access Control" tab

In Access Control it is possible to create policies that restrict access to the GSM's management interface, in order to make sure that only specific IPs can access said interface.

Administration

Administrators

Users Profiles

MFA

Auth Servers

Identity Provider

Audit Log

Access Control

2 records

☐

IP Address

☐

192.168.254.50

☐

10.0.0.0/8

Actions

< 1 >

10 / page

Access Control

In this section it is possible to control the users able to access the GSM's control through IP attribution or the Allowed list.



# GSM - CLI - COMMAND LINE INTERFACE

The Blockbit GSM provides a Command Line Interface (CLI) console feature that enables the administrator to execute administration and troubleshooting commands for the main system services.

To run the configuration, you need an SSH client and console. The recommended minimum applications are:

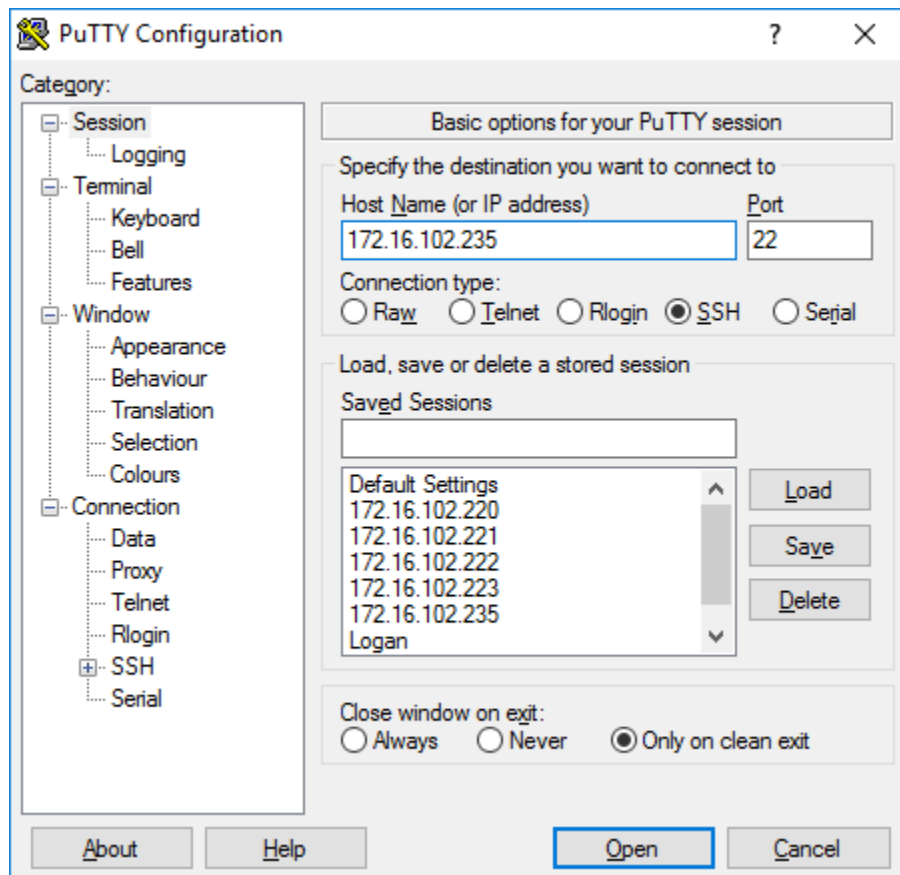
- *PUTTY*; or
- *CygWin*; or
- *Mobaxterm*.

Here's how to access the Blockbit GSM CLI console, step by step:

1. Verify that the access device has a recommended SSH client already installed. Let's exemplify the process using the "PUTTY" application;

2. Access the SSH console. Fill in the fields:

- **Host Name (or IP Address):** Enter the IP address of the GSM BLOCKBIT. E.g.: 172.16.102.235;
- Click "Open".



*PuTTY Configuration*

3. The console will be displayed prompting for user and password;

In "login as:" Enter the admin user and press "Enter".  
After "password:" Enter the admin password and press "Enter".

The image below shows the commands of the main system services.

```
admin >help
arp
arping
configure-bgp
configure-ospf
configure-ospf6
configure-pim
configure-rip
configure-rip6
configure-syslog
conntrack
date
debug-atp
debug-auth
debug-dhcp
debug-dpi
debug-firewall
debug-ha
debug-ips
debug-ppp
debug-sdwan
debug-sync
debug-vpn
debug-webfilter
dig
disable-bgp
disable-logsessions
disable-ospf
disable-pim
disable-rip
disable-sip
disable-snmp
admin >

enable-bgp
enable-logsessions
enable-ospf
enable-pim
enable-rip
enable-root
enable-sip
enable-snmp
ethtool
exit
fdisk
free
fsck
fwrecovery
fwreload
grep
help
history
host
hostname
ifconfig
ifstat
iostat
iotest
ip
ipcalc
iplist
iptraf
ldapsearch
less
lscpu

lsusb
migrate-logsessions
mkfs
more
mtr
netads
netstat
nslookup
ntpdate
passwd
ping
reboot
reset
reset-admin-blocks
reset-admin-password
reset-admin-sessions
reset-logs
reset-stats
rewizard
route
sar
sensors
service-disable
service-enable
service-start
service-status
service-stop
set-bypass
set-ethernet-channels
set-irqbalance-dynamic
set-irqbalance-static

show-license
show-sessions
show-uuid
show-version
show-vpn-conn
show-vpn-info
show-wwan
shutdown
speedtest
ssh
sync-users
sysctl
tcpdump
tcptop
tcptrack
telnet
tracepath
tracert
update-bases
update-license
update-system
upgrade-kernel
uptime
vmstat
vtysh
watch-cpu
watch-io
watch-mem
watch-srv
wc
whois
```

#### Blockbit GSM – Command Line Interface

Next, we will present each command.

- [arp];
- [arping];
- [date];
- [debug-backup];
- [debug-deployer];
- [debug-rotation];
- [debug-sync];
- [disable-snmp];
- [enable-root];
- [enable-snmp];
- [ethtool];
- [exit];
- [fdisk];
- [free];
- [fsck];
- [grep];
- [help];
- [history];
- [hostname];
- [ifconfig];
- [ifstat];
- [iostat];
- [iotest];
- [ip];
- [ipcalc];
- [less];
- [logger-config];
- [logger-devices-add];
- [logger-devices-list];
- [logger-disable];
- [logger-enable];
- [logger-key];

- [lscpu];
- [mkfs];
- [more];
- [netstat];
- [ntpddate];
- [passwd];
- [ping];
- [reboot];
- [reset];
- [reset-admin-blocks];
- [reset-admin-password];
- [reset-admin-sessions];
- [reset-logs];
- [rewizard];
- [route];
- [sar];
- [set-network-dns];
- [set-network-gateway];
- [set-network-hostname];
- [set-network-interface];
- [set-network-timezone];
- [show-devices];
- [show-license];
- [show-uuid];
- [show-version];
- [shutdown];
- [tcpdump];
- [tcptop];
- [telnet];
- [tracepath];
- [traceroute];
- [update-gsm];
- [update-license];
- [upgrade-blockbit];
- [uptime];
- [vmstat];
- [whois].

# GSM - [arp]

Used to map the network address (for example, an IPv4 address) to a physical address (also called a MAC address), such as an Ethernet address. Displays and modifies the Internet Address to Ethernet addresses relations table. ARP has been implemented with many combinations of network technologies and the data link layer. IPv4 is the most common case.

Use this command to identify a network communication problem or to identify connected IP events and statuses.

How to use:

```
Modo de uso
admin >arp -h
Usage:
  arp [-vn]  [<HW>] [-i <if>] [-a] [<hostname>] <-Display ARP cache
  arp [-v]   [-i <if>] -d <host> [pub] <-Delete ARP entry
  arp [-vnD] [<HW>] [-i <if>] -f [<filename>] <-Add entry from file
  arp [-v]   [<HW>] [-i <if>] -s <host> <hwaddr> [temp] <-Add entry
  arp [-v]   [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub <-'''-

      -a display (all) hosts in alternative (BSD) style
      -e display (all) hosts in default (Linux) style
      -s, --set          set a new ARP entry
      -d, --delete      delete a specified entry
      -v, --verbose      be verbose
      -n, --numeric      don't resolve names
      -i, --device       specify network interface (e.g. eth0)
      -D, --use-device   read <hwaddr> from given device
      -A, -p, --protocol specify protocol family
      -f, --file         read new entries from file or from /etc/ethers

<HW>=Use '-H <hw>' to specify hardware address type. Default: ether
List of possible hardware types (which support ARP):
  ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
  netrom (AMPR NET/ROM) rose (AMPR ROSE) arcnet (ARCnet)
  dlci (Frame Relay DLCI) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
  irda (IrLAP) x25 (generic X.25) infiniband (InfiniBand)
  eui64 (Generic EUI-64)
admin >
```

Command Line Interface – arp

**Example:** Display the table of IP addresses and physical hosts (devices) addresses on the network:

```
admin >arp -a
? (172.16.12.85) at 00:26:8b:04:eb:bd [ether] on eth0
? (192.168.254.15) at 00:30:48:c2:02:a4 [ether] on eth2.254
? (172.16.13.248) at 0c:c4:7a:11:0f:96 [ether] on eth0
? (172.16.12.81) at 00:30:48:de:78:ae [ether] on eth0
? (192.168.254.4) at e6:9c:1f:89:11:32 [ether] on eth2.254
? (192.168.253.34) at 7e:49:6f:55:42:00 [ether] on eth2.253
? (172.16.12.92) at <incomplete> on eth0
? (172.16.12.90) at 10:98:36:fb:c9:1b [ether] on eth0
? (172.16.20.22) at 00:0b:ab:f1:9b:bc [ether] on eth3
? (172.16.12.71) at <incomplete> on eth0
? (172.16.20.20) at 00:0c:29:b7:34:cf [ether] on eth3
? (172.16.20.19) at 04:7d:7b:fd:53:d7 [ether] on eth3
? (172.16.12.65) at 78:2b:cb:c4:e7:12 [ether] on eth0
? (172.16.12.64) at <incomplete> on eth0
? (172.16.12.77) at 90:b1:1c:f6:2f:e2 [ether] on eth0
? (192.168.254.22) at 00:e0:4c:68:19:bf [ether] on eth2.254
admin >
```

Command Line Interface – arp – Example

# GSM - [arping]

Used to discover and identify connected hosts using ARP table associated with the analog response to ping using the ICMP protocol.

How to use:

```
admin >arping -h
Usage: arping [-fqbdUAV] [-c count] [-w timeout] [-I device] [-s source] destination
  -f : quit on first reply
  -q : be quiet
  -b : keep broadcasting, don't go unicast
  -D : duplicate address detection mode
  -U : Unsolicited ARP mode, update your neighbours
  -A : ARP answer mode, update your neighbours
  -V : print version and exit
  -c count : how many packets to send
  -w timeout : how long to wait for a reply
  -I device : which ethernet device to use
  -s source : source ip address
  destination : ask for what ip address
admin >
```

*Command Line Interface – arping*

**Example:** Find out the MAC address of a given IP:

```
admin >arping -c 5 -I eth0 172.16.12.85
ARPING 172.16.12.85 from 172.16.12.1 eth0
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 6.465ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 2.099ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.773ms
Unicast reply from 172.16.12.85 [00:26:8B:04:EB:BD] 0.761ms
^CSent 4 probes (1 broadcast(s))
Received 4 response(s)
admin >
```

*Command Line Interface – arping - Example*

# GSM - [date]

Used to list and change the current date and time.

How to use:

```
admin >date --help
Usage: date [OPTION]... [+FORMAT]
or: date [-u|--utc|--universal] [MMDDhhmm[[CC]YY][.ss]]
Display the current time in the given FORMAT, or set the system date.
...
Mandatory arguments to long options are mandatory for short options too.
-d, --date=STRING      display time described by STRING, not 'now'
-f, --file=DATEFILE    like --date once for each line of DATEFILE
-I[TIMESPEC], --iso-8601[=TIMESPEC] output date/time in ISO 8601 format.
                        TIMESPEC='date' for date only (the default),
                        'hours', 'minutes', 'seconds', or 'ns' for date
                        and time to the indicated precision.
-r, --reference=FILE    display the last modification time of FILE
-R, --rfc-2822          output date and time in RFC 2822 format.
                        Example: Mon, 07 Aug 2006 12:34:56 -0600
```

Command Line Interface – date

```
--rfc-3339=TIMESPEC    output date and time in RFC 3339 format.
                        TIMESPEC='date', 'seconds', or 'ns' for
                        date and time to the indicated precision.
                        Date and time components are separated by
                        a single space: 2006-08-07 12:34:56-06:00
-s, --set=STRING        set time described by STRING
-u, --utc, --universal  print or set Coordinated Universal Time (UTC)
--help                  display this help and exit
--version               output version information and exit
```

```
admin >
```

Command Line Interface – date 2

**Example 1:** List the current date and time:

```
admin >date
Thu Sep  1 09:59:08 BRT 2016
admin >
```

Command Line Interface – date – Example 1

**Example 2:** Update date and time based on America / São Paulo time zone:

```
admin > date --date='TZ="America/Sao_Paulo" 11:00'  
Thu Sep 1 11:00:00 BRT 2016  
admin >  
_OK ticket:57ddcb336098c149eebca22604e3a01a
```

Command Line Interface – date – Example 2

# GSM - [debug-backup]

This command displays the logs of the Manager's backups and restore routines, Loggers and Firewalls (Snapshots and Images).

```
admin >debug-backup -h
Usage: [OPTIONS] [TYPE] Pattern
       debug-backup Show debug logs for Targets

Optional Arguments
  -p, --profile      Set the profile name
  -s, --specific     Search for specific text on log
  -h, --help         Display this help message and exit

Examples:
  debug-backup -p PROFILE_NAME -s "2019-02-20 19:47"

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>
```

*Command Line Interface – debug-backup*

How to use:

```
admin >debug-backup
date="2021-01-14 15:37:01" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_ma
nager"
date="2021-01-14 15:37:05" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="" service="backup_ma
nager"
date="2021-01-14 15:39:02" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="U
TM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="running" status_message="" service="backup_ma
nager"
date="2021-01-14 15:40:02" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="U
TM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="downloading" status_message="" service="bac
kup_manager"
date="2021-01-14 15:40:03" device_id="5" backup_id="62" backup_name="Backup_200.32" device_type="firewall" action="backup" device_name="U
TM 2.1 - 200.32" storage_name="Storage_SMB" storage_type="smb" backup_type="snapshot" status="done" status_message="" service="backup_ma
nager"
date="2021-01-14 15:41:03" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_ma
nager"
date="2021-01-14 15:41:07" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="" service="backup_ma
nager"
date="2021-01-14 15:45:02" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_ma
nager"
date="2021-01-14 15:45:05" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="error" status_message="No available space d
isk" service="backup_manager"
date="2021-01-14 15:49:04" device_id="4" backup_id="59" backup_name="Douglas Sistema" device_type="firewall" action="backup" device_name="
"UTM 2.1 - 200.31" storage_name="Storage_SMB" storage_type="smb" backup_type="system" status="running" status_message="" service="backup_ma
nager"
admin >
```

*Command Line Interface – debug-backup*

Displays the following information:

- **Date:** Sets the date and time;
- **Device\_id:** Determines the device ID;
- **Device\_type:** Defines the type of the device, which can be:
  - manager;
  - firewall;
  - analyzer.
- **Action:** Determines what action the routine will take:
  - backup;
  - restore.
- **Device\_name:** Displays the device name;
- **backup\_name:** Shows the name of the backup file;
- **storage\_name:** Displays the name of the remote store;
- **storage\_type:** Sets the type of remote storage;
- **backup\_type:** Determines the type of backup and can be:



- snapshot;
  - image;
  - logger.
- **Status:** Displays the status message, which can be:
  - waiting;
  - running;
  - error;
  - success.
- **Status\_message:** If the status has displayed a message (most common in the case of errors), this line displays the status message.

# GSM - [debug-deployer]

Used to monitor deployer settings and package installation on devices.

**How to use:**

```
admin >debug-deployer
2017-05-15 17:57:50: (Task:sync-device - Dev:6) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:8) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:9) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:7) Finish sync-device
2017-05-15 17:57:51: (Task:sync-device - Dev:8) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:6) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:2) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:4) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:5) Finish sync-device
2017-05-15 17:57:52: (Task:sync-device - Dev:3) Finish sync-device
```

Command Line Interface – debug-deployer

# GSM - [debug-rotation]

This command is used to consult the maintenance logs via the stored CLI.

```
admin >debug-rotation -h
Usage: [OPTIONS] Pattern
       debug-rotation Show debug logs for log rotation

Optional Arguments
  -dev, --device      Serach for specific device
  -s, --specific      Search for specific text on log
  -h, --help          Display this help message and exit

Examples:
  debug-logrotate -dev d1 -s "2019-02-20 19:47"

Copyright BLOCKBIT® (http://www.blockbit.com/)
All rights reserved <info@blockbit.com>

admin >|
```

*Command Line Interface – debug-rotation -h*

How to use:

```
admin >debug-rotation -h
Feb 19 10:02:37 loggerstand21-80 gsm-apply-rotate: total_space_disk="150" total_used_disk_ini="4.30%" device_id="5" device_name="Logger Remoto" date="2021-2-19 10:2" deleted_date_ini="logstash-2021.02.17" de
leted_date="2021-02-10" deleted_date="2021-02-17" deleted_date="2021-02-18" deleted_date="2021-02-19" deleted_date_end="" Total_used_disk_end="410" total_free_space_disk="146" current_total_index="0" service
="log-rotation"
```

*Command Line Interface – debug-rotation -h*

The command displays the following information:

- **Date:** Displays the Date and Time;
- **Device\_id:** Shows the device ID;
- **Device\_name:** Displays the device name;
- **Deleted\_date\_ini:** Displays the start date of the deleted log period;
- **Deleted\_date\_end:** Displays the end date of the deleted log period;
- **Current\_total\_index:** Shows the current total of log indexes;
- **Total\_space\_disk:** Displays the total space used by storage;
- **Total\_free\_space\_disk:** Shows the total available space.

# GSM - [debug-sync]

Used to monitor the communication between the Blockbit GSM and devices. Displays updates and device status.

**How to use:**

```
admin >debug-sync
2017-05-15 19:30:24: (Task:status-device - Dev:7) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:7) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:6) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:6) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:4) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:4) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:3) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:3) Finish status-device
2017-05-15 19:30:24: (Task:status-device - Dev:9) Authentication OK
2017-05-15 19:30:24: (Task:status-device - Dev:9) Finish status-device
admin >
```

*Command Line Interface – debug-sync*

# GSM - [disable-snmp]

Disables the SNMP service.

**How to use:**

```
admin >disable-snmp
snmpd is disabled!
admin >
```

*Command Line Interface – disable-snmp*



Disables only the service, the settings will remain.

# GSM - [enable-root]

Enable root access to the system, it will be necessary to enter the password compatible with the key that will appear on the screen.

**How to use:**

```
admin >enable-root  
Challenge: 7bad30ac339b94cc259d756a02b62ff7  
Type the password: █
```

Command Line Interface – enable-root

# GSM - [enable-snmp]

SNMP Enables and configures (SNMPv1, SNMPv2 or SNMPv3).

How to use:

```
admin >enable-snmp
Location: Sao Paulo
Organization: BLOCKBIT
E-mail: admin@blockbit.com
Enable SNMPv1 (Y/N)? Y
Enable SNMPv2 (Y/N)? Y
Community name: BLOCKBIT
Network Access (Leave blank to default 0.0.0.0/0): 172.16.102.0/24
Enable SNMPv3 (Y/N)? Y
Auth Protocol (MD5 or SHA): MD5
Username: blockbit
User password (minimum of 8 characters): password
Encryption Protocol (3DES or DES): 3DES
Encryption Password: password
Enable SNMPv1
Enable SNMPv2
Community: BLOCKBIT
Network Access: 172.16.102.0/24
Enable SNMPv3
Auth Protocol: MD5
Username: blockbit
Encryption Protocol: 3DES

Confirm (Y/N)? Y
```

*Command Line Interface – enable-snmp*

After confirming the above configuration, the following settings are displayed:

```

snmp is enabled!

syslocation "Sao Paulo"

syscontact "admin@blockbit.com"
syscontact "BLOCKBIT"

com2sec local localhost BLOCKBIT
com2sec mynetwork 172.16.102.0/24 BLOCKBIT

group MyRWGroup v1 local
group MyRWGroup v2c local
group MyRWGroup usm local

group MyROGroup v1 mynetwork
group MyROGroup v2c mynetwork
group MyROGroup usm mynetwork

view all included .1.3.6.1.2.1.1
view all included .1.3.6.1.2.1.2
view all included .1.3.6.1.4.1.2021
view all included .iso.org.dod.internet.mgmt.mib-2.system
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrSystem.hrSystemUptime
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrDevice
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrSWRunPerf
view all included .iso.org.dod.internet.mgmt.mib-2.host.hrStorage
view all included .iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry
view all included .1.3.6.1.4.1.8072.1.3.2.4.1.2
view all included .1.3.6.1.2.1.31

pass .1.3.6.1.2.1.31.1.1.1.18 /bin/bash /opt/omne/conf/mibs/net-ifalias

access MyROGroup "" any noauth exact all none none
access MyRWGroup "" any noauth exact all none none
rouser blockbit
admin >

```

Command Line Interface - enable-snmp - Example configurations

The information obtained through SNMP can be better viewed through Zabbix, for more information about this access this [page](#). Note that if you want to use Zabbix, the name of your community cannot have spaces. Ex.: *Community Name: Blockbit Community*.



If you want to use a community name with spaces in Zabbix, you will need to name it in quotes. Ex.: *Community Name: "Blockbit Community"*



# GSM - [ethtool]

Used to display and detail information regarding network interfaces, check online and offline interfaces, change speed, change negotiation form and verify which interface is physically located.

How to use:

```
admin >ethtool -h
ethtool version 3.15
Usage:
    ethtool DEVNAME Display standard information about device
    ethtool -s|--change DEVNAME      Change generic options
    [ speed %d ]
    [ duplex half|full ]
    [ port tp|au|bnc|mii|fibre ]
    [ mdix auto|on|off ]
    [ autoneg on|off ]
    [ advertise %x ]
    [ phyad %d ]
    [ xcvr internal|external ]
    [ wol p|u|m|b|a|g|s|d... ]
    [ sopass %x:%x:%x:%x:%x:%x ]
    [ msglvl %d | msglvl type on|off ... ]
```

Command Line Interface – ethtool

**Exemplo:** Identify a specific network interface:

```
admin >ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supported pause frame use: Symmetric
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised pause frame use: Symmetric
    Advertised auto-negotiation: Yes
    Speed: 1000Mb/s
    Duplex: Full
    Port: Twisted Pair
    PHYAD: 1
    Transceiver: internal
    Auto-negotiation: on
    MDI-X: off (auto)
    Supports Wake-on: pumbg
    Wake-on: g
    Current message level: 0x00000007 (7)
                           drv probe link
    Link detected: yes
Admin >
```

Command Line Interface – ethtool - Example

# GSM - [exit]

Used to exit the session.

**How to use:**

```
Modo de uso  
admin >exit |
```

Command Line Interface – exit

# GSM - [fdisk]

Used for managing hard disk partitions. You can list and identify HDD-SSD storage devices, create physical partitions, logical partitions, delete, display information, and so on.

**How to use:**

```
admin >fdisk -h
Usage:
fdisk [options] <disk>    change partition table
fdisk [options] -l <disk> list partition table(s)
fdisk -s <partition>      give partition size(s) in blocks
Options:
-b <size>                  sector size (512, 1024, 2048 or 4096)
-c[=<mode>]                compatible mode: 'dos' or 'nondos' (default)
-h                          print this help text
-u[=<unit>]                display units: 'cylinders' or 'sectors' (default)
-v                          print program version
-C <number>                specify the number of cylinders
-H <number>                specify the number of heads
-S <number>                specify the number of sectors per track
admin >
```

Command Line Interface – fdisk

**Example:** List existing disks and partitions:

```

admin >fdisk -l
WARNING: fdisk GPT support is currently new, and therefore in an experimental phase.
Use at your own discretion.

Disk /dev/sda: 128.0 GB, 128035676160 bytes, 250069680 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: gpt

#          Start          End          Size Type          Name
1          2048           4095          1M BIOS boot parti
2          4096          1052671        512M Microsoft basic
3         1052672        42049535        19.6G Microsoft basic
4         42049536        70758399        13.7G Microsoft basic
5         70758400        74891263         2G Linux swap
6         74891264        79024127         2G Microsoft basic
7         79024128        250069646       81.6G Microsoft basic

Disk /dev/napper/luks-ba8b8ea1-522e-49c2-9c48-02e8db50ec5d: 21.0 GB, 20988297216
bytes, 40992768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-049e58a3-626a-46bf-8019-3db9fd8b6241: 87.6 GB, 87573208576
bytes, 171041423 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-999d4257-849e-4a76-9bbf-6a0ae186ac98: 2113 MB, 2113929216
bytes, 4128768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/luks-92f58453-e018-4e1f-a014-2489dfb715e1: 14.7 GB, 14696841216
bytes, 28704768 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/napper/cryptoswap: 2116 MB, 2116026368 bytes, 4132864 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

admin >

```

Command Line Interface – fdisk – Example

# GSM - [free]

Used to check memory size and usage on the server.

How to use:

```
admin >free --h
free: option '--h' is ambiguous; possibilities: '--human' '--help'

Usage:
  free [options]

Options:
  -b, --bytes          show output in bytes
  -k, --kilo           show output in kilobytes
  -m, --mega           show output in megabytes
  -g, --giga           show output in gigabytes
  --tera              show output in terabytes
  -h, --human          show human-readable output
  --si                use powers of 1000 not 1024
  -l, --lohi           show detailed low and high memory statistics
  -t, --total          show total for RAM + swap
  -s N, --seconds N   repeat printing every N seconds
  -c N, --count N     repeat printing N times, then exit
  -w, --wide           wide output

  --help              display this help and exit
  -V, --version        output version information and exit

For more details see free(1).
admin >
```

*Command Line Interface – free*

**Example:** Check memory consumption:

```
admin >free -m
              total        used        free      shared  buff/cache   available
Mem:          3952         172         186         216        3593        3324
Swap:         1995           80        1915
admin >
```

*Command Line Interface – free – Example*

# GSM - [fsck]

Used to check and correct errors on disks and file systems.

How to use:

```
admin >fsck -h
/usr/sbin/fsck.ext4: invalid option -- 'h'
Usage: /usr/sbin/fsck.ext4 [-panyrcdfvtDFV] [-b superblock] [-B blocksiz]
      [-I inode_buffer_blocks] [-P process_inode_size]
      [-l|-L bad_blocks_file] [-C fd] [-j external_journal]
      [-E extended-options] device

Emergency help:
-p          Automatic repair (no questions)
-n          Make no changes to the filesystem
-y          Assume "yes" to all questions
-c          Check for bad blocks and add them to the badblock list
-f          Force checking even if filesystem is marked clean
-v          Be verbose
-b superblock Use alternative superblock
-B blocksiz  Force blocksiz when looking for superblock
-j external_journal Set location of the external journal
-l bad_blocks_file Add to badblocks list
-L bad_blocks_file Set badblocks list
admin >
```

Command Line Interface – fsck

**Example:** Check for possible errors on a particular partition:

```
Admin >fsck /dev/sda3
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/dev/sda3: clean, 702/192000 files, 52661/768000 blocks
...
reloading firewall chains
reloading firewall zones
reloading firewall input
iptables: No chain/target/match by that name.
iptables: No chain/target/match by that name.
reloading firewall redirects
reloading firewall security rules
reloading firewall multilink rules
reloading firewall vpn rules
reloading firewall atp rules
admin >
```

Command Line Interface – fsck - Example

# GSM - [grep]

This command has the function to perform a search for the occurrence of regular expressions that match the searched pattern. It is used in conjunction with other commands to filter output results.

**Example:** Filter debug-web output to only view requests destined for a specific URL:

```
admin -debug-web|grep blockbit.com
type=web date=2018-03-14 10:51:43 bytes=745 mac=00:00:00:00:00:00 src=172.16.13.82:16959 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=ww
w.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
type=web date=2018-03-14 10:52:10 bytes=1011 mac=00:00:00:00:00:00 src=172.16.13.82:16962 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=ww
w.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
type=web date=2018-03-14 10:52:10 bytes=1011 mac=00:00:00:00:00:00 src=172.16.13.82:16958 dst=104.198.103.7:443 code=TCP_TUNNEL/- method=CONNECT rule=WEB: Navegação Permitida user=- site=ww
w.blockbit.com url=www.blockbit.com agent=[Mozilla/5.0(WindowsNT10.0;Win64;x64)AppleWebKit/537.36(KHTML,likeGecko)Chrome/64.0.3282.186Safari/537.36]
```

*Command Line Interface – grep - example*

**Example 2:** Filter ethtool command output using regex:

```
admin >ethtool eth0|grep -ie "speed\|detected"
Speed: 10000Mb/s
Link detected: yes
```

*Command Line Interface – grep – example 2*

# GSM - [help]

Used to display a list of all commands available in the interface.

How to use:

```
admin >help
arp          ifconfig      ntpdate      show-devices
arping       ifstat        passwd       show-license
date         iotest       ping         show-uuid
debug-deploy ip          reboot      show-version
debug-sync   ipcalc      reset        shutdown
enable-root  less        reset-admin-block tcpdump
ethtool      logger-config reset-admin-password tcptop
exit         logger-devices-add reset-admin-sessions telnet
fdisk        logger-devices-list reset-logs    tracepath
free         logger-disable  rewizard     traceroute
fsck         logger-enable   route        update-gsm
grep         logger-key      sar          update-license
help         lscpu          set-network-dns uptime
history      mkfs           set-network-gateway vmstat
hostname     more           set-network-interface whois
hystory      netstat        set-network-timezone
admin >|
```

*Command Line Interface – help*



# GSM - [history]

When using this command, a history of all recently used commands is displayed.

**How to use:**

```
admin >history
1: aa
2: help
3: ifconfig eth0 172.31.102.235
4: route add default gw 172.31.0.1
5: ifconfig
6: hrlp
7: help
8: route -n
9: ifconfig eth0 172.31.102.236
10: route add default gw 172.31.0.1
11: route -n
12: ifconfig
13: route -n
14: ifconfig
15: ifconfig eth0 172.31.102.236/16
16: route add default gw 172.31.0.1
17: ifconfig
18: grep
19: grep log myfile
20: ls
21: fgrep log myfile
22: grep
23: ?
24: debug-deployer
25: debug-sync
26: debug-sync | grep log
27: history
admin >
```

Command Line Interface – history

# GSM - [hostname]

Used to view or change the hostname of your Blockbit UTM device.

How to use:

```
Modo de uso
admin >hostname -h
Usage: hostname [-b] {hostname|-F file}      set host name (from file)
        hostname [-a|-A|-d|-f|-i|-I|-s|-y]    display formatted name
        hostname                                display host name

        {yp,nis,}domainname {nisdomain|-F file} set NIS domain name (from file)
        {yp,nis,}domainname                    display NIS domain name

        dnsdomainname                          display dns domain name

        hostname -V|--version|-h|--help        print info and exit

Program name:
        {yp,nis,}domainname=hostname -y
        dnsdomainname=hostname -d

Program options:
        -a, --alias                alias names
        -A, --all-fqdns            all long host names (FQDNs)
        -b, --boot                set default hostname if none available
        -d, --domain              DNS domain name
        -f, --fqdn, --long        long host name (FQDN)
        -F, --file                read host name or NIS domain name from given file
        -i, --ip-address          addresses for the host name

        -I, --all-ip-addresses    all addresses for the host
        -s, --short               short host name
        -y, --yp, --nis          NIS/YP domain name

Description:
        This command can get or set the host name or the NIS domain name. You can
        also get the DNS domain or the FQDN (fully qualified domain name).
        Unless you are using bind or NIS for host lookups you can change the
        FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
        part of the FQDN) in the /etc/hosts file.
admin >
```

*Command Line Interface – hostname*

**Example:** Use the command to display the current name of your Blockbit UTM device:

```
admin >hostname
gsm.blockbit.com
admin >
```

*Command Line Interface – hostname - Example*

# GSM - [ifconfig]

Used to configure and manage interface settings. You can enable, disable, and list the status of each of the interfaces. Can also be used to optimize the system configuration.

How to use:

```
admin >ifconfig -h
Usage:
  ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>]
  [add <address>[/<prefixlen>]]
  [del <address>[/<prefixlen>]]
  [[-]broadcast <address>] [[-]pointopoint <address>]
  [netmask <address>] [dstaddr <address>] [tunnel <address>]
  [outfill <NN>] [keepalive <NN>]
  [hw <HW> <address>] [mtu <NN>]
  [[-]trailers] [[-]arp] [[-]allmulti]
  [multicast] [[-]promisc]
  [mem_start <NN>] [io_addr <NN>] [irq <NN>] [media <type>]
  [txqueuelen <NN>]
  [[-]dynamic]
  [up|down] ...
  <HW>=Hardware Type.
  List of possible hardware types:
    loop (Local Loopback) slip (Serial Line IP) cslip (VJ Serial Line IP)
    slip6 (6-bit Serial Line IP) cslip6 (VJ 6-bit Serial Line IP) adaptive (Adaptive
Serial Line IP)
    ash (Ash) ether (Ethernet) ax25 (AMPR AX.25)
    netrom (AMPR NET/ROM) rose (AMPR ROSE) tunnel (IPIP Tunnel)
    ppp (Point-to-Point Protocol) hdlc ((Cisco)-HDLC) lapb (LAPB)
    arcnet (ARCnet) dlci (Frame Relay DLCI) frad (Frame Relay Access Device)
    sit (IPv6-in-IPv4) fddi (Fiber Distributed Data Interface) hippi (HIPPI)
    irda (IrLAP) ec (Econet) x25 (generic X.25)
    infiniband (InfiniBand) eui64 (Generic EUI-64)
  <AF>=Address family. Default: inet
  List of possible address families:
    unix (UNIX Domain) inet (DARPA Internet) inet6 (IPv6)
    ax25 (AMPR AX.25) netrom (AMPR NET/ROM) rose (AMPR ROSE)
    ipx (Novell IPX) ddp (Appletalk DDP) ec (Econet)
    ash (Ash) x25 (CCITT X.25)
admin >
```

*Command Line Interface – ifconfig*

**Example:** View information about all network interfaces, active and disabled:

```

admin >ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.102.235 netmask 255.255.254.0 broadcast 172.16.103.255
    inet6 fd29:2e81:cb18:0:20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x20<link>
    inet6 2002:db5:db5:0:20c:29ff:fe57:b1e7 prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:57:b1:e7 txqueuelen 1000 (Ethernet)
    RX packets 23001360 bytes 5108284564 (4.7 GiB)
    RX errors 0 dropped 1210 overruns 0 frame 0
    TX packets 28303075 bytes 4079603075 (3.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255
    ether 00:0c:29:57:b1:f1 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth2: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:57:b1:fb txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth3: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:57:b1:05 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local loopback)
    RX packets 123895270 bytes 37387210708 (34.8 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 123895270 bytes 37387210708 (34.8 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

admin >

```

Command Line Interface – ifconfig - Example

# GSM - [ifstat]

Used to view network traffic statistics.

How to use:

```
admin >ifstat -h
Usage: ifstat [OPTION] [ PATTERN [ PATTERN ] ]
-h, --help                this message
-a, --ignore ignore history
-d, --scan=SECS           sample every statistics every SECS
-e, --errors show errors
-n, --nooutput            do history only
-r, --reset               reset history
-s, --noupdate            don;t update history
-t, --interval=SECS      report average over the last SECS
-V, --version             output version information
-z, --zeros               show entries with zero activity
admin >
```

Command Line Interface – ifstat

**Example:** List overall traffic statistics of all network interfaces:

```
admin >ifstat
#kernel
Interface      RX Pkts/Rate  TX Pkts/Rate  RX Data/Rate  TX Data/Rate
                RX Errs/Drop  TX Errs/Drop  RX Over/Rate  TX Coll/Rate
lo              19982K 0      19982K 0      425601K 0     425601K 0
                0 0          0 0          0 0          0 0
eth0            896411 0      789041 0      676523K 0     687826K 0
                0 0          0 0          0 0          0 0
eth1            829588 0      821426 0      229273K 0     646217K 0
                0 1476      0 0          0 0          0 0
eth3            302159 0      19735 0       24840K 0      1616K 0
                0 30        0 0          0 0          0 0
ifb0            537040 0      537040 0      107390K 0     107390K 0
                0 0          0 0          0 0          0 0
ipsec0          0 0        0 0          0 0          0 0
                0 0          0 0          0 0          0 0
admin >
```

Command Line Interface – ifstat - Example

# GSM - [iotest]

Used to perform an input/output (I/O) write test on the "file system" partition structure of the Blockbit UTM disk.

**How to use:**

```
admin >iotest
Testing root filesystem
1000000+0 registros de entrada
1000000+0 registros de saída
2048000000 bytes (2,0 GB) copiados, 89,0756 s, 23,0 MB/s
Cleaning
admin >
```

*Command Line Interface – iotest - Example*

# GSM - [ip]

Through this command, you can perform the display, manipulation, and routing of devices, interfaces and network tunnels.

How to use:

```
admin >ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | addr | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddr | mroute | mrule | monitor | xfrm |
                  netns | l2tp | tcp_metrics | token }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                   -f[amily] { inet | inet6 | ipx | dnet | bridge | link } |
                   -4 | -6 | -I | -D | -B | -0 |
                   -l[oops] { maximum-addr-flush-attempts } |
                   -o[neline] | -t[imestamp] | -b[atch] [filename] |
                   -rc[vbuf] [size]}
```

Command Line Interface – ip

# GSM - [ipcalc]

Used for IPv4 and IPv6 network mask/subnet mask calculation. It has options to identify the prefix (mask), the network address and the broadcast address.

How to use:

```
admin >ipcalc -h
ipcalc: ip address expected
Usage: ipcalc [OPTION...]
  -c, --check           Validate IP address for specified address family
  -4, --ipv4            IPv4 address family (default)
  -6, --ipv6            IPv6 address family
  -b, --broadcast       Display calculated broadcast address
  -h, --hostname        Show hostname determined via DNS
  -m, --netmask         Display default netmask for IP (class A, B, or C)
  -n, --network         Display network address
  -p, --prefix          Display network prefix
  -s, --silent          Don't ever display error messages

Help options:
  -?, --help           Show this help message
  --usage              Display brief usage message
admin >
```

Command Line Interface – ipcalc.

**Example:** Calculate a subnet, its network, and broadcast addresses:

```
admin >ipcalc -n -b -p 192.168.7.0/23
PREFIX=23
BROADCAST=192.168.7.255
NETWORK=192.168.6.0
admin >
```

Command Line Interface – ipcalc – Example.



# GSM - [less]

Used to paginate files or standard inputs. It is possible to direct the output of another command using the pipe "|".

**How to use:** Use the less command as output from another command that returns a very extensive amount of information.

```
admin >iplist | less
admin >

ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 00:0c:29:71:fe:66 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.1/24 brd 192.168.1.255 scope global eth0
        valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok

ZONE WAN (3) 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb state UP
qlen 1000
    link/ether 00:0c:29:71:fe:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.11/24 brd 192.168.0.255 scope global eth1
        valid_lft forever preferred_lft forever
eth1: negotiated 1000baseT-FD flow-control, link ok
ZONE (WAN) eth2: negotiated 1000baseT-FD flow-control, link ok
ZONE DMZ (2) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UP qlen 1000
    link/ether 00:0c:29:71:fe:84 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.11/24 brd 172.16.102.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok
(END)
```

Command Line Interface – less

# GSM - [logger-config]

This command enables a Configuration Wizard for the installation of a logger server. There are two operation modes available: Standalone or Integrated, the difference between these being:

## Standalone

In this operation mode, the server is used exclusively for remote logging, it cannot be used for any other function. It is mandatory to use the Blockbit firmware.

## Integrated

This operation mode allows you to use the local GSM itself where the manager is installed as a logger server. However, it is necessary to devote an entire disk only to this function, regardless of whether it is virtual or physical.

## How to use:

**Example 1:** For the installation of a standalone logger it is necessary to choose this mode of operation when requested in "Enter the logger operating mode", next we will analyze each of the options that appear in the wizard:

```
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.102.236
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
DNS (ex: 1.1.1.2): 172.16.102.184
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sdb: 2147 MB  AVAILABLE
Disk /dev/sda: 34.4 GB  SYSTEM
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
```

Command Line Interface – logger-config – Example 1

- **Interface:** GSM interface type. E.g.: eth0;
- **IP address:** GSM IP address. E.g.: 172.31.102.236;
- **Mask:** GSM network mask. E.g.: 255.255.0.0;
- **Gateway:** Determines the GSM gateway. E.g.:172.31.0.1;
- **DNS:** Determines the GSM DNS. E.g.:172.16.102.148;
- **Timezone:** Determines the time zone with which GSM has been configured. E.g.: America / Sao\_Paulo;
- **Timezone:** Determines the time zone with which GSM has been configured. E.g.: America / Sao\_Paulo;
- **Generate Key:** To generate the secret key, type "y" and press "enter". It is important to save this sequence because it will be used during the creation of the Logger in the GSM Analyzer visual interface (check "Create Logger Device").



Note that if the user chooses that a key is not generated when the prompt displays "Generate Key?", you can use the command "[logger-key -c](#)" or perform "[logger-config](#)" again.

At the end of the wizard you should see results similar to those shown by the image below:

```

admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: standalone
Interface (ex: eth0): eth0
IP address (ex: 1.1.1.10): 172.31.102.236
Mask (ex: 255.255.255.0): 255.255.0.0
Gateway (ex: 1.1.1.1): 172.31.0.1
DNS (ex: 1.1.1.2): 172.16.102.184
Timezone (ex: America/Sao_Paulo): America/Sao_Paulo

Disk /dev/sdb: 2147 MB AVAILABLE
Disk /dev/sda: 34.4 GB SYSTEM
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
131072 inodes, 524288 blocks
26214 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=536870912
16 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5fe6d5e6d34f249f3a136378c753707a05bf0fae5647932932a4b4c1905bfedf110e95615b4a1549779c1aa15fab12c7fa796903ff641c1b01347a866bf
1f6864c57a15639a4b3d56194fa17eb854f8ad43cd0d0f6b39b36e9fcea6e56c56da8dba8f9aa9c990277ad852e522ae3dfd6313ed58326353fb71fc29051733ba709bb
0ae040c78a63c129c14a6a218650dde3e9c711866bd13e323150ed2188bc3d6d3685eadb0ce102ac886e89ff74768a884abb2e70dcaef52f3bd0583ed0f4fcb01722446
ca8629853f8618fd407e2cc9b7e42743f6a3b199f955cc1c017860483e2bc749501e955365f6f2e2128185a52aa1e72be7f7c3120a6bfd70e1d8fe02584f3c83a0cf80a5d
f1b340c23654979251f13b29d4f4992aaf2b9ce4d82979cdaeefc9bd0e678a99a1410ad7532b61c694b4d024f3a1e03c8295d21dce9b9bd43a9369bdaf5a0aa3cfb5b2
a23f1a6b463280a7c005cc83e2f8a8d7a9d778235aa631ceea861880244d1ac7d02c18391a6f7d64b5b7236f4f40f6f80ee4e3007d5b50d2f7ee0454c6efe9c5cf0ae9f5d
c9a0f9b1a10e9e24f2ddc914595b1b0c1477e508cc0ab7f0ad04ef45129e58160fa985aeb4f1761230f0f25e4b570b76b5aa79f7ee343e0f16514371674f3623fccab3
5c457332d0f50bb42f60dd0d9e325c80869355a5d0b9d9e225fb374f27254fed2836cbf866439b90af1a64705f0d1934ee5628328647242c1b04ab3ac748a5dc3cb10e
abf46b142f89e0a0eab0f7ac93c6ef5eede60992c4edccfc2a888690f19b2ab20c01be676b39c984278b581ad978286edf01b2bfdda45f8ac8c8c765a0d207c936a8b81fe
262f2c3913a1840377a8a14ab4701a89943b300f57f77961cbe287a5468eb7a052574c83f34d36d6d1489098e6af1d3fe647cb70bab82ec82c8ca051e52ef4386f172c51b
b9a427cb4a021cc68e1e9887ac755342e9570

Completed

Now configure the logger in administrative interface
admin >

```

Command Line Interface – logger-config – Standalone

**Example 2:** For the installation of an integrated logger it is necessary to opt for this mode of operation when requested in "Enter the logger operating mode". Next, we will analyze each of the options that appear in the wizard:

```

admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated

Disk /dev/sda: 34.4 GB SYSTEM
Disk /dev/sdb: 2147 MB AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mke2fs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y

```

Command Line Interface – logger-config – Example 2

- **Disk:** Determines the disk in which the logger will be installed. You will see a summary of the disks that make up the appliance, and their status (for example, "Available" represents an available disk and "System" a disk used by the system). You must enter the directory of the disk that will be used. After this step, a message warning that the entire disk will be used and not just a partition will appear, to proceed, type "y" and press "enter". Ex: /dev/sdb;
- **Generate Key:** To generate the secret key, type "y" and press "enter". It is important to save this sequence because it will be used during the creation of the Logger in the GSM Analyzer visual interface (check "Create Logger Device").



Note that if the user chooses that a key is not generated when the prompt displays "Generate Key?", you can use the command "**logger-key -c**" or perform "**logger-config**" again.

At the end of the wizard you should see results similar to those shown by the image below:

```

admin >
admin >logger-config
Enter the logger operating mode: [ standalone / integrated ]: integrated

Disk /dev/sda: 34.4 GB  SYSTEM
Disk /dev/sdb: 2147 MB  AVAILABLE
Disk (ex: /dev/sdb): /dev/sdb
mkfs 1.42.9 (28-Dec-2013)
/dev/sdb is entire device, not just one partition!
Proceed anyway? (y,n) y
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
131072 inodes, 524288 blocks
26214 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=536870912
16 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done

Generate key? [y/N]: y
Key:
53616c7465645f5fd6dc4e9d919bc6deaa94284d30b752d877f48cae914e5dda322aa39c3a867ed26dfbfa105efbbb93635fd754f8f00b6b4bd096fd0f4f117db265c00088
6e64b863275ad72647143f4b38fa4c9dab1403bbaacabb9fa03e8dd77db5e845849a7b6f8ea3e91e15d47dd7989a087d60460bce90d225cf9827b8c5bef0fca39eb6862859
7219486dfb0e58cd3bab365d051198a0592af05aebf7f012d02f420e0c0a8b6dea95c6595800707d232e3a3704b9ba0119f422fb0b71a247e9a77225a070a1b59ab1d5356
02d39e0c8abd83c3d41430556fabba5dc090b199b24f0b7b887c33a313bc649c107447afdb8fd5e6c2872cfed801d5c17eed15698ed886519744fb31811cbf3d5a841597
2132dfa21e6f0e8fcc35671ce942933be5bcfe329c6bc5be6a39fe4658d2ec4c9c792782bfc4ccf5ac17813ce0fab8ace325a9f5d57df66d6ad9ba501ade152716a8d7927
f9d3aff1887a047a33045b0904df8b1a8bfff490ff4110f9da23b5a4a89f2804fefabd455e810b21a984d6feal29dc8c09882c54b7a89a30c115c2fb29171c259feee1a377
918fe8fcb0a843351a56fb72968459ad595d8f0f3e676eec4de95af5f3d61852b1caf76ff076f3503a1ddf7ff3eb1d8618855b68d29bd333eb7d2311ff2d522c197207a63
fdeb5a7489fcbcd6e21ce4d6f1f169afaa7fc0a1a3ea4b4cad1b40655c1d8d25f586f368ac629d4826fcaa99033adde5474e577501a95ce7fc01ec7bcbdaa5a0f614c3429
2867c8b03487769919c05e7d4695469befee193df003487584d75bd2640c2810715781c4a8a5a78dac3a01d4c4c07762f025a8a9e35292e3d10e2cc60966e035bf85ef07b
b1d7966b41e4a2c1b27721cd6098d3a1a4fd4315603e426f0539bc64e3369bb27fe78b912b9ef4df40c9150737132b8b9b8f11556ea0cd97a2aa55a82bcb5c0aaf1439ab9
ffd9c9

Completed

Now configure the logger in administrative interface

admin >

```

## Command Line Interface – logger-config – Integrated

# GSM - [logger-devices-add]

Used to add devices to the logger, it is necessary to pass the device path in order to execute the addition.

**How to use:**

```
admin >logger-devices-add /dev/sdb  
admin >
```

*Command Line Interface – logger-devices-add.*

# GSM - [logger-devices-list]

This command is used to display a list of devices used by the logger.

**How to use:**

```
admin >logger-devices-list
Disk /dev/sdb: 34.4 GB  P00L
Disk /dev/sda: 34.4 GB  SYSTEM
admin >
```

*Command Line Interface – logger-devices-list*

# GSM - [logger-disable]

Command to disable the logger in the pool.

**How to use:**

```
admin >logger-disable  
admin >
```

Command Line Interface – logger-disable

# GSM - [logger-enable]

Command to enable the logger in the pool.

**How to use:**

```
admin >logger-enable  
admin >
```

Command Line Interface – logger-enable



# GSM - [logger-key]

Used to display the secret key of the logger, it is used during the creation of the Logger in the GSM [Analyzer](#) visual interface. When passing the parameter "-c" the command generates keys.

## How to use:

```
admin >logger-key
53616c7465645f5fd6dc4e9d919bc6deaa94284d30b752d877f48cae914e5dda322aa39c3a867ed26dfbfa105efbbb93635fd754f8f00b6b4bd96fd0f4f117db265c00088
6e64b863375ad73647143f4b38fa4c9dab14036bacabb9fa03e8ddf7db5e845849a7b6f8ea3e91e15d47dd7989a087d60460bce90d225cf9827b8c5bef0fca396b6862859
7219486dfb9e58cd3bab365d051198a0592ef05a6bf7f012d02f429e9cba8b6dea95c6595890797d232e3a3704b9ba0119f422fb9b71a247c9a77225a979a1b59ab1d5356
02d39e0c8abd83c3d41430556fabba5dc090b199b24f0b7b887c33a313bc649c107447afdb8fd5e6c2872cfe801d5c17eed15698ed886519744fb31811cbf3d5a841597
2132dfa21e5f0e8fccc35671ce94293be5bcfe329c6bc5be6a39fe4658d2ec4c9c7392782bfc4ccf5ac17813ce0fab8ace325a9f5d57df66d6ad9ba501ade152716a8d7927
f9d3aff1e87a047a33045b0904dfbb1a8bff490ffa110f9da23b5a4a89f2804fefabd455e810b21a984d6feal29dc8c09802c54b7a89a30c115c2fb29171cc259feee1a377
918fe8fcbb0a843351a56fb729e8459ad595d8f0f3e67e6ec4de95afsf3d61852b1caf76ff076f3503a1df7ff3aeb1d8618855b68d29bd33aeb7d2311ff2d522c197207a63
fdeb5a7489fcbcd6e21ce4d6f1f169afaa7fc0a1a3ea4b4cad1b40655c1d8d25f586f368ac629d4826fcaa99033adde5474e577501a95ce7fc01ec7bcfdaa5a0f614c3429
2867c8b03487769919c05e7d4695469befee193df003487584d75bd2640c2810715781c4a8a5a78dac3a01d4c4c07762f025a8a9e35292e3d10e2cc6096e035bf85ef07b
b1d7966b41e4a2c1b27721cd6098d3a1a4fd4315603e426f0539bc64e3369bb27fe78b912b9ef4df40c9150737132b8b9b8f11556ea0cd97a2aa55a82bcb5c0aaf1439ab9
ffd9c9
admin >
```

*Command Line Interface – ethtool*

# GSM - [lscpu]

Used to display information about the CPU architecture.

How to use:

```
admin >lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) per core:    1
Core(s) per socket:    4
Socket(s):              1
NUMA node(s):          1
Vendor ID:              GenuineIntel
CPU family:             6
Model:                  55
Model name:             Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
Stepping:               8
CPU MHz:                2400.093
BogoMIPS:               4000.16
Virtualization:         VT-x
L1d cache:              24K
L1i cache:              32K
L2 cache:               1024K
NUMA node0 CPU(s):     0-3
admin >
```

Command Line Interface – lscpu

# GSM - [mkfs]

Used to perform formatting. You will need to determine which device will be formatted. Ex: mkfs -t ext4 / dev / sdb;

How to use:

```
admin >mkfs
Usage: mkfs.ext4 [-c|-l filename] [-b block-size] [-C cluster-size]
        [-i bytes-per-inode] [-I inode-size] [-J journal-options]
        [-G flex-group-size] [-N number-of-inodes]
        [-m reserved-blocks-percentage] [-o creator-os]
        [-g blocks-per-group] [-L volume-label] [-M last-mounted-directory]
        [-O feature[,...]] [-r fs-revision] [-E extended-option[,...]]
        [-t fs-type] [-T usage-type ] [-U UUID] [-jnqvDFKSV] device [blocks-count]
admin >
```

Command Line Interface – mkfs

## GSM - [more]

Used to paginate files or standard inputs. It is possible to direct the output of another command using the pipe "|".

**How to use:** Use the "more" command as output from another command that returns a very extensive amount of information.

```
admin >iplist | more
ZONE LAN (1) 5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.16.20.1/24 brd 172.16.20.255 scope global eth3
        valid_lft forever preferred_lft forever
eth3: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 8: eth0.102@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.102.1/24 brd 172.16.102.255 scope global eth0.102
        valid_lft forever preferred_lft forever
eth0.102: negotiated 1000baseT-FD flow-control, link ok

ZONE DMZ (2) 7: eth0.101@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
noqueue state UP
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.101.1/24 brd 172.16.101.255 scope global eth0.101
        valid_lft forever preferred_lft forever
eth0.101: negotiated 1000baseT-FD flow-control, link ok
ZONE LAN (1)
ZONE LAN (1) 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:0b:ab:ac:a3:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.16.12.1/23 brd 172.16.13.255 scope global eth0
        valid_lft forever preferred_lft forever
eth0: negotiated 1000baseT-FD flow-control, link ok
[--csv|-C] [--raw] [--xml] [--split] [--mpls] [--no-dns]
    [--show-ips] [--address interface] [--filename=FILE|-F]
    [--ipinfo=item_no|-y item_no] [--aslookup|-z]
    [--psize=bytes/-s bytes] [--order fields]
    [--report-wide|-w] [--inet] [--inet6] [--max-ttl=NUM] [--first-
ttl=NUM]
    [--bitpattern=NUM] [--tos=NUM] [--udp] [--tcp] [--port=PORT] [--
timeout=SECONDS]
    [--interval=SECONDS] HOSTNAME
admin >
```

*Command Line Interface – more*

# GSM - [netstat]

Used to display listening ports on the server.

How to use:

```
admin >netstat
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 127.0.0.1:20518         0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:4200           0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:10519        0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:1464         0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:9497         0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:42971        0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:64668        0.0.0.0:*               LISTEN
tcp      0      0 0.0.0.0:444            0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:63551        0.0.0.0:*               LISTEN
tcp      0      0 127.0.0.1:49571        0.0.0.0:*               LISTEN
tcp6     0      0 :::80                  :::*                    LISTEN
tcp6     0      0 :::443                  :::*                    LISTEN
udp      0      0 0.0.0.0:123            0.0.0.0:*               *
udp      0      0 127.0.0.1:323          0.0.0.0:*               *
udp6     0      0 :::123                  :::*                    *
udp6     0      0 :::1:323                :::*                    *
admin >
```

*Command Line Interface – netstat*

# GSM - [ntpdate]

Used to set your device's date and local time by querying network NTP (Network Time Protocol) servers available on the network.

**How to use:**

```
admin >ntpdate -h

/sbin/ntpdate: unknown option -h
usage: /sbin/ntpdate [-46bBdqsuV] [-a key#] [-e delay] [-k file] [-p samples] [-o
version#] [-t timeo] [-U username] server ...
admin >
```

*Command Line Interface – ntpdate*

**Example:** Update the date and time with public NTP servers:

```
admin >ntpdate a.ntp.br
1 Sep 18:06:33 ntpdate[8569]: adjust time server 200.160.0.8 offset -0.000371 sec
admin >
```

*Command Line Interface – ntpdate – Example*

# GSM - [passwd]

Used to set or change the default admin password for the user

How to use:

```
admin >passwd
Mudando senha para o usuário admin.
Mudando senha para admin.
Senha UNIX (atual):
Nova senha:
Redigite a nova senha:
passwd: todos os tokens de autenticações foram atualizados com sucesso.
admin >
```

*Command Line Interface – passwd*

# GSM - [ping]

Used to test connectivity between devices on the network. Uses the ICMP protocol datagram

How to use:

```
admin >ping 192.168.1.99
PING 192.168.1.99 (192.168.1.99) 56(84) bytes of data.
64 bytes from 192.168.1.99: icmp_seq=1 ttl=128 time=2.65 ms
64 bytes from 192.168.1.99: icmp_seq=2 ttl=128 time=1.55 ms
64 bytes from 192.168.1.99: icmp_seq=3 ttl=128 time=6.86 ms
64 bytes from 192.168.1.99: icmp_seq=4 ttl=128 time=4.16 ms
64 bytes from 192.168.1.99: icmp_seq=5 ttl=128 time=16.5 ms
64 bytes from 192.168.1.99: icmp_seq=6 ttl=128 time=1.87 ms
64 bytes from 192.168.1.99: icmp_seq=7 ttl=128 time=4.58 ms
64 bytes from 192.168.1.99: icmp_seq=8 ttl=128 time=2.20 ms
64 bytes from 192.168.1.99: icmp_seq=9 ttl=128 time=1.61 ms
64 bytes from 192.168.1.99: icmp_seq=10 ttl=128 time=3.89 ms
^C
--- 192.168.1.99 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 1.553/4.598/16.589/4.298 ms
admin >
```

Command Line Interface – ping



# GSM - [reboot]

Used to reboot the system.

**How to use:** [Standard command output]:

```
admin >reboot  
Connection to 192.168.1.1 closed by remote host.  
Connection to 192.168.1.1 closed.
```

*Command Line Interface – reboot*

# GSM - [reset]

Used to reset the system.

**How to use:**

```
admin >reset
```

Command Line Interface – reset

# GSM - [reset-admin-blocks]

Used to release blocked sessions for the WEB interface "admin" user.

**How to use:** [Standard command output]:

```
Modo de uso [Saída padrão do comando]
admin >reset-admin-blocks
blocked sessions removed
admin >
```

*Command Line Interface – reset-admin-blocks – Example*

# GSM - [reset-admin-password]

Used to apply a reset of the WEB interface "admin" user password. Automatically prompted to create a new password.

**How to use:** [Standard command output]:

```
admin >reset-admin-password  
Type admin password:  
Re-type admin password:  
admin >
```

Command Line Interface – reset-admin-password

# GSM - [reset-admin-sessions]

Used to remove "Active" sessions from the WEB interface admin user.

**How to use:** [Standard command output]:

```
admin >reset-admin-sessions  
admin sessions removed  
admin >
```

Command Line Interface – reset-admin-sessions

# GSM - [reset-logs]

Delete all logs from the analyzer.

**How to use:** [Standard command output]:

```
admin >reset-logs  
admin >
```

*Command Line Interface – reset-logs*

# GSM - [rewizard]

Used to apply a reset in the Blockbit GSM device settings. This command should only be used in cases of real need for total system reconfiguration.

**How to use:** [Standard command output]:

```
admin >rewizard -d
Do you want to reset this device (y/n)?y
omne-apply-cluster-reset: running
omne-apply-cluster-reset: stop postgres
omne-apply-cluster-reset: remove wizard flag
omne-apply-cluster-reset: remove databases
omne-apply-cluster-reset: remove sessions
omne-apply-cluster-reset: remove known_hosts
omne-apply-cluster-reset: finish
admin >
```

*Command Line Interface – rewizard*

# GSM - [route]

Used to display and manipulate the IP address routing table.

How to use:

```
admin >route -h
Uso: route [-nNvee] [-FC] [famílias_de_endereços] Lista as tabelas de rotea-
                                                mento do kernel
route [-v] [-FC] {add|del|flush} ... Modifica tabela de rotea-
                                                mento da família.

route {-h|--help} [família_de_endereços] Sintaxe para a AF (Família
route {-V|--version} Mostra a versão do comando e sai.

-v, --verbose listagem detalhada
-n, --numeric don't resolve names
-e, --extend mostra outras/mais informações
-F, --fib mostra a Base de Informações de Repasse (default)
-C, --cache mostra cache de roteamento no lugar da FIB

<AF>=Use -4, -6, '-A <af>' or '--<af>'; default: inet
Lista das famílias de endereços possíveis (que suportam roteamento):
inet (DARPA Internet) inet6 (IPv6) ax25 (AX.25 AMPR)
netrom (NET/ROM AMPR) ipx (Novell IPX) ddp (Appletalk DDP)
x25 (CCITT X.25)
admin >
```

Command Line Interface – route

Static routes added through the CLI console (command line) are not saved and are not loaded after booting

Example 1.: [Standard command output]:

```
admin >route -n
Tabela de Roteamento IP do Kernel
Destino Roteador MáscaraGen. Opções Métrica Ref Uso Iface
0.0.0.0 192.168.0.1 0.0.0.0 UG 0 0 0 eth1
192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
admin >
```

Command Line Interface – route – Example 1

Example 2: Configuring static routing for an extended network:



```

admin >route add -net 192.168.254.0/24 gw 172.16.102.1 dev eth3
admin >
admin >route -n
Tabela de Roteamento IP do Kernel
Destino      Roteador      MáscaraGen.    Opções Métrica Ref  Uso Iface
0.0.0.0      192.168.0.1    0.0.0.0        UG      0      0      0 eth1
172.16.102.0 0.0.0.0        255.255.255.0  U      0      0      0 eth3
192.168.0.0   0.0.0.0        255.255.255.0  U      0      0      0 eth1
192.168.1.0   0.0.0.0        255.255.255.0  U      0      0      0 eth0
192.168.254.0 172.16.102.1   255.255.255.0  UG      0      0      0 eth3
admin >

```

Command Line Interface – route – Example 2

# GSM - [sar]

Used to display system activity reports.

How to use:

```
admin >sar
Linux 3.10.0-229.20.1.el7.x86_64 (host.blockbit.com) 11/22/18 _x86_64_ (4 CPU)

00:00:01      CPU      %user      %nice      %system      %iowait      %steal      %idle
00:10:01      all       1.45       0.00       0.98       0.06       0.00      97.51
00:20:01      all       1.44       0.00       0.97       0.01       0.00      97.58
00:30:01      all       1.44       0.00       0.99       0.11       0.00      97.46
00:40:01      all       1.41       0.00       1.01       0.03       0.00      97.55
00:50:01      all       1.39       0.00       0.96       0.01       0.00      97.65
01:00:01      all       1.41       0.00       0.96       0.01       0.00      97.63
01:10:01      all       1.12       0.00       0.77       0.01       0.00      98.10
01:20:01      all       1.44       0.00       1.04       0.01       0.00      97.51
01:30:01      all       1.42       0.00       1.01       0.01       0.00      97.56
01:40:01      all       1.49       0.00       1.03       0.01       0.00      97.47
01:50:01      all       1.50       0.00       1.03       0.01       0.00      97.47
02:00:01      all       1.39       0.00       0.98       0.15       0.00      97.48
02:10:01      all       1.40       0.00       0.98       0.04       0.00      97.58
02:20:01      all       1.43       0.00       0.97       0.01       0.00      97.60
02:30:01      all       1.36       0.00       0.94       0.01       0.00      97.70
02:40:01      all       1.39       0.00       0.95       0.01       0.00      97.65
02:50:02      all       1.39       0.00       0.97       0.01       0.00      97.64
03:00:01      all       1.43       0.00       0.99       0.01       0.00      97.58
03:10:01      all       1.43       0.00       1.00       0.01       0.00      97.56
03:20:01      all       1.49       0.00       1.07       0.01       0.00      97.43
03:30:01      all       1.45       0.00       1.02       0.01       0.00      97.52
03:40:01      all       1.37       0.00       0.95       0.01       0.00      97.66
03:50:01      all       1.32       0.00       0.94       0.03       0.00      97.71
04:00:01      all       1.49       0.00       1.09       0.02       0.00      97.39
04:10:01      all       1.46       0.00       1.02       0.01       0.00      97.51
04:20:01      all       1.45       0.00       1.04       0.02       0.00      97.49
04:30:01      all       1.42       0.00       0.97       0.03       0.00      97.58
04:40:01      all       1.42       0.00       0.98       0.01       0.00      97.59
04:50:01      all       1.39       0.00       0.97       0.01       0.00      97.63
05:00:01      all       1.43       0.00       1.00       0.01       0.00      97.57
05:10:01      all       1.47       0.00       1.05       0.01       0.00      97.47
05:20:01      all       1.49       0.00       1.10       0.01       0.00      97.40
05:30:01      all       1.49       0.00       1.06       0.09       0.00      97.35
05:40:01      all       1.46       0.00       1.05       0.04       0.00      97.44
05:50:01      all       1.46       0.00       1.03       0.01       0.00      97.51
06:00:01      all       1.46       0.00       1.03       0.01       0.00      97.50

06:00:01      CPU      %user      %nice      %system      %iowait      %steal      %idle
06:10:01      all       1.43       0.00       1.03       0.01       0.00      97.53
06:20:01      all       1.43       0.00       0.98       0.01       0.00      97.59
06:30:02      all       1.45       0.00       1.01       0.01       0.00      97.53
06:40:01      all       1.38       0.00       0.94       0.01       0.00      97.68
06:50:01      all       1.21       0.00       0.85       0.01       0.00      97.93
07:00:01      all       1.41       0.00       1.02       0.01       0.00      97.57
07:10:01      all       0.98       0.00       0.68       0.01       0.00      98.33
07:20:01      all       1.41       0.00       1.03       0.01       0.00      97.55
07:30:01      all       1.44       0.00       0.97       0.01       0.00      97.59
07:40:01      all       1.42       0.00       0.98       0.01       0.00      97.59
07:50:01      all       1.38       0.00       0.94       0.01       0.00      97.66
08:00:01      all       1.41       0.00       0.95       0.01       0.00      97.63
08:10:01      all       1.40       0.00       0.95       0.01       0.00      97.64
08:20:01      all       1.42       0.00       0.97       0.01       0.00      97.60
08:30:01      all       1.42       0.00       0.98       0.07       0.00      97.53
08:40:01      all       1.43       0.00       1.00       0.07       0.00      97.50
08:50:01      all       1.43       0.00       0.98       0.01       0.00      97.58
09:00:01      all       1.45       0.00       1.00       0.01       0.00      97.55
09:10:01      all       1.45       0.00       1.03       0.01       0.00      97.52
09:20:01      all       1.48       0.00       1.03       0.01       0.00      97.48
09:30:01      all       1.49       0.00       1.07       0.01       0.00      97.43
09:40:01      all       1.49       0.00       1.03       0.01       0.00      97.47
Average:      all       1.41       0.00       0.99       0.02       0.00      97.58
admin >
```

Command Line Interface – sar

# GSM - [set-network-dns]

Configures the DNS address on the server.

**How to use:**

```
admin >set-network-dns 176.16.102.161  
admin >
```

Command Line Interface – set-network-dns

# GSM - [set-network-gateway]

Used to set the network gateway.

**How to use:**

```
admin >set-network-gateway 172.31.0.1  
admin >
```

*Command Line Interface – set-network-gateway*

# GSM - [set-network-hostname]

This command has the function of allowing the administrator user to define the hostname of the system through the CLI.

```
admin >set-network-hostname -h
hostnamectl [OPTIONS...] COMMAND ...

Query or change system hostname.

  -h --help                Show this help
  --version                Show package version
  --no-ask-password        Do not prompt for password
  -H --host=[USER@]HOST    Operate on remote host
  -M --machine=CONTAINER  Operate on local container
  --transient              Only set transient hostname
  --static                 Only set static hostname
  --pretty                 Only set pretty hostname

Commands:
  status                   Show current hostname settings
  set-hostname NAME       Set system hostname
  set-icon-name NAME       Set icon name for host
  set-chassis NAME         Set chassis type for host
  set-deployment NAME     Set deployment environment for host
  set-location NAME        Set location for host
admin >
```

Command Line Interface – set-network-hostname

## How to use:

To define the hostname, just type the command and add the desired name, as shown below:


```
admin >set-network-hostname test
admin >
```

Command Line Interface - set-network-hostname - Example

If the device is of the Manager type, the command will apply the hostname information so that it appears when accessing the interface located in the Hostname field under [System in the "General" tab](#). An example is shown below:

# System

[General](#) [License](#) [Updates](#) [Backups](#) [Storages](#) [High Availability](#)

Settings 


**Hostname**

test


**Domain**

blockbit.com

**Timezone**

America/Sao\_Paulo - Brazil (southeast: GO, DF, MG, ES, RJ, SP, PR, SC, RS) 

**\* Language**

Portuguese 

Settings - System - General

In addition, it is possible to run the command `hostname`, as shown below:

```
admin >hostname  
test
```

Command Line Interface – hostname

If the device is of the Logger type, the command will apply the hostname information only to the Operating System.

# GSM - [set-network-interface]

Configures the network interface. You must determine the interface, address, and mask in front of the command as shown below:

**How to use:** [Standard command output]:

```
admin >set-network-interface --interface eth0 --address 172.31.102.235 --mask 255.255.0.0
admin >
```

*Command Line Interface – set-network-interface.*

# GSM - [set-network-timezone]

Used to determine network timezone.

**How to use:**

```
admin >set-network-timezone America/Sao_Paulo  
admin >
```

*Command Line Interface – set-network-timezone*



# GSM - [show-devices]

Displays a listing with the names and IDs of all devices registered in the GSM.

**How to use:**

```
admin >show-devices
Device Name: '172.31.208.13'; Device ID: '6384'
Device Name: '172.31.208.14'; Device ID: '18655'
Device Name: '172.31.208.66'; Device ID: '1940'
Device Name: '172.31.208.12'; Device ID: '55754'
Device Name: '172.31.208.140'; Device ID: '54942'
Device Name: '172.31.208.80'; Device ID: '25916'
Device Name: 'UTM QA - 172.16.100.5'; Device ID: '64403'
Device Name: 'UTM MASTER'; Device ID: '6704'
admin >
```

Command Line Interface – show-devices

# GSM - [show-license]

Displays information about the license.

**How to use:**

```
Type '?' or 'help' to get the list of allowed commands  
admin >show-license  
3F1F-6A54-83AE-F837  
admin >
```

*Command Line Interface – show-license*

## GSM - [show-uuid]

Used to display the Blockbit GSM identification number. This ID is used for identifying the hardware for validation of the use license.

**How to use:** [Standard command output]:

```
admin >show-uuid  
BlockBit Network Appliance UUID  
94248368-3E53-11E6-AE26-EDD8677A1442  
admin >
```

Command Line Interface – show-uuid

# GSM - [show-version]

Command to display version information.

**How to use:**

```
admin >show-version  
BLOCKBIT UTM 1.5.1 build 18103013  
admin >█
```

*Command Line Interface – show-version*

# GSM - [shutdown]

Used to turn off the system.

**How to use:** [Standard command output]:

```
admin >shutdown -h  
Connection to 192.168.1.1 closed by remote host.  
Connection to 192.168.1.1 closed.
```

*Command Line Interface – shutdown*

# GSM - [tcpdump]

Used to monitor, capture, and analyze packets being transmitted over the network. Thus, it allows the administrator to analyze the behavior of the network, aiding in the identification of problems, infected stations, malicious traffic, bottlenecks, etc.

How to use:

```
admin >tcpdump -h
tcpdump version 4.5.1
libpcap version 1.5.3
Usage: tcpdump [-aAbCdEfHIJKLlNOpqRStuUvX] [-B size] [-c count]
               [-C file_size] [-E algo:secret] [-F file] [-G seconds]
               [-i interface] [-j tstamptype] [-M secret]
               [-P in|out|inout]
               [-r file] [-s snaplen] [-T type] [-V file] [-w file]
               [-W filecount] [-y datalinktype] [-z command]
               [-Z user] [expression]

admin >
```

Command Line Interface – tcpdump

**Example:** Monitor all local network interface traffic - Eth0 interface:

```
admin >tcpdump -i eth0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:35:53.129859 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 220346669, win 53006,
length 0
20:35:53.133304 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.142155 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 1:189, ack 0, win
21, length 188
20:35:53.142216 IP utm.ssh > 172.16.12.80.58139: Flags [P.], seq 189:225, ack 0, win
21, length 36
20:35:53.142419 IP 172.16.12.80.58139 > utm.ssh: Flags [.], ack 225, win 52950,
length 0
20:35:53.144878 IP utm.28489 > 172.16.13.245.domain: 49669+ PTR? 80.12.16.172.in-
addr.arpa. (43)
20:35:53.145312 IP 172.16.13.245.58067 > google-public-dns-a.google.com.domain:
12406+ [1au] PTR? 80.12.16.172.in-addr.arpa. (54)
20:35:53.151967 IP 172.16.12.144.36793 > 13.68.106.67.26886: UDP, length 182
20:35:53.158607 IP google-public-dns-a.google.com.domain > 172.16.13.245.58067: 12406
NXDomain 0/0/1 (54)
20:35:53.158889 IP 172.16.13.245.domain > utm.28489: 49669 NXDomain 0/0/0 (43)
Admin >
```

Command Line Interface – tcpdump – Example

# GSM - [tcptop]

Used to extract and display traffic information from network interfaces, such as total packets captured, total packets received total packets blocked by the kernel, and total packets trafficked by the TOP 10 IP addresses.

**How to use:**

```
Modo de uso
admin >tcptop
you must specify the interface: [eth0,eth1 ...]
admin >
```

Command Line Interface – tcptop

**Example:** Display top 10 traffic information for eth1 interface:

```
admin >tcptop eth1
Wait capturing frames ...
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
10000 packets captured
10070 packets received by filter
21 packets dropped by kernel
 3268 IP 177.185.5.137
 3090 IP 192.168.0.2
 1626 IP 192.168.3.2
  481 IP 201.86.139.109
  290 IP 8.8.8.8 > 192
  288 IP 192.168.3.2 > 8
  246 IP 201.31.172.3
admin >
```

Command Line Interface – tcptop – Example

# GSM - [telnet]

Used for remote access and simulation tests of a terminal. Can be used for connection response testing of service and even sending tests of an email message.

How to use:

```
admin >telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-8] [-E] [-L] [-S tos] [-a] [-c] [-d] [-e char] [-l user]
        [-n tracefile] [-b hostalias ] [-r]
        [host-name [port]]
admin >
```

*Command Line Interface – telnet*

**Example:** [Standard command output]:

```
admin >telnet
telnet> ?
Commands may be abbreviated.  Commands are:

close          close current connection
logout         forcibly logout remote user and close the connection
display        display operating parameters
mode           try to enter line or character mode ('mode ?' for more)
open           connect to a site
quit           exit telnet
send           transmit special characters ('send ?' for more)
set            set operating parameters ('set ?' for more)
unset          unset operating parameters ('unset ?' for more)
status         print status information
toggle         toggle operating parameters ('toggle ?' for more)
slc            change state of special charaters ('slc ?' for more)
z             suspend telnet
!             invoke a subshell
environ        change environment variables ('environ ?' for more)
?             print help information
telnet>
```

*Command Line Interface – telnet – Example*

**Example 1:** Connection Tests with a Remote Service Ts (Terminal Service) on a Specific Port:

```
admin >telnet 172.16.13.245 3389
Trying 172.16.13.245...
Connected to 172.16.13.245.
Escape character is '^['.
```

*Command Line Interface – telnet – Example 1*

**Example 2:** Connection tests with a remote service on a specific port with the connection failure response:



```
admin >telnet 172.16.102.11 22
Trying 172.16.102.11...
telnet: connect to address 172.16.102.11: Connection timed out
admin >
```

*Command Line Interface – telnet – Example 2*

# GSM - [tracpath]

Used to plot a path to a designated network address, reporting the "lifetime" or TTL lag and the maximum transmission unit (MTU) along the path.

How to use:

```
admin >tracpath -h
Usage: tracpath [-n] [-b] [-l <len>] [-p port] <destination>
admin >
Exemplo: Testes para traçar o roteamento ou caminho até o end. www.google.com.br
especificando a porta TCP/80 (http).
admin >tracpath -p 3389 172.16.13.245
1?: [LOCALHOST] pmtu 1500
1: 172.16.13.245 0.555ms reached
Resume: pmtu 1500 hops 1 back 128
admin >tracpath -n -b -p 80 www.google.com
1?: [LOCALHOST] pmtu 1500
1: 10.70.64.1 (10.70.64.1) 13.510ms
1: 10.70.64.1 (10.70.64.1) 12.625ms
2: 201.6.37.65 (c9062541.virtua.com.br) 12.592ms
3: 201.6.40.37 (c9062825.virtua.com.br) 11.712ms
4: 201.6.42.93 (c9062a5d.virtua.com.br) 11.800ms
5: no reply
6: no reply
7: no reply
8: no reply
9: no reply
10: no reply
11: no reply
12: no reply
13: no reply
14: no reply
15: no reply
16: no reply
17: no reply
18: no reply
19: no reply
20: no reply
21: no reply
22: no reply
23: no reply
24: no reply
25: no reply
26: no reply
27: no reply
28: no reply
29: no reply
30: no reply
31: no reply
Too many hops: pmtu 1500
Resume: pmtu 1500
admin >
```

Command Line Interface – tracpath

**Example:** Test to trace the route or path to the address [www.google.com](http://www.google.com) specifying TCP / 80 port (HTTP).

# GSM - [traceroute]

Used to map a path to a designated network address. The "traceroute" command supports some advanced parameters that differentiate it from "tracpath", including the selection of protocols, such as TCP, UDP, ICMP or others.

How to use:

```
admin >traceroute --help
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m
max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [
-q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]

Options:
  -4                      Use IPv4
  -6                      Use IPv6
  -d --debug              Enable socket level debugging
  -F --dont-fragment      Do not fragment packets
  -f first_ttl --first=first_ttl
                          Start from the first_ttl hop (instead from 1)
  -g gate,... --gateway=gate,...
                          Route packets through the specified gateway
                          (maximum 8 for IPv4 and 127 for IPv6)
  -I --icmp               Use ICMP ECHO for tracerouting
  -T --tcp                Use TCP SYN for tracerouting (default port is 80)
  -i device --interface=device
                          Specify a network interface to operate with
  -m max_ttl --max-hops=max_ttl
                          Set the max number of hops (max TTL to be
                          reached). Default is 30
  -N squeries --sim-queries=squeries
                          Set the number of probes to be tried
                          simultaneously (default is 16)
  -n                      Do not resolve IP addresses to their domain names
  -p port --port=port
                          Set the destination port to use. It is either
                          initial udp port value for "default" method
                          (incremented by each probe, default is
                          33434), or initial seq for "icmp" incremented
                          as well, default from 1), or some constant
                          destination port for other methods (with default of 80
                          for "tcp", 53 for "udp", etc.)
```

Command Line Interface – traceroute\_1

```

-t tos --tos=tos          Set the TOS (IPv4 type of service) or TC (IPv6
                           traffic class) value for outgoing packets
-l flow_label --flowlabel=flow_label
                           Use specified flow_label for IPv6 packets
-w waittime --wait=waittime
                           Set the number of seconds to wait for response
                           to a probe (default is 5.0). Non-integer (float
                           point) values allowed too
-q nqueries --queries=nqueries
                           Set the number of probes per each hop. Default is 3
-r                          Bypass the normal routing and send directly to a
                           host on an attached network
-s src_addr --source=src_addr
                           Use source src_addr for outgoing packets
-z sendwait --sendwait=sendwait
                           Minimal time interval between probes (default 0).
                           If the value is more than 10, then it specifies a
                           number in milliseconds, else it is a number of
                           seconds (float point values allowed too)
-e --extensions            how ICMP extensions (if present), including MPLS
-A --as-path-lookups       Perform AS path lookups in routing registries and
                           print results directly after the corresponding
                           addresses
-M name --module=name      Use specified module (either builtin or external)
                           for traceroute operations. Most methods have
                           their shortcuts (`-I' means `-M icmp' etc.)

-O OPTS,... --options=OPTS,...
                           Use module-specific option OPTS for the

```

Command Line Interface – traceroute\_2

```

--sport=num               traceroute module. Several OPTS allowed,
                           separated by comma. If OPTS is "help", print
                           info about available options
--fwmark=num              Use source port num for outgoing packets.
                           Implies '-N 1'
-U --udp                  Set firewall mark for outgoing packets
                           Use UDP to particular port for tracerouting
                           (instead of increasing the port per each probe),
                           default port is 53
-UL                       Use UDPLITE for tracerouting (default dest port
                           is 53)
-D --dccp                 Use DCCP Request for tracerouting (default port
                           is 33434)
-P prot --protocol=prot   Use raw packet of protocol prot for tracerouting
--mtu                     Discover MTU along the path being traced. Implies
                           '-F -N 1'
--back                    Guess the number of hops in the backward path and
                           print if it differs
-V --version              Print version info and exit
--help                    Read this help and exit

Arguments:
+   host                  The host to traceroute to
    packetlen             The full packet length (default is the length of an IP
                           header plus 40). Can be ignored or increased to a minimal
                           allowed value

admin >

```

Command Line Interface – traceroute\_3

**Example:** Tests to trace the routing or path to the Google DNS IP address, IP 8.8.8.8 in the UDP protocol (17):

```
admin >tracert -n -p 53 -t 17 8.8.8.8
tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.70.64.1  15.412 ms  15.242 ms  15.152 ms
 2  201.6.37.65  15.607 ms  15.618 ms  15.566 ms
 3  201.6.40.37  15.511 ms  16.380 ms  21.774 ms
 4  201.6.42.93  22.970 ms  22.917 ms  22.697 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
...
27  * * *
28  * * *
29  * * *
30  * * *
admin >
```

Command Line Interface – traceroute – Example 1

# GSM - [update-gsm]

Used to check, download and install GSM Blockbit update packages.

How to use: [Standard command output]:

```
admin >update-gsm
Loaded plugins: fastestmirror
Determining fastest mirrors
gsm-apply-update: running
gsm-apply-update: >/etc/yum.repos.d/BlockBit-centos.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-epel.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-gsm.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-bases.repo
gsm-apply-update: >/etc/yum.repos.d/BlockBit-elastic.repo
gsm-apply-update: update system packages
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
bases-local | 2.9 kB 00:00:00
centos-local | 2.9 kB 00:00:00
elastic-local | 2.9 kB 00:00:00
epel-local | 2.9 kB 00:00:00
gsm-local | 2.9 kB 00:00:00
(1/15): bases-local/2.0/x86_64/filelists_db | 2.9 kB 00:00:00
(2/15): bases-local/2.0/x86_64/primary_db | 24 kB 00:00:01
(3/15): bases-local/2.0/x86_64/other_db | 43 kB 00:00:01
(4/15): centos-local/2.0/x86_64/filelists_db | 19 kB 00:00:00
(5/15): elastic-local/2.0/x86_64/primary_db | 370 kB 00:00:04
(6/15): elastic-local/2.0/x86_64/other_db | 13 kB 00:00:01
(7/15): centos-local/2.0/x86_64/primary_db | 1.1 kB 00:00:00
(8/15): centos-local/2.0/x86_64/other_db | 857 kB 00:00:06
(9/15): elastic-local/2.0/x86_64/primary_db | 211 kB 00:00:02
(10/15): elastic-local/2.0/x86_64/other_db | 202 kB 00:00:02
(11/15): epel-local/2.0/x86_64/primary_db | 6.9 kB 00:00:00
(12/15): epel-local/2.0/x86_64/filelists_db | 2.9 kB 00:00:01
(13/15): epel-local/2.0/x86_64/other_db | 5.1 kB 00:00:00
(14/15): gsm-local/2.0/x86_64/primary_db | 44 kB 00:00:01
(15/15): gsm-local/2.0/x86_64/other_db | 3.3 kB 00:00:00
(15/15): gsm-local/2.0/x86_64/filelists_db | 1.7 MB 00:00:07
Metadata Cache Created
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Resolving Dependencies
--> Running transaction check
--> Package atp-blacklist.x86_64 0:202011020812-0.el7.centos will be updated
--> Package atp-blacklist.x86_64 0:202102150811-0.el7.centos will be an update
--> Package atp-geoip.x86_64 0:202011020901-0.el7.centos will be updated
--> Package atp-geoip.x86_64 0:202102150901-0.el7.centos will be an update
--> Package atp-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package atp-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package bbos-scripts.x86_64 0:2.0.6-80 will be updated
--> Package bbos-scripts.x86_64 0:2.0.7-69 will be an update
--> Package gsm-apply.x86_64 0:2.0.6-80 will be updated
--> Package gsm-apply.x86_64 0:2.0.7-69 will be an update
--> Package gsm-backend.x86_64 0:2.0.6-80 will be updated
--> Package gsm-backend.x86_64 0:2.0.7-69 will be an update
--> Package gsm-console.x86_64 0:2.0.6-80 will be updated
--> Package gsm-console.x86_64 0:2.0.7-69 will be an update
--> Package gsm-manager.x86_64 0:2.0.6-80 will be updated
--> Package gsm-manager.x86_64 0:2.0.7-69 will be an update
--> Package gsm-repos.x86_64 0:2.0.6-80 will be updated
--> Package gsm-repos.x86_64 0:2.0.7-69 will be an update
--> Package gsm-schema.x86_64 0:2.0.6-80 will be updated
--> Package gsm-schema.x86_64 0:2.0.7-69 will be an update
--> Package ips-threats.x86_64 0:202011030809-0.el7.centos will be updated
--> Package ips-threats.x86_64 0:202102160809-0.el7.centos will be an update
--> Package wgs-class.x86_64 0:20201030800-0.el7.centos will be updated
--> Package wgs-class.x86_64 0:202102120800-0.el7.centos will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Updating:
atp-blacklist x86_64 202102150811-0.el7.centos bases-local 1.2 M
atp-geoip x86_64 202102150901-0.el7.centos bases-local 12 M
atp-threats x86_64 202102160809-0.el7.centos bases-local 2.7 M
bbos-scripts x86_64 2.0.7-69 gsm-local 14 k
gsm-apply x86_64 2.0.7-69 gsm-local 43 k
gsm-backend x86_64 2.0.7-69 gsm-local 65 k
gsm-console x86_64 2.0.7-69 gsm-local 20 k
gsm-manager x86_64 2.0.7-69 gsm-local 76 M
gsm-repos x86_64 2.0.7-69 gsm-local 11 k
gsm-schema x86_64 2.0.7-69 gsm-local 25 k
ips-threats x86_64 202102160809-0.el7.centos bases-local 1.4 M
wgs-class x86_64 202102120800-0.el7.centos bases-local 285 M
=====

Transaction Summary
=====
Upgrade 12 Packages

Total download size: 378 M
Downloading packages:
Delta RPMs disabled because /usr/bin/applydeltarpm not installed.
warning: /var/cache/yum/x86_64/2.0/bases-local/packages/atp-blacklist-202102150811-0.el7.centos.x86_64.rpm: Header V4 RSA/SHA1 Signature,
key ID b08c6759: NOKEY
Public key for atp-blacklist-202102150811-0.el7.centos.x86_64.rpm is not installed
(1/12): atp-blacklist-202102150811-0.el7.centos.x86_64.rpm | 1.2 MB 00:00:06
Public key for bbos-scripts-2.0.7-69.x86_64.rpm is not installed ] 647 kB/s | 4.0 MB 00:09:52 ETA
(2/12): bbos-scripts-2.0.7-69.x86_64.rpm | 14 kB 00:00:01
(3/12): gsm-apply-2.0.7-69.x86_64.rpm | 43 kB 00:00:01
(4/12): gsm-console-2.0.7-69.x86_64.rpm | 20 kB 00:00:00
(5/12): gsm-backend-2.0.7-69.x86_64.rpm | 65 kB 00:00:01
(6/12): gsm-repos-2.0.7-69.x86_64.rpm | 11 kB 00:00:00
(7/12): gsm-schema-2.0.7-69.x86_64.rpm | 25 kB 00:00:00
(8/12): atp-threats-202102160809-0.el7.centos.x86_64.rpm | 2.7 MB 00:00:05
(9/12): atp-geoip-202102150901-0.el7.centos.x86_64.rpm | 12 MB 00:00:12
(10/12): ips-threats-202102160809-0.el7.centos.x86_64.rpm | 1.4 MB 00:00:03
(11/12): gsm-manager-2.0.7-69.x86_64.rpm | 76 MB 00:00:25
(12/12): wgs-class-202102120800-0.el7.centos.x86_64.rpm | 285 MB 00:01:05
=====
Total 4.9 MB/s | 378 MB 00:01:17
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-BlockBit
Importing GPG key 0xB08C6759:
```



The screenshot above does not represent the output of the command in its entirety. The command will release the console when finished and will display the message "gsm-apply-update: finish", to validate that the update was done correctly, use the command "[show-version](#)".

# GSM - [update-license]

Used to register Blockbit UTM through the CLI. License must be entered in front of command. **[Update-license]** should only be used if the license is deactivated and released by Blockbit for activation, it is extremely important to keep in mind that: If this command is executed when the license is already properly activated it will be DEACTIVATED.

## How to use:

```
admin >update-license 3F1F-6A54-83AE-F837
status:true
admin >
```

*Command Line Interface – update-license*

## Atenção



*Attention for the proper use of the [update-license] command: If the command is executed twice, or if it is executed when the license is active, it will be DISABLED. Also, for the correct use of this command it must be released to be able to register it correctly.*



# GSM - [upgrade-blockbit]

This command is used to check, download and upgrade Blockbit GSM to the most current version.



**ATTENTION:** We ALWAYS recommend that a FULL BACKUP of the latest system version and reports be made before any update or upgrade procedure is performed and that the files are saved in a safe place.



The upgrade process interferes with the interfaces configured in standalone type loggers. Therefore, if the user environment has a standalone logger using an interface other than eth0, after the upgrade process, it will be necessary to edit and change the interface so that there is no future redirection problem.

When running the command, the system will ask the user to confirm that all reports have been exported and that a system backup has been generated. For the command to be executed, this double confirmation from the user will be necessary.



**ATTENTION:** At the end of the execution of this command, it will be necessary to restart your GSM.

## How to use:

```
admin >upgrade-blockbit
Are you sure do you want upgrade version 2.0 to 2.1 (restart system is required)? [y/N]y
Have you export all reports? [y/N]y
Have you made a full system backup? [y/N]y

Testing connection to update server:
Connection succeeded

will restart when the upgrade is complete
Upgrading...

- No SSL mode enabled
- Downloading packages
Checking for license...
Checking for available upgrade...
Downloading kernel upgrade...
##### 100.0%
Kernel upgrade downloaded
Kernel upgrade downloaded. Installing...
Checking environment...
Preparing environment...
Environment ok.
Testing installer integrity...
Installer integrity ok.
Unpacking installer...
Installer unpacked.
Running installer...
Finding installation disk...
Mounting installation disk
Installing new kernel files. It will take a while...
Installing new initramfs...
Setting new kernel as bootable...
Cleaning up old entries...
New kernel installed!
Kernel upgraded from 3.10.0-957.10.1 to 5.8.8-1
A reboot is required.
```

Command Line Interface – upgrade-blockbit

# GSM - [uptime]

Displays for how long the server is running.

**How to use:**

```
admin >uptime
 09:57:34 up 16:43,  1 user,  load average: 0.00, 0.01, 0.05
admin >
```

Command Line Interface – uptime

# GSM - [vmstat]

Used to report information about processes, memory, paging, I / O blocks, and CPU activities.

How to use:

```
admin >vmstat --help

Usage:
  vmstat [options] [delay [count]]

Options:
  -a, --active           active/inactive memory
  -f, --forks            number of forks since boot
  -m, --slabs            slabinfo
  -n, --one-header       do not redisplay header
  -s, --stats            event counter statistics
  -d, --disk             disk statistics
  -D, --disk-sum         summarize disk statistics
  -p, --partition <dev> partition specific statistics
  -S, --unit <char>     define display unit
  -w, --wide             wide output
  -t, --timestamp        show timestamp

  -h, --help             display this help and exit
  -V, --version          output version information and exit

For more details see vmstat(8).
admin >
```

Command Line Interface – vmstat

Example: Standard command output:

```
admin >vmstat
procs -----memory----- ---swap-- -----io----- -system-- -----cpu-----
r b swpd free buff cache si so bi bo in cs us sy id wa st
1 0 86316 178524 7820 3685772 0 0 1 9 5 7 1 1 98 0 0
```

Command Line Interface – vmstat - Example

# GSM - [whois]

Used to query information about an Internet domain.

How to use:

```
admin >whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-H                      hide legal disclaimers
                        --verbose    explain what is being done
                        --help      display this help and exit
                        --version    output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l          find the one level less specific match
-L          find all levels less specific matches
-m          find all one level more specific matches
-M          find all levels of more specific matches
-c          find the smallest match containing a mnt-irt attribute
-x          exact match
-b          return brief IP address ranges with abuse contact
-B          turn off object filtering (show email addresses)
-G          turn off grouping of associated objects
-d          return DNS reverse delegation objects too
-i ATTR[,ATTR]...    do an inverse look-up for specified ATTRIBUTES
-T TYPE[,TYPE]...    only look for objects of TYPE
-K          only primary keys are returned
-r          turn off recursive look-ups for contact information
-R          force to show local copy of the domain object even
              if it contains referral
-a          also search all the mirrored databases
-s SOURCE[,SOURCE]... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST  find updates from SOURCE from serial FIRST to LAST
-t TYPE          request template for object of TYPE
-v TYPE          request verbose template for object of TYPE
-q [version|sources|types] query specified server info
admin >
```

Command Line Interface – whois

**Example:** Standard command output:

```

admin >whois www.blockbit.com.br

% Copyright (c) Nic.br
% The use of the data below is only permitted as described in
% Full by the terms of use at https://registro.br/termo/en.html ,
% being prohibited its distribution, commercialization or
% reproduction, in particular, to use it for advertising or
% any similar purpose.
% 2017-05-15 20:28:07 (BRT -03:00)

domain:      blockbit.com.br
owner:       BR CONNECTION COM E SERV DE INFORM LTDA
ownerid:     02.423.535/0001-09
responsible: Clober Ribas
country:     BR
owner-c:     DESBL
admin-c:     LUGSI383
tech-c:      DESBL
billing-c:   LUGSI383
nsrserver:   e.sec.dns.br
nsstat:      20170514 AA
nslastaa:    20170514
nsrserver:   f.sec.dns.br
nsstat:      20170514 AA
nslastaa:    20170514
dsrecord:    15352 RSASHA1 BE22F76C273FA8F48FFE62C87614CEE323CE118D
dsstatus:    20170514 DSOK
dslastok:    20170514
saci:        yes
created:     20161213 #16449760
changed:     20170213
expires:     20181213
status:      published

nic-hdl-br:  DESBL
person:      Departamento de Seguran Blockbit
e-mail:      domain@blockbit.com
country:     BR
created:     20170213
changed:     20170213

nic-hdl-br:  LUGSI383
person:      LUCIANO GOMES DA SILVA
e-mail:      lgomes@blockbit.com
country:     BR
created:     20161105
changed:     20170201

% Security and mail abuse issues should also be addressed to
% cert.br, http://www.cert.br/ , respectively to cert@cert.br
% and mail-abuse@cert.br
%
% whois.registro.br accepts only direct match queries. Types
% of queries are: domain (.br), registrant (tax ID), ticket,
% provider, contact handle (ID), CIDR block, IP and ASN.
admin >

```

Command Line Interface – whois – Example



 [www.blockbit.com](http://www.blockbit.com)

# GSM - Manuals and How tos

This section contains some useful documents for operating the GSM:

How to: [Convert HyperV OVA](#)

Manual: [GSM API](#)