



Corero Network Security

SmartWall Threat Defense Director Central Management Server User Guide

Software 9.7.5

09 December 2020

Part Number: 9101-0975-00-J

Legal and Copyright Information

Corero Network Security, Inc. (Corero) reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of Corero to provide notification of such revision or change. Corero provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. Corero may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If you are a United States government agency, this documentation and the software described herein are provided to you subject to the following:

This paragraph applies to all acquisitions of the software by or for the United States Government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement or other activity with the United States Government (collectively, the "Government"). All technical data and computer software are commercial in nature and developed solely at private expense. The software and documentation respectively are "commercial computer software" and "commercial computer software documentation" as defined in DFARS 252.227-7014 (June 1995) and "commercial items" as defined in FAR 2.101(a) and, to the maximum extent permitted by law, are provided with only such rights as are provided in Corero's standard commercial license for the software and documentation and this notice. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. Corero's standard commercial license for the software and documentation and this notice shall govern the Government's use of the software, documentation, and technical data, and shall supersede any conflicting contractual terms or conditions. If these terms and conditions fail to meet the Government's needs or is inconsistent in any respect with Federal law, the Government must return the software and the documentation unused to Corero. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): "Restricted Rights – Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT. 1988)." The Contractor is Corero Network Security, Inc.

You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this document.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Corero.

The products described in this document are protected by US Patent No. 9,442,782, US Patent No. 10,341,364, and European Patent No. 1319296.

Any software on removable media described in this documentation, is furnished under a license agreement which is located on the Corero web site.

Corero®, First Line of Defense®, SecureWatch®, and SmartWall® are registered trademarks of Corero Network Security, Inc. All other trademarks and registered trademarks are the property of their respective holders.

For warranty, licensing and maintenance agreement information, visit http://www.corero.com/support/End_User_Agreements.html.

Copyright © 2014- 2020, Corero Network Security, Inc.

CONTENTS

Legal and Copyright Information	2
Contents	3
TDD Documentation	12
CoreroSmartWall DDoS Protection Solution	13
SmartWall Threat Defense Director	15
Working with the SmartWall TDD applications and documentation	16
Core Concepts	17
Provisioning Command Line Interface (pCLI)	17
Policy	17
Protection Profiles	17
Clusters	17
Devices	17
Segments	17
Defense Mode	18
Analytics	18
Sampled Traffic	18
Telemetry	18
NETCONF	19
SmartWall Service Portal	19
Accessing the TDD Components	20
SWA	20
CMS	20
vNTD	21

CONTENTS

Supported web browsers for the Web UI	21
Juniper Networks MX Series router	22
Juniper Networks MX Series router requirements	22
Get Started	23
Getting Started	25
View System Status	26
To view the current status of your network	27
Working in the CMS	28
Supported web browsers for the Web UI	28
Web UI Interface	29
Committing your changes	31
Working with different Protection Profiles	31
Web UI default values	31
Notifications	31
Using the CLI	32
Alarms and Notifications	33
Alarm types	33
Perceived severity	33
Notifications	34
Viewing System Alarms	34
Managing the Alarm Handling Log and Status Change list	36
Deleting Alarms	38
Tune Policy	39
Policy	42
TDD deployment policy settings	42

CONTENTS

To open the CMS built in help	42
Protection Profiles	43
Using Protection Profiles	43
Creating Protection Profiles	44
Importing and Exporting Protection Profiles	46
Packet Rules	47
To open the CMS built in help	47
Packet Rules	47
To open the CMS built in help	47
Packet Rules	47
To open the CMS built in help	47
Flex-Rules	48
Flex-Rule Rule Actions	48
Flex-Rule Thresholds and Rate Limits	48
Types of Flex-Rule	50
Flex-Rule Filters	51
Evaluation order	52
Enable/Disable a Flex-Rule	52
Managing Flex-Rules	52
Types of Flex-Rule Filters	56
Managing Flex-Rule Filters	59
Managing Flex-Rule IP Tables	63
Smart-Rules	65
Smart-Rule Thresholds	65
Rate Limits	67

CONTENTS

Smart-Rule Types	67
Configuring Smart-Rules for Service Floods	72
Configuring Smart-Rules for Reflection Floods	75
Configuring Smart-Rules for Server Floods	79
Configuring Smart-Rules for Source Floods	82
Configuring Smart-Rules for ICMP Floods	84
Edit the Smart-Rule Scale Percentages	85
Advanced Settings	86
To open the CMS built in help	86
Address Groups	87
Syslog messages	88
Creating Address Groups	88
Exporting and Importing Address Groups	90
Enabling IP Reporting for an Address Group	92
Manage Network	95
SmartWall Network	97
Clusters	99
Deployment Options and Clusters	100
Analytics reporting per cluster	101
Managing Clusters	101
Devices	105
Clusters	105
Authentication Groups	105
SNMP	106
Viewing Device Status	107

CONTENTS

Adding a Device to the CMS	112
Managing Authentication Groups	113
Changing Device Credentials	116
Enabling SNMP for a Defense device	116
Disabling an Interface	117
Upgrading a Device's Software	118
Changing a Device's IP Address	120
Syncing a Device	121
Rebooting a Device	123
Redeploying a Device	123
Segments	125
Link State Propagation	125
Analytics reporting per Segment	126
Viewing Segment Status	126
Configuring a Segment	126
Connecting a Bypass Device to a Segment	128
Enabling Link State Propagation	128
Operating Modes	130
To open the CMS built in help	130
Manage Services	131
BGP Mitigation	132
Connect to BGP routers	133
Entry states	134
ExaBGP strings for FlowSpec routes	136
Configuring a Direct BGP Connection for RTBH	137

CONTENTS

Configuring a BGP Connection for RTBH via REST API	140
Configuring a BGP Connection for FlowSpec	144
Configuring BGP Mitigation DIP Thresholds	146
Managing the Black Hole Address List	148
Managing the FlowSpec routes List	150
Manage CMS	153
CMS System	156
Initial CMS System Actions	157
Uploading an HTTPS Certificate	157
Uploading a SecureWatch Package	157
Connecting to SWA or Another Syslog Server	160
Changing the CMS Timezone	164
Users	165
CMS user roles	165
Types of user authentication	166
IP Filters	167
Support login	167
Managing Local Users	168
Configuring LDAP Authentication	170
Configuring RADIUS Authentication	173
Setting the Authentication Order	176
Setting Web UI Timeouts	177
Enabling Support Account	177
Configuring CMS IP Filter Management	178
Snapshots	181

CONTENTS

Snapshoting your CMS Configuration	181
Scheduling Backups	183
CMS Software	186
Upgrading the CMS Software Version	186
Rolling Back to an Old CMS Software Version	187
SNMP	188
Supported SNMP versions	188
SNMP traps	188
CMS MIBs	189
Configuring the CMS SNMP Settings	189
Managing SNMP trap destinations	191
CMS Licenses for vNTD	193
Viewing License Capacity	193
Adding a vNTD License	195
Licensing/delicensing a vNTD	197
SSH Keys	198
SSH Keys for Authentication Groups	198
SSH Keys for authenticating Remote devices	198
Importing an SSH Key	198
Support Tasks	200
Viewing the Audit Log	200
Downloading Diagnostic Files	201
Restarting the CMS	203
Resetting the CMS to the Default Configuration	203
Reference	205

CONTENTS

Rules Reference	207
To open the CMS built in help	207
CMS Alarms and SNMP Trap Notifications	207
SNMP Trap Notifications	212
SNMP MIBs	213
Viewing a Corero MIB	213
OID numbers	215
CMS Web User Interface	232
To open the CMS built in help	232
CMS CLI Overview	232
Accessing the CLI	232
CLI Modes	232
View possible completions	232
Commit a change	233
Example: Using Set and Commit commands to Add a new NTD120 and NBA pair	233
Using pipes	234
Viewing tables	235
Example: Using the show command and pipes to view device information	235
pCLI Overview	239
Accessing the pCLI	239
Using the pCLI	239
pCLI Commands	239
CMS REST API Overview	249

CONTENTS

Using the REST API	249
Accessing the REST API documentation	253
REST API Examples	255
Requesting Technical Support	260
Self-Help Online Tools and Resources	260
Creating a Service Request with JTAC	260
Requesting Licenses	261
Glossary	262

TDD Documentation

There are three main documents which you can use to learn more about the SmartWall TDD:

Document	Location	Use
SmartWall TDD Getting Started Guide	The appropriate guide (KVM or ESXi) is provided by your Support representative or available on the Juniper support portal	Deploy a SmartWall TDD on your own servers. After completing the tasks in this guide, your TDD will be ready for use.
SmartWall TDD User Guide	PDF help from the top menu of the SWA Web UI or available on the Juniper support portal	Manage your SmartWall TDD. Contains TDD specific tasks and reference information for the SWA Web UI.
SmartWall TDD CMS User Guide	Context sensitive help site built into the CMS Web UI or available on the Juniper support portal	Understand general system tasks, enabling you manage your Defense devices and troubleshoot any issues. Contains reference information for the CMS Web UI, CLI, pCLI and REST API.

Note: The SmartWall TDD User Guide available from inside the SWA and CMS User Guide available from inside the CMS contain additional information compared to the versions of the guides available on the Juniper Support Portal. This information is only available to customers and is not publicly accessible.

CoreroSmartWall DDoS Protection Solution

The SmartWall DDoS Protection Solution can be deployed in a number of ways to best fit your infrastructure and protection needs.

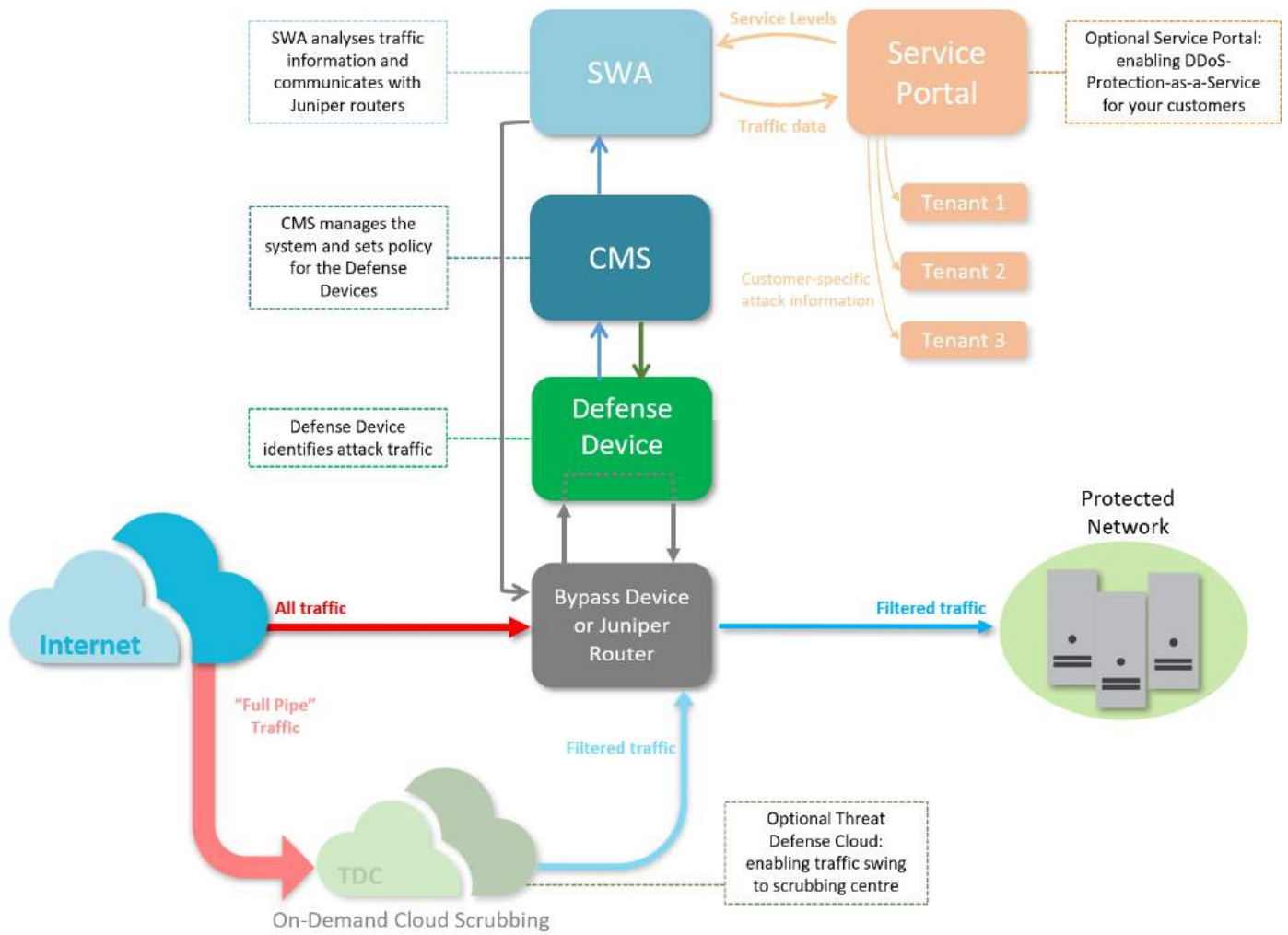
There are two main deployment models for the core SmartWall components:

- **SmartWall Threat Defense System (SmartWall TDS)** – SmartWall TDS uses appliances deployed at the edge of your network to protect your internal resources from DDoS attack traffic. It comprises of three main components: Defense devices (with optional zero-power bypass protection), the SmartWall Central Management Server (CMS), and SmartWall SecureWatch Analytics (SWA).
- **SmartWall Threat Defense Director (SmartWall TDD)** – SmartWall TDD works together with Juniper Networks® routers to filter out DDoS attack traffic at the edge of your network, without needing to deploy additional appliances at every protected location. It comprises of four main components: Edge routers, Defense devices (acting as Detection Engines for the routers), the SmartWall Central Management Server (CMS), and SmartWall SecureWatch Analytics (SWA).

The following components are also available and can be deployed with a SmartWall TDS or SmartWall TDD solution:

- **SmartWall Threat Defense Cloud (SmartWall TDC)** – SmartWall TDC enables your inbound traffic to be automatically routed via a cloud scrubbing center when an attack becomes large enough that it could overwhelm your available internet bandwidth.
- **SmartWall Service Portal (Service Portal)** – The Service Portal enables you to offer DDoS-Protection-as-a-service to your customers, providing each with their own portal access to view only their attack information. Each customer can be assigned a specific mitigation level and receive attack alerts and scheduled reports.

Note: Some of the documentation you receive will be tailored to your specific solution, but as some applications are generic you may see the options for other solutions shown in the guides.

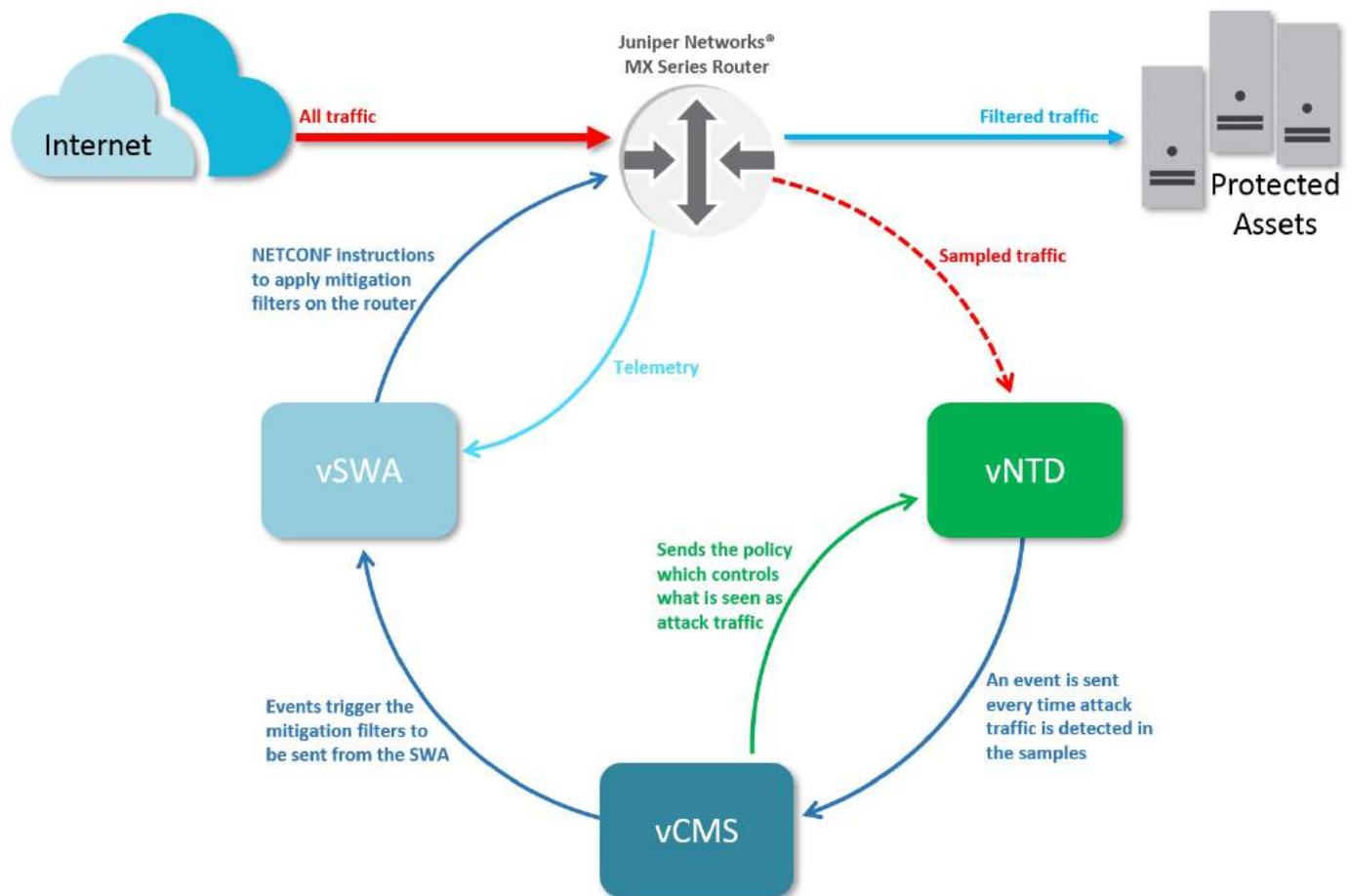


SmartWall Threat Defense Director

The SmartWall Threat Defense Director (SmartWall TDD) works together with Juniper Networks® MX Series routers to filter out DDoS attack traffic at the edge of your network.


A SmartWall TDD system requires the following components:

- **Remote Devices** – The Juniper Networks MX Series router at the edge of the network being protected. They send sampled traffic to the vNTD and are directed by vSWA to apply firewall filters to block DDoS attack traffic.
- **Defense Director** – A bundle of three virtual applications:
 - **vSWA** – The SmartWall SecureWatch Analytics Virtual Edition (vSWA) receives information from the Detection Engine (via the vCMS) to identify the DDoS attacks currently active against your network. The vSWA application then sends firewall filter commands to the router to filter the attack traffic as it arrives at the router. The vSWA application also displays real-time and historical statistics that enable you to analyze attacks on your network.
 - **vCMS** – The SmartWall Central Management Server Virtual Edition (vCMS) controls the Detection Engine and enables you to configure the attack mitigation policy used to distinguish attack traffic from normal network traffic.
 - **Detection Engine (vNTD)** – The SmartWall Network Threat Defense Virtual Edition (vNTD) is the Detection Engine for the SmartWall TDD. It detects DDoS attack traffic in mirrored samples sent from the edge routers.
- **Additional Detection Engines** – The Defense Director bundle includes a single Detection Engine (vNTD). You may need to purchase additional Detection Engines for your deployment.



Working with the SmartWall TDD applications and documentation

The same three applications which power the SmartWall TDD are also used in the Corero SmartWall Threat Defense System (SmartWall TDS). The SmartWall TDS is primarily used inline or in a scrubbing configuration, where the Defense devices block traffic directly. As the system shares common components, you may see the following types of information relating to the SmartWall TDS:

- Some features in the CMS are designed for NTD inline mitigation and will not be available in a SmartWall TDD deployment. When working in the CMS, if you are unsure if a feature applies to the SmartWall TDD, click  the help icon in the top left and look for a note labeled **TDD deployments**.
- In the CMS interface, events, and documentation you will see references to "blocking traffic". In a SmartWall TDD deployment, this should be interpreted as "identifying DDoS attacks".

Core Concepts

Provisioning Command Line Interface (pCLI)

When you install a SmartWall device or application, you need to execute essential configuration tasks using the Corero Provisioning Command Line Interface (pCLI). The pCLI is a set of commands you can use to define the initial configuration of each SmartWall® component. For initial configuration of any component, type `setup` in the pCLI to launch a wizard which will guide you through the initial configuration options.

Policy

A Policy is a configuration of the attack mitigation features which tells the Defense devices how to handle incoming traffic. Each policy is contained in a Protection Profile.

Protection Profiles

A Protection Profile is a container for a configuration of the attack mitigation features (Policy) in the CMS. When you associate a Protection Profile with a Cluster, it provides all the Defense devices in that Cluster with the same Policy for handling incoming traffic. You can create one Protection Profile for your network or multiple Protection Profiles each containing a different Policy.

Clusters

A Cluster is a set of identically configured Defense devices. When you create a new Cluster you must associate it with a Protection Profile containing the Policy which controls how the devices in that Cluster respond to traffic.

Devices

There are two types of devices in the SmartWall TDD system:

- **Defense devices** – This is broader term for the vNTDs (SmartWall Network Threat Defense Virtual Edition devices) which are used purely as Detection Engines in a SmartWall TDD deployment
- **Remote Devices** – This is a broader term for the Juniper Networks MX Series router used to mitigate DDoS attack traffic

While the SmartWall TDD only uses the above device types, in the user interface and documentation you should be aware that device can refer to any of the Defense devices compatible with the SmartWall TDS system (vNTD, NTD1100, NTD280, and NTD120) or a Bypass Device.

Segments

A Segment is an interface pair to which DDoS protection is applied. The segment is associated with a port pair on a Defense device. The first time you connect a Defense device to the CMS, it identifies the available interfaces and records them as Segments.

Note: A vNTD has two available interface ports which act as one Segment. For SmartWall TDD deployments only the 1st interface will be used. The 2nd interface should be disabled in the CMS.

Defense Mode

The Defense Mode is the default traffic handling mode which tells the system whether it should use the rest of the Policy features to block attack traffic, just inspect the traffic, or send the traffic to the internal network without any inspection.

For a TDD deployment, when you select a defense mode you have the following options:

- **Mitigate** mode – The TDD system instructs the router to discard attack traffic.
- **Monitor** mode – The router will complete all steps as if it was mitigating traffic (i.e. sending telemetry to SWA) but will accept the attack traffic.

Note: In the CMS documentation and user interface, the Defense Mode is described for an inline SmartWall TDS deployment where the Defense device is able to directly block traffic. In the TDD system the blocking is only ever performed by the routers. Pass-through mode only applies to the TDS system.

Analytics

Analytics is the process of collecting and analyzing the event and system information generated by the Defense devices. The Defense devices send analytics syslog messages to the CMS where that information is aggregated and sent to SWA.

Sampled Traffic

This is a feed of a proportion of the traffic received by the Juniper Networks MX Series router ahead of any mitigation. The vNTD uses this traffic to detect DDoS attacks, and enables the TDD system to generate the filter instructions it sends to the Remote Device to block that attack traffic and permit non-attack traffic. For example, if you have 1Tbps of traffic coming into a Remote Device, and a sample rate of 1:1000, the vNTD will see 1Gbps of sampled traffic.

Caution: Do not use truncated samples on the Juniper Networks MX Series router.

Telemetry

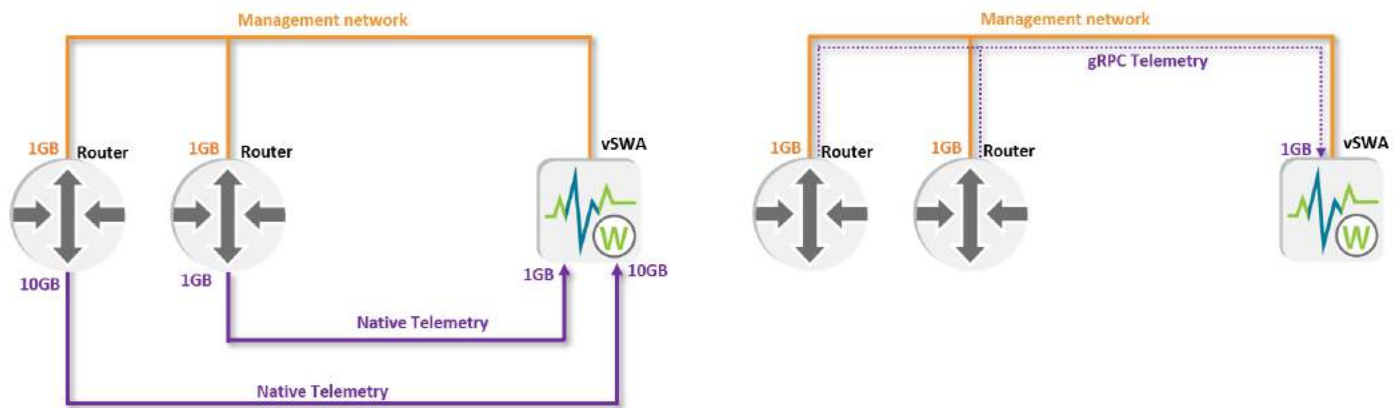
Telemetry is sent from the Juniper Networks MX Series router to the vSWA. It shows the network traffic processed by the router including what was permitted or blocked by the TDD system.

The TDD requires a telemetry feed from every monitored router to the SWA application. There are two main telemetry delivery methods:

- **Native telemetry** (UDP) – Telemetry is sent over your traffic network between the router and SWA. This requires a dedicated 10GB port on the router and a 10GB, or 1GB, port on the SWA host.
- **gRPC telemetry** – Telemetry is sent over the 1GB Management network. With gRPC telemetry you have the option to encrypt the telemetry traffic using SSL certificates.

You decide which telemetry type is used when you [configure the Juniper Networks MX Series router](#). If you choose gRPC telemetry, you must download 2 additional software files to the router during set up and then provide additional configuration information when [adding the router to the SWA as a remote device](#).

You decided which telemetry type is used when you configure the Juniper Networks MX Series router (See SmartWall TDD Getting Started Guide for instructions). If you choose gRPC telemetry, you must download 2 additional software files to the router during set up and then provide additional configuration information when [adding the router to the SWA as a remote device](#).



NETCONF

The TDD system uses NETCONF to configure the ephemeral firewall rules in the Juniper Networks MX Series router to block or permit network traffic.

SmartWall Service Portal

The SmartWall Service Portal enables you to offer Corero SmartWall DDoS Protection, as a managed service, to your customers. The Service Portal is a customer-facing DDoS protection portal which uses traffic data from your SmartWall TDD and displays the information in easy to read dashboards and reports. Your customers can log in to the portal and view the attacks you have protected them against. For information on Service Portal versions which are compatible with your SmartWall TDD, see the SmartWall TDD release notes.

Note: If you do not have a Service Portal and would like to add one to your existing TDD system, contact your support representative for more information.

Accessing the TDD Components

After you deploy the SmartWall TDD, you will have 4 configured component types working together to protect your network:

- Juniper Networks MX Series router
- SmartWall Network Threat Defense devices (vNTD devices working as Detection Engines)
- SmartWall Central Management Server (CMS)
- SmartWall SecureWatch Analytics(SWA)

For regular operation, you will mostly use the SWA application, but you will also need to maintain some configuration settings in the CMS application, including managing your Defense devices.

SWA

You can access the SWA Web UI through a browser by typing the IP address of your SWA application followed by :8000 (e.g. <https://10.10.100.200:8000>) or by the DNS address, if you set one up during installation. You can access all analytics and TDD functions through the Web UI.

After initial configuration, if you need to perform a higher level operation, like changing the application IP address or NTP server, you can access the pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<SWAipAddress>`

Monitor users also have read-only access to the **REST API** on port 8089.

Caution: If you plan to allow monitor access to the REST API, you should [configure IP filtering](#) to limit access to only trusted accessors and ensure you have [changed the default passwords](#).

CMS

There are 3 ways to access the CMS:

- **Web UI** – You can access the CMS Web UI through a browser by typing the IP address of your CMS application (e.g. <https://10.10.100.100>) or DNS address, if you set one up during installation. You can access all main CMS functions through the Web UI.
- **CLI** – You can access the CMS CLI using an SSH client to connect to the IP Address of your CMS, on the default port 2024 . You can access all CMS functions through the CLI.
- **REST API** – You can access the REST API using any tool that sends HTTP requests to a URL, but it is most easily available using Swagger: In a browser type the IP address of your CMS followed by /api(e.g. <https://10.10.100.100/api>) and log in with your CMS credentials. You can affect Protection Policy changes through the REST API and view device status information.

After initial configuration, if you need to perform a higher level operation, like changing the application IP address or NTP server, you can access the pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<CMSipAddress>`

vNTD

After initial configuration, you can manage the vast majority of the Defense device configuration from within the CMS (Network>Devices). If you need to perform a higher level operation, like changing the device's IP address or NTP server, you can access the device's pCLI by opening the console connection or using an SSH client: `ssh -p 2222 <username>@<vNTDipAddress>`

Supported web browsers for the Web UI

- **Chrome:** 71 or newer
- **Edge:** 44 or newer
- **Firefox:** 64 or newer
- **Safari:** 12 or newer
- **Internet Explorer:** not supported

Juniper Networks MX Series router

After initial configuration, you should be able to manage the connection to the router in the SWA (Mitigation > Remote Devices). If you need to access the router, you can use an SSH client: : `ssh -p 22 <username>@<MXipaddress>`

Juniper Networks MX Series router requirements

Your Juniper Networks MX Series router must meet the following criteria:

- It must support Sampled Mirror, Flexible Filtering, Ephemeral Configuration, and Remote Telemetry.
- Your router should be running one of the following JunOS versions:
 - For production deployments:
 - 17.2R3
 - 17.3R3
 - **17.3R3-S8 recommended**
 - 17.4R2
 - 18.1R3
 - 18.2R2
 - 18.3R1
 - **18.3R3-S2 recommended**
 - **19.2R3 recommended**
 - **20.1R2 recommended**

Note: Recommended versions have had a broad and successful use with Corero SmartWall TDD.

- For lab tests or proof of concept deployments:
 - Any of the above
 - 16.2R3 minimum

Caution: For JunOS versions not listed, please refer to your support representative for compatibility.

SECTION 1

Get Started

This section of the CMS User Guide provides introductory information on navigating and interacting with the CMS application.

Tip: For information on hardware or virtual application installation, see the Getting Started Guide for your specific product.

This section discusses the following:

Getting Started	25
View System Status	26
To view the current status of your network	27
Working in the CMS	28
Supported web browsers for the Web UI	28
Web UI Interface	29
Committing your changes	31

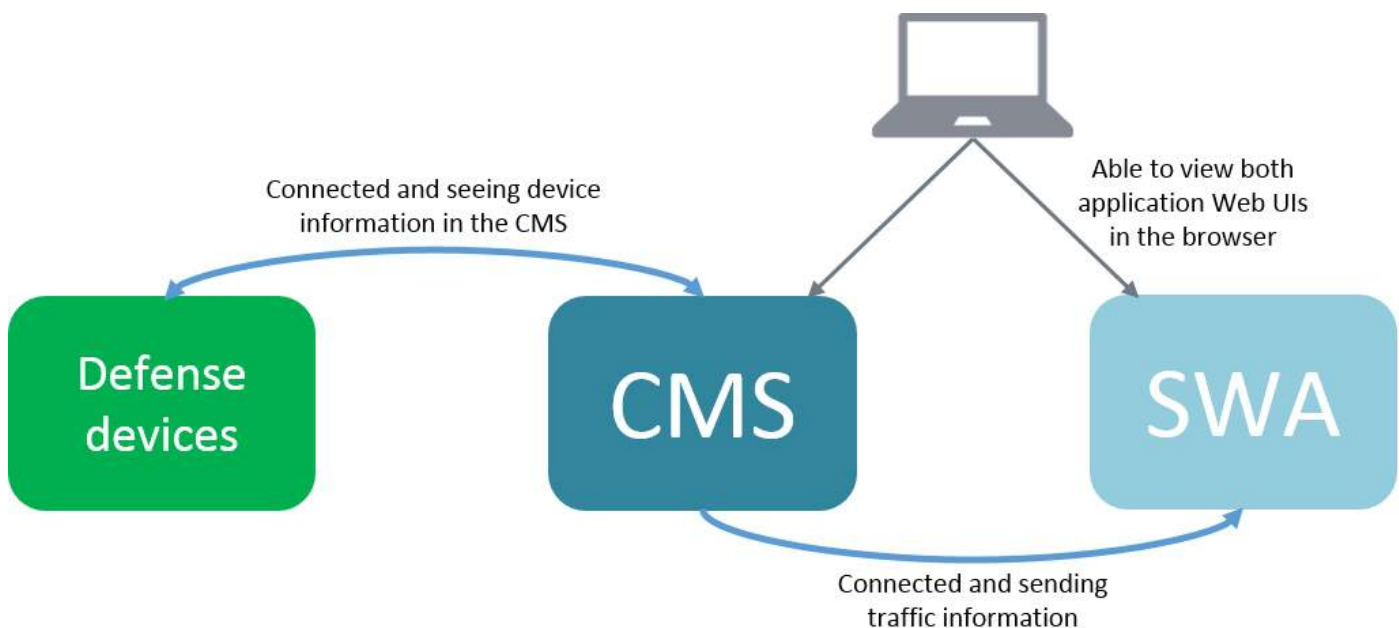
Working with different Protection Profiles	31
Web UI default values	31
Notifications	31
Using the CLI	32
Alarms and Notifications	33
Alarm types	33
Perceived severity	33
Notifications	34
Viewing System Alarms	34
Managing the Alarm Handling Log and Status Change list	36
Deleting Alarms	38

Getting Started

This topic provides a brief overview of the next steps an admin user should take following installation. This should be used as a guide to help you plan your own strategy and may have to be modified to suit your network.

After you install your SmartWall system, you should have it in the following state:

- Your SmartWall devices are online and connected to a SmartWall Central Management Server (CMS). They should be showing the Deployment State: **not-in-cluster**. This means that the devices are currently passing traffic straight to the internal network, because they haven't yet inherited an attack mitigation Policy.
- The CMS should be connected to SmartWall SecureWatch Analytics (SWA) and sending syslog messages. You should have [added a signed certificate to the CMS](#) and be able to open the CMS in a browser and see the Web UI (e.g. `https://10.10.100.100`).
- Finally, the CMS and the SWA can be [connected to the SecureWatch Service](#). You should be able to open the SWA in a browser (using the SWA IP Address on port 8000, e.g. `https://10.10.100.200:8000`) and see traffic information.



Now that all components of the SmartWall system are online and connected, you can start to configure your SmartWall policy. Below is a recommended general configuration procedure, but the specifics will depend on your attack mitigation needs:

1. The CMS initially contains a single Protection Profile called "default". If all your devices are going to handle the same sort of traffic, you probably only need one Policy and, therefore, one Protection Profile to contain it. Alternatively you may need to [create additional Protection Profiles](#) to store the attack mitigation Policies you want different groups of devices to use.
2. The CMS initially contains a single Cluster called "default" which is associated with the default Protection Profile. Logically group your devices and then [create an additional Cluster](#) for each group you need. When you create a Cluster, you associate it with a Protection Profile; this means that every device you add to that Cluster will use the same attack mitigation Policy. You may need several clusters because you have several Protection Profiles you want to use, or you may have only one Protection Profile, but choose to use multiple Clusters to group your devices by another criteria so you can more easily identify them when you're looking at the SWA.
3. [Add your devices to their Clusters](#). Look at the [Devices table](#) to check all your devices are now showing as In Sync.

Note: While an **In Sync** device now has the default attack mitigation Policy, it won't be blocking any traffic yet, as the default Global Defense Mode is **Monitor**. This means that traffic is still going through the device to the internal network, but it is being inspected and the CMS is sending security events to the SWA.

4. Before you change the Defense Mode to to start blocking attack traffic, you may need to [tune the Policy](#) stored in each Protection Profile, for your network. In the CMS Web UI, you can see all the Policy configuration settings under **Policy** in the left menu.
5. Use the SWA to see what effect your Policy changes have had on the system. If you can still see attack traffic coming through without triggering any rules, you may need to tighten some settings. Also, if you now see some non-attack traffic triggering rules it shouldn't, you may need to adjust some of your changes. You can find out more about using the SWA in the **SmartWall SWA User Guide**.
6. Once you are happy that only attack traffic is triggering rules (whose action would normally be to block that traffic), you can [change the Global Defense Mode](#) to **Mitigate**. The Defense devices will now start to block attack traffic as per your attack mitigation Policy.

DDoS attacks are constantly evolving, so you should regularly check the SWA often to ensure that your Policy is still optimized for protecting your system from attack. If you use the SecureWatch Service, then Corero Security Operations Center will be constantly monitoring your SWA for new attacks. They can use this information to continually optimize the attack mitigation Policy for your network.

View System Status

When you first log into the CMS you can see the system dashboard. This provides an overview of your system health and its ability to mitigate attack traffic.

To view the current status of your network

1. Navigate to the Home screen. This is the first screen you see when you log into the CMS.
2. Check the Status panel for any parts of the system showing warnings or errors. If there is a warning or error, click **Click to view issue**.
3. Use the Status Issue list to identify the device, segment, interface, or operating mode which is causing the issue.
4. Return to the Home page to further investigate:
 - **Device issue** – In the devices table, search for the device name to see an overview of its current status or click on the table to open the Devices screen.
 - **Segment issue** – In the Segments table, search for the Segment name to see an overview of its current status or click on the table to open the Segments screen.
 - **Interface issue** – If the issue table provides a specific interface, you can find more information on it's current status by clicking on the devices table to open the Devices screen and opening the **INTERFACES** tab.
 - **Operating Mode issue** – If the Global Operating Modes are not set to mitigate attack traffic, or if you have overrides in place which are not mitigating traffic, you will see Operating Mode warnings. In the Operating Modes panel, click **Change** to edit the Defense and Bypass Modes.

Working in the CMS

There are 3 ways to access the SmartWall Central Management Server (CMS):

- **Web UI** – You can access the CMS Web UI through a browser by typing the IP address of your CMS application (e.g. <https://10.10.100.100>) or DNS address, if you set one up during installation. You can access all main CMS functions through the Web UI.
- **CLI** – You can [access the CMS CLI](#) using an SSH client to connect to the IP Address of your CMS, on the default port 2024 . You can access all CMS functions through the CLI.
- **REST API** – You can [access the REST API](#) using any tool that sends HTTP requests to a URL, but it is most easily available using Swagger: In a browser type the IP address of your CMS followed by /api(e.g. <https://10.10.100.100/api>) and log in with your CMS credentials. You can affect Protection Policy changes through the REST API and view device status information.

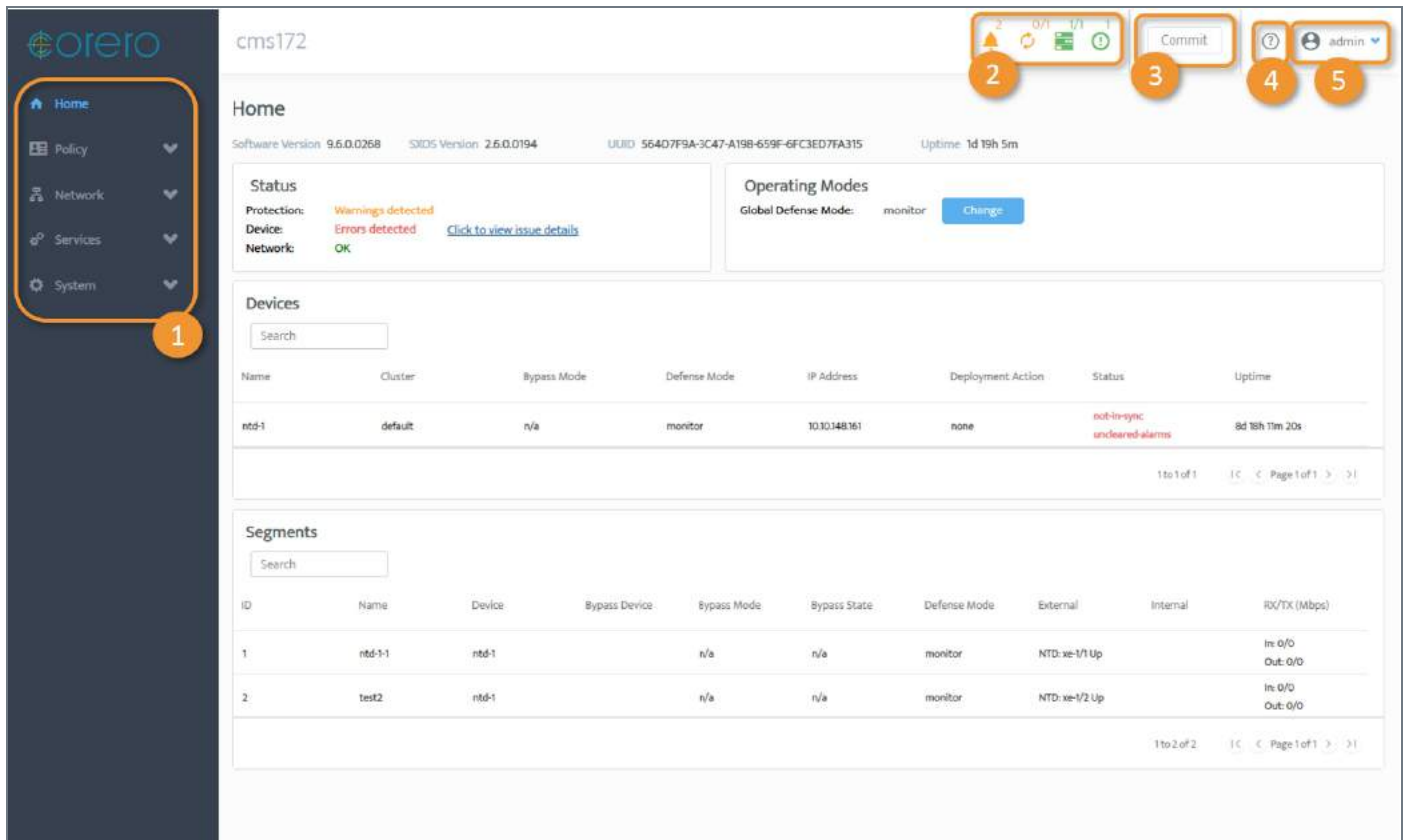
There are three standard user roles available for the CMS. The role you have, affects what you can do in the CMS:

- **cns-admin** – The administrative role. An admin user can edit all **Policy**, **Network**, and **System** configurations, including managing users.
- **cns-defense** – A non-administrative role which enables its users to edit all **Policy** options but no Network or System administrative settings
- **cns-monitor** – A primarily read-only role which enables its users to view settings without being able to enact any changes (aside from their own password)

Supported web browsers for the Web UI

- **Chrome:** 71 or newer
- **Edge:** 44 or newer
- **Firefox:** 64 or newer
- **Safari:** 12 or newer
- **Internet Explorer:** not supported

Web UI Interface



The screenshot shows the Corero SmartWall CMS Web UI Interface. The interface is divided into a sidebar menu on the left and a main content area. The sidebar menu includes links for Home, Policy, Network, Services, and System. The main content area displays system status, operating modes, and tables for devices and segments. Numbered callouts 1 through 5 highlight specific UI elements: 1 points to the sidebar menu, 2 points to the top status bar, 3 points to the 'Commit' button, 4 points to the user profile dropdown, and 5 points to the user name 'admin'.

Note: The screenshots in this guide show the interface as a **cns-admin** user. Some features or screens may not be visible to other user roles.

Surrounding the main interface area there are the following navigation and information aids:

1. Menu





The expandable menu on the left of the screen contains a link back to the **Home** screen and then four expandable sections:

- **Policy** – Options related to creating Protection Profiles and tuning the Policies they contain
- **Network** – Options related to managing Clusters, devices, and Segments
- **Services** – Options related to using the SmartWall system with external devices
- **System** – Options related to managing the CMS, and its connection to SmartWall SecureWatch Analytics


2. Status bar

At the top right of the screen, there are 4 icons that summarize the status of the CMS and your devices. If the icon is green, this indicates there are no problems. If the icon turns orange, then something needs your attention.

The icons represent:


-  **Alarms** – When this icon is orange, there is an uncleared alarm. Click this icon to open the Alarm Center and view the list of cleared and uncleared alarms.
-  **Devices in sync** – When this icon is orange, there is a device which is not in-sync. Click this icon to open the Devices screen to sync the device.
-  **Devices reachable** – When this icon is orange, there is a device which is not reachable by the CMS. Click this icon to open the Devices screen to see what device cannot be reached.
-  **Notifications** – Click this icon to view or clear previous notifications from this session.

3. Commit button

In the top right of the screen, you can see the  button. This remains inactive until you make a change that needs to be saved and sent to a Defense device. When it is active, you can click the button to view a list of your pending changes. On that dialog, click **Commit** to send those changes to the appropriate devices, or **Discard** to delete those pending changes.

Caution: If you log out, or the CMS logs you out after a period of inactivity, you will lose any changes which you have not committed.

4. Help button

On the top right of the screen, you can click the  help button to open the CMS knowledgebase in a new tab. You can search for the information you need or browse the help guide using the left hand menu.

5. Account settings

On the top far right of the screen, you can see your account name. Click this to display a drop-down with two options:

- **Change Password** – Enables you to change your user account password
- **Log Out** – Logs you out of the CMS

Committing your changes

In the Web UI, most changes are temporarily stored in the CMS and are only saved when they are committed. For example, when you make a change to a Protection Profile in the CMS, it won't be pushed to the devices associated with that Protection Profile until you use the **Commit** button to review and then **Commit** your changes.

There are some exceptions to this rule: BGP Mitigation table entries are performed immediately, and some system level settings also do not require a commit.

When you have changes available for committing, the Commit button turns green. Click it to open the Commit dialog. Here you can choose to revert your pending changes (**Discard**), or commit the pending changes (**Commit**).

In the CLI, to save a change you need to type the `commit` command . You can do this after one or multiple changes. To revert all your changes since the last commit, you can type the `revert` command.

Caution: After a period of inactivity the CMS will log you out. Any changes you have not yet committed will be lost.

It is possible to experience commit conflicts in the CMS. If you are unable to commit due to a conflict, **Discard** the changes, re-do your changes and commit.

Working with different Protection Profiles

Unlike the CLI, where you must specify the Protection Profile you want to edit before you can access any of the attack mitigation features, in the Web UI you select an attack mitigation feature and then choose which Protection Profile you want to edit. The Protection Profile remains selected as you move between attack mitigation features. If you want to edit a different Protection Profile, you need to choose it from the **Selected Protection Profile** drop-down before you make any changes.

Web UI default values

A new Protection Profile contains default values for many Policy features. You can overwrite these defaults with your own values, that are more applicable to your specific network traffic. If at any point you want to return to the default value there are two methods to do this:

- For drop-down lists, click the black **x** at the right of the field
- For other fields, completely delete the existing value and the default value will appear

Notifications

In the Web UI, notifications inform you of your successful and unsuccessful actions. They appear on the right of the screen in green (successful) or red (unsuccessful) pop-ups. The CMS stores a list of your notifications from this session. When you log out the notification list is cleared.

To view previous notifications

1. In the Status bar, click  the Notification icon.

To clear your notifications list without logging out

1. In the Status bar, click  the Notification icon.
2. Click **Clear all**.

Using the CLI

To access the CLI you need to SSH to your CMS application using the following command in an SSH client (replacing the placeholders with your account username and CMS IP address):

```
ssh -p 2024 <username>@<ipaddress>
```

When you first log in to the CMS CLI, you're in operational mode where you can view settings and status information. If you want to make a change, you need to enter configuration mode by typing the command: `configure`. Type the `exit` command to return to operational mode.

To investigate possible commands in either mode, press the **Tab** key at any point to view possible completions. If there is only one possible completion, the tab key will auto-complete that command. Press the **Enter** key to submit commands.

You can focus on an area of the CLI using the `edit` command. For example, `edit policy protection-profile <ppName>`, where `<ppName>` is the name of one of your Protection Profiles, reduces your options to only affect that Protection Profile. You can now use the `set` command to make Policy changes, confident that you're only affecting your chosen Protection Profile. Use the `exit` command to return to the full configuration mode.


Using the corresponding CLI commands in this guide

In this guide, alongside every Web UI method for completing a task, there is a set of Corresponding CLI commands. You can use these commands to perform the same task in the CLI. In the commands, there are two types of placeholder you must replace; both are shown in italics:

- *[option1|option2|option3]* – Replace with one of the fixed options. This placeholder can be recognized by the square brackets and pipe characters separating the options. You must choose just one of the available options.
- *<specificInformation>* – Replace with information specific to your system. This placeholder can be recognized by the chevrons either side. The whole thing (chevrons included) must be replaced with a piece of specific information (e.g. a device name, a threshold rate, etc)

Alarms and Notifications

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Alarms Screen reference topic](#).

When an uncleared alarm appears, the alarm symbol  on your CMS Status bar will turn orange. Click that to view Alarm Center and see the current system alarms in a table.

Alarm types

In the Alarms table, there are six possible alarm types:

- **Device status alarms** – Something has happened affecting the status of a device (e.g. the device is out of sync)
- **Device upgrade alarm** – Something has happened to a device during an attempted upgrade (e.g. upgrade has failed)
- **Device alarms** – Something has happened to cause a device to restart or reset.
- **CMS alarms** – Something has happened during a CMS software upgrade or rollback
- **Analytics alarms** – Something has happened to the analytics process
- **Resource alarms** – Something has happened to the underlying CMS application (e.g. low on disk space)

Tip: You can see the full list of alarms in the Reference area of the Corero SmartWall CMS User Guide . In the same list, you can see the [SNMP trap notifications](#) these alarms correspond to.

For each alarm, you can see the **Alarm Type**, the **Specific Problem** within that type, and the **Alarm Text** giving further information.

Perceived severity

Every alarm has a perceived severity that tells you how potentially problematic the alarm situation could be to the SmartWall system:


- **Critical** – This could be very damaging to your system and should be investigated immediately (note that critical alarms will not self-clear, you must do something to remedy the situation)
- **Major** – Something has happened that could interrupt the system's ability to function fully (e.g. a device is restarting)
- **Minor** – Something potentially problematic has happened that is unlikely to interrupt the systems ability to function
- **Cleared** – This alarm is there to notify you that a previous alarm situation has resolved, view the history of this alarm to see more details.

Note: The alarm system does not differentiate between unexpected actions and actions you have taken. For example, when you reboot a device using the CMS, you will see a major alarm when the device goes down and then a cleared alarm once it has restarted.

Notifications


Unlike alarms, notifications in the Web UI inform you of your successful and unsuccessful interactions with the Web UI. They appear on the right of the screen in green (successful) or red (unsuccessful) pop-ups. You can view a list of your notifications for this session on the Status bar. The notification list is cleared when you log out, but you can choose to clear your notification list mid-session using the **Clear all** button.

Viewing System Alarms

When the  alarm icon in the Status bar turns orange, you have an uncleared alarm which may require attention. To view the alarms, you need to open Alarm Center.

Tip: The CMS can produce a range of alarms. You can see the full list in the [alarms reference area](#).

To open Alarm Center

1. In the Status bar, click on the  alarm icon.
2. In the Alarms table, you can see a list of cleared and uncleared alarms.

CLI Commands

Command

`show alarms`

`alarm-list`

`alarm`

`last-changed`

`number-of-alarms`

`summary`

`critical`

`indeterminates`

Output

All alarm information

All alarm list information

List of current alarms

Time of the last change to the alarm list

Total number of alarms in the current alarm list

All alarm summaries

Number of current critical alarms

Number of current indeterminate alarms



majors	Number of current major alarms
minors	Number of current minor alarms
warnings	Number of current warning alarms

Managing the Alarm Handling Log and Status Change list



When an alarm requires your attention, you can keep a log of the steps you take to investigate and resolve it. You can also view the steps other CMS users are taking. Additionally, you can view a list of the status change events that have occurred.

Note: If the alarm is for a device, the Status Change list only shows related previous alarms for that specific device.



To view the alarm handling log and status change list

1. In the Status bar, click on the  alarm icon.
2. In the Alarms table, next to the alarm you are working on, click the  edit button.
3. On the **Alarm Handling** tab, you can view the alarm handling log.
4. Click the **Status Change** tab to view the status change list.

To create a new alarm handling log entry

1. In the Status bar, click on the  alarm icon.
2. In the Alarms table, next to the alarm you are working on, click the  edit button.
3. On the Alarm Handling tab, select a **State** from the drop-down.
4. (Optional) **Write a comment** to provide a description of your progress.
5. Click **Add**.

To remove all but the last log entry and status

1. In the Status bar, click on the  alarm icon.
2. In the Alarms table, next to the alarm you want to compress, click the  edit button.
3. Click **Compress** to compress both the alarm handling log and the status change list.

Caution: Once you compress an alarm's history, you cannot restore it. When you click **Compress**, you compress the alarm handling log and the status change list at the same time.

CLI Commands

Tip: Use the CLI's tab complete function to help fill in the alarm information.

View alarm handling log

```
show alarms alarm-list alarm <deviceName> <alarmType> <alarmPath> <specific
Problem> alarm-handling
```

View status change list

```
show alarms alarm-list alarm <deviceName> <alarmType> <alarmPath> <specific
Problem> status-change
```

Create a new log entry

```
request alarms alarm-list alarm <deviceName> <alarmType> <alarmPath>
<specific Problem> handle-alarm state
[ack|closed|investigation|none|observation] description "<description>"
commit
```

Remove all but the last log entry and status



```
request alarms alarm-list alarm <deviceName> <alarmType> <alarmPath>
<specific Problem> compress
commit
```

Deleting Alarms


To clear old alarms from alarm center, you can delete them individually or delete all alarms.

Caution: Once you delete an alarm you cannot recover it. Do not delete an uncleared alarm.

To delete a single alarm

1. In the Status bar, click on the  alarm icon.
2. In the Alarms table, next to the alarm you are working on, click the  delete button.
3. Click **OK**.

To delete all alarms

1. In the Status bar, click on the  alarm icon.
2. Check that all the alarms in the table are cleared, then click **Purge All**.
3. Click **OK**.

CLI Commands

Delete a single alarm

Tip: Use the CLI's tab complete function to help fill in the alarm information.

```
request alarms alarm-list alarm <deviceName> <alarmType> <alarmPath>
<specific Problem> purge
commit
```

Delete multiple alarms

Tip: Rather than pressing **Enter** after purge-alarms, you can press **Tab** to see the options for filtering the alarms that you delete. For example, you could choose to only delete cleared alarms or only delete alarms where you were the last one to make an alarm handling log entry.

```
request alarms purge-alarms
commit
```

SECTION 2

Tune Policy

A Policy is used by Defense devices to separate attack traffic from non-attack traffic. This Policy is stored and configured in the CMS then sent to associated Defense devices.

This section discusses the following:

Policy	42
TDD deployment policy settings	42
To open the CMS built in help	42
Protection Profiles	43
Using Protection Profiles	43
Creating Protection Profiles	44
Importing and Exporting Protection Profiles	46
Packet Rules	47

To open the CMS built in help	47
Packet Rules	47
To open the CMS built in help	47
Packet Rules	47
To open the CMS built in help	47
Flex-Rules	48
Flex-Rule Rule Actions	48
Flex-Rule Thresholds and Rate Limits	48
Types of Flex-Rule	50
Flex-Rule Filters	51
Evaluation order	52
Enable/Disable a Flex-Rule	52
Managing Flex-Rules	52
Types of Flex-Rule Filters	56
Managing Flex-Rule Filters	59
Managing Flex-Rule IP Tables	63
Smart-Rules	65
Smart-Rule Thresholds	65
Rate Limits	67
Smart-Rule Types	67
Configuring Smart-Rules for Service Floods	72
Configuring Smart-Rules for Reflection Floods	75
Configuring Smart-Rules for Server Floods	79
Configuring Smart-Rules for Source Floods	82
Configuring Smart-Rules for ICMP Floods	84

Edit the Smart-Rule Scale Percentages	85
Advanced Settings	86
To open the CMS built in help	86
Address Groups	87
Syslog messages	88
Creating Address Groups	88
Exporting and Importing Address Groups	90
Enabling IP Reporting for an Address Group	92

Policy

A Policy is a configuration of the attack mitigation features which tells the Defense devices how to handle incoming traffic. Each Policy is contained in a [Protection Profile](#).


TDD deployment policy settings

The Policy area in the CMS is designed primarily for inline deployments where the Defense device is responsible for blocking attack traffic. In TDD deployments, the Defense device does not block traffic, instead it uses its policy to identify attack traffic and send that information to the SWA which can send mitigation filters directly to your router. Because all mitigations need to be understood by the router, TDD deployments have a more specific range of policy options which can be safely sent.

Caution: If you modify any other Policy settings in the CMS, you will not change the type of mitigations sent to the router. It could instead cause the Defense device to identify the wrong traffic as attack traffic. This can lead to good traffic being blocked and attack traffic being allowed through to your network. If you think you need to modify any other part of the Policy (including the Flex-Rule Filter definitions), you must contact your support representative to make a corresponding change to the SWA application.

For information about the additional features you can see in the CMS Web UI, you can use the CMS built in help.

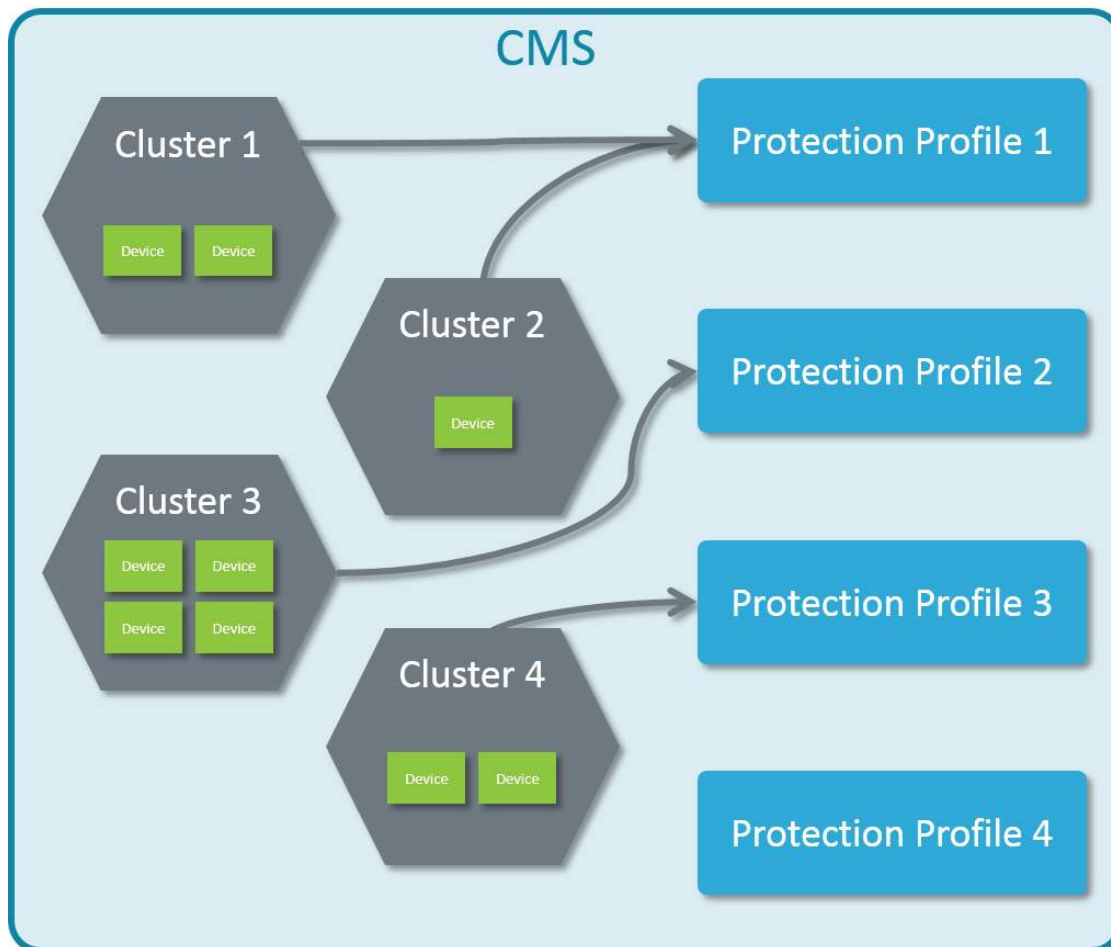
To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Protection Profiles

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Protection Profiles Screen reference topic](#).

A Protection Profile is a container for a configuration of the attack mitigation features (a Policy). When you associate a Protection Profile with a Cluster, it provides the Defense devices in that Cluster with the Policy for handling incoming traffic. You can create one Protection Profile for your network or multiple Protection Profiles each containing a different Policy. After installation, the CMS initially has a single default Protection Profile.



Using Protection Profiles

The [Policy](#) in a new Protection Profile only contains default values until you configure it for your network. On each Policy screen in the SmartWall Central Management Server, you must first select the Protection Profile you want to edit before you make any changes to the configuration.

For a Protection Profile to affect traffic, you must associate it with a [Cluster](#) containing the Defense devices whose Policy you want to change. Once you apply that change, the devices in that Cluster will now use the new Protection Profile to handle traffic.



Note: Clusters cannot exist without a Protection Profile. Before you can add Defense devices to a new CMS, you need to create a Protection Profile. You might want to create a single default Protection Profile for use during set up and then re-assign your Clusters once you're happy.



Creating Protection Profiles

A Protection Profile is a container for a defense Policy. This stores all the rules and thresholds which instruct Defense devices how to react to incoming traffic. Your CMS comes with a default Protection Profile but you can choose to create more if your network requires multiple Policies.

Caution: If you try and delete a Protection Profile, which is associated with one or more Clusters, you will be unable to **Commit** your changes until you associate those Clusters with a different Protection Profile or delete them.

To create a new Protection Profile

1. Use the left-hand menu to navigate to **Policy > Protection Profiles**.
2. Decide what base values you want to use for the new Protection Profile:
 - To create a new Protection Profile with default values click **Add**.
 - To create a new Protection Profile based on an existing one, click  the clone button next to the Profile you want to clone. This pre-populates the Name and Description fields which you can then edit.
3. Type a **Name** for this new Protection Profile. You must only use alphanumeric, spaces, or .-&()/@:= symbols.
4. (Optional) Type a **Description** (this only appears on the [Protection Profiles screen](#))
5. Click **Save**.
6. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: From the Protection Profile table, you can edit  or delete  existing Protection Profiles.

CLI Commands

Create a new Protection Profile

```
configure
```

```
set policy protection-profile <ppName> description "<description>"
```

```
commit
```

Tip: Once you're comfortable using the CLI you can continue tuning the new protection profile in the same command. Use the tab key to see the tuning options once you set the name.

Clone a Protection Profile

```
configure
request policy protection-profile <ppName> clone name <newProfileName>
commit
```

Edit an existing Protection Profile

```
configure
edit policy protection-profile <ppName> description "<description>"
commit
exit
```

Tip: Use the tab key after the description to see the current description string.

Rename a Protection Profile

```
configure
request policy protection-profile <ppName> rename name <newName>
commit
```

Delete a Protection Profile

```
configure
delete policy protection-profile <ppName>
commit
```

Next steps

1. Currently, your new Protection Profile's Policy contains only default values. You need to use the Policy features to tune it for the expected traffic.
2. To push this new Policy to a device, you need to associate the Protection Profile with a Cluster. You can [edit an existing Cluster](#) to use this new Protection Profile, or [create a new Cluster](#) associated with this Protection Profile then add device's to it.

Tip: If you want to test a policy change before applying it to all devices in a Cluster, you can clone the Protection Profile. Then make your change in the clone and assign it to a Cluster containing a


single test device. When you're happy, you can edit the main Cluster to use the new Protection Profile.

Importing and Exporting Protection Profiles

You can export your Protection Profiles to store externally or use with another CMS application. Once you import a Protection Profile you can view it in your Profiles list and use it like any other.


Caution: Protection Profiles can only be imported into a CMS using the same major version number as the CMS it was exported from. If you store Profiles externally, you should replace your stored files after every major CMS upgrade.

To export a Protection Profile

1. Use the left-hand menu to navigate to **Policy > Protection Profiles**.
2. In the Profiles table, locate the Protection Profile you want to export and click  the export button next to it.
3. The Protection Profile is saved as a .pkg file and downloads through your browser.

To import a Protection Profile from another CMS

Note: The CMS validates .pkg files before they are imported. A corrupted or otherwise unusable file will be rejected.

1. Export the Protection Profile from the other CMS (see above).
2. Save the exported .pkg file somewhere accessible from the CMS you want to import it into.
3. Log into the new CMS in a browser.
4. Use the left-hand menu to navigate to **Policy > Protection Profiles**.
5. Click **Import**.
6. Navigate to your saved pkg file. Select it and click Open.
7. (Optional) Edit the **Name** and **Description**.
8. Click **Save**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click  . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

Export a Protection Profile

configure

```
request policy protection-profile <ppName> export remote-uri <remoteUri>
remote-password <remotePassword>
```

```
commit
```

Import a Protection Profile

```
configure
```


```
request policy import protection-profile name <newProfileName> remote-uri  
<remoteUri> remote-password <remotePassword>
```

```
commit
```

Packet Rules

For information on managing Inspection Control, access the built in help available in the CMS Web UI.


To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Packet Rules

For information on managing Source Control, access the built in help available in the CMS Web UI.


To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Packet Rules

For information on managing Packet Rules, access the built in help available in the CMS Web UI.

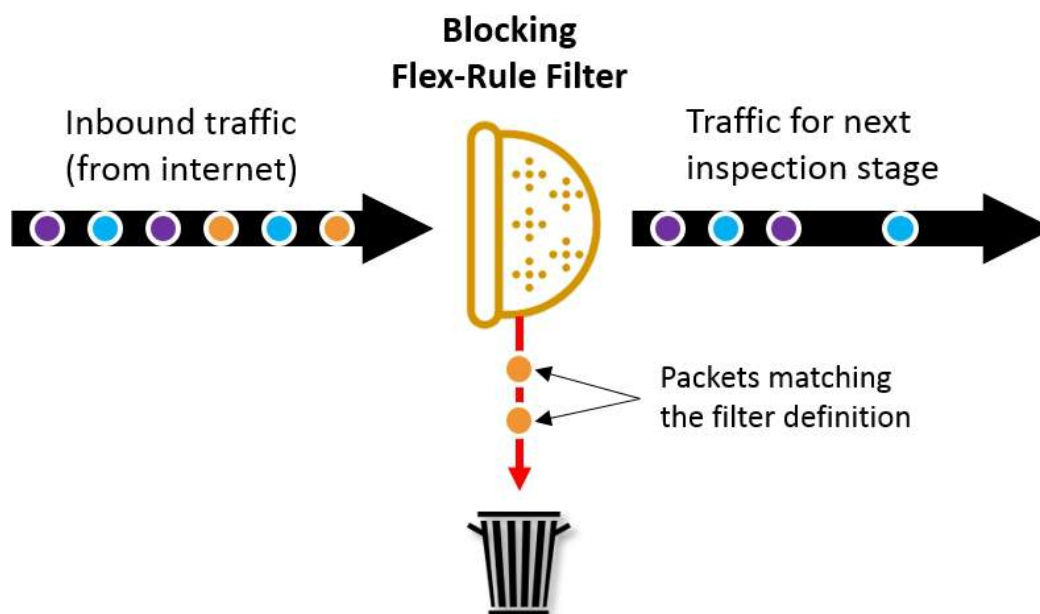
To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Flex-Rules

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Flex-Rules Screen reference topic](#).

Flex-Rules is an attack mitigation feature which enables you to define custom filters which can block or detect specific packets. Filters are written as a Berkeley Pack Filter (BPF) syntax expression.



Flex-Rule Rule Actions

When traffic matches a Flex-Rule filter's definition, how that traffic is handled is decided by the Rule Action of the Flex-Rule. The following are possible Rule Actions:

Note: Not all Rule Actions are available for every type of Flex-Rule.

- **Block** – The Defense device blocks traffic which matches the filters on this Flex-Rule.
- **Detect** – The Defense device inspects traffic which matches the filters on this Flex-Rule and sends event syslog messages; it does not block the packets.
- **Egress** – The Defense device sends traffic directly to the internal network (bypassing any further policy checks).
- **Disabled** – The Defense device does not check if traffic matches the filters on the Flex-Rule

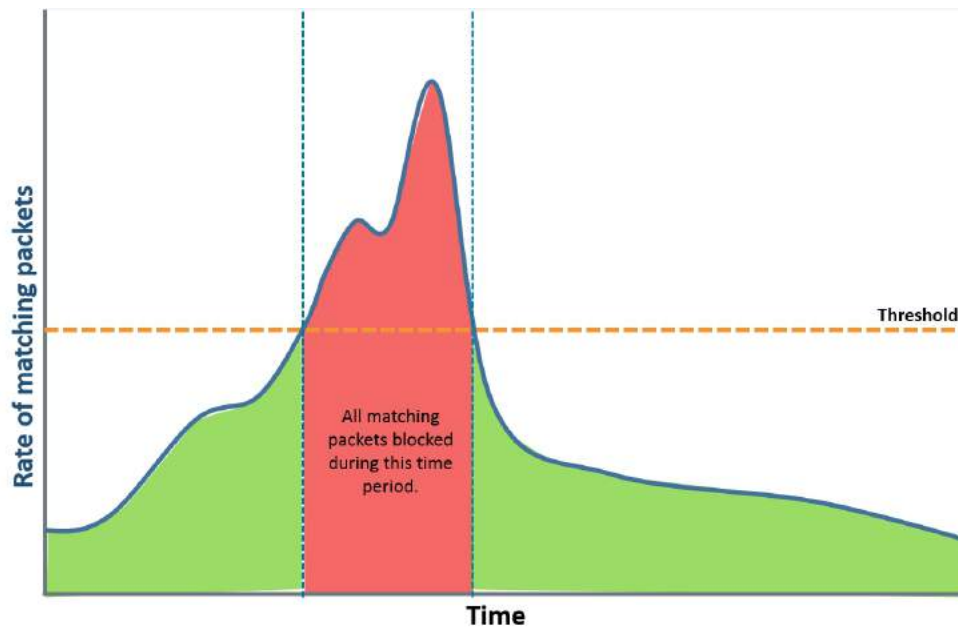
Flex-Rule Thresholds and Rate Limits

By default, a Flex-Rule's Rule Action is triggered when any packets match a filter on that rule and, when the Rule Action is triggered, it affects all matching packets. You can alter this behavior using Thresholds to only trigger the Rule

Action above a certain traffic rate, and using Rate Limits to allow some matching traffic through when the Rule Action is in effect.

Thresholds

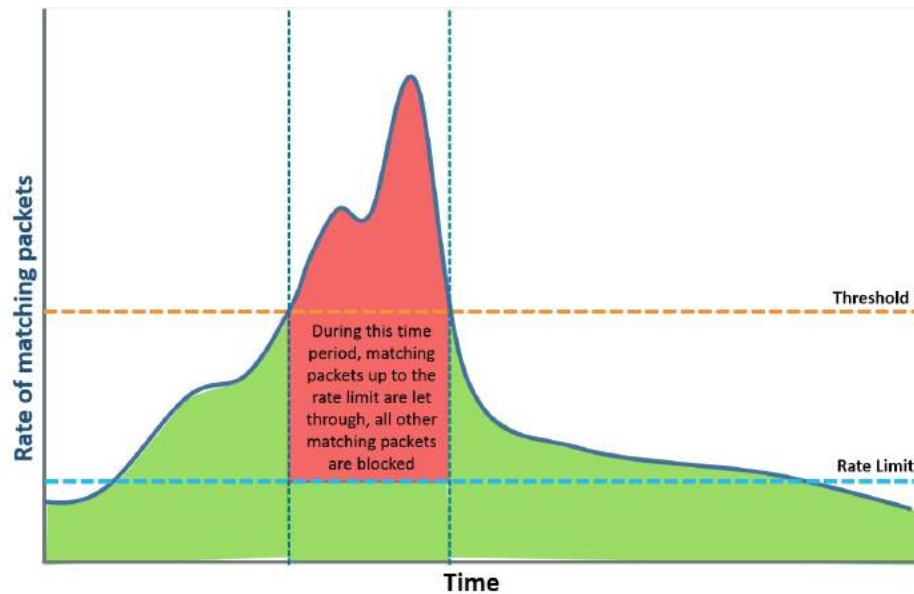
If you want to only trigger the Rule Action once a specific rate of matching traffic is detected, you need to set a traffic rate Threshold. The graph below shows how a non-zero Threshold affects traffic which matches a filter on a Block Flex-Rule.



There can be a short delay between the traffic passing a threshold and the Flex-Rule triggering. This is because the Flex-Rule takes an average traffic rate and, if traffic rises slowly, the Flex-Rule doesn't see the threshold has been crossed straight away. However, when traffic rises sharply, the rule triggers almost immediately providing a fast response against large attacks.

Rate Limits

A Rate Limit tells the Defense device to let a certain rate of traffic through once the Threshold has been crossed. For example, if you set the Rate Limit to 5000pps then once the Threshold is crossed, the Defense device allows 5000 matching packets through every second and performs the Rule Action on the rest. If you set the Rate Limit to 0, it will perform the Rule Action on all matching traffic once the Threshold is crossed. The graph below shows how a non-zero Rate Limit and Threshold affect traffic which matches a filter on a Block Flex-Rule.



Detecting traffic rates for Thresholds and Rate Limits

There are two types of detection method you can use to measure thresholds:

- **Packet Rate (pps)** – Use the number of matching packets to determine traffic rate
- **Bit Rate (bps)** – Use the size (in bits) of matching traffic to determine traffic rate

By default, only the Packet Threshold and Rate Limit contain a value (0 to signify the Rule Action is trigger by any rate of traffic matching a filter). If you edit the Packet Rate fields to enable a Threshold and Rate Limit, you can choose to leave the Bit rate fields blank or also to add a Bit Threshold and Rate Limit. If both detection methods are used, the Threshold that is reached first will trigger the Rule Action.

Tip: If you want to only use Bit Rate as your detection method, you can set very high Packet Rate values. This ensures it is always the Bit Threshold which triggers the Rule Action.

Types of Flex-Rule

TDD Deployments: All Flex-Rules should be disabled except for the TDD specific Flex-Rules (cns-002621, cns-002622, cns-002623, and cns-002624) and the TDD Flexible Configuration Tool Flex-Rules (cns-002611, cns-002612, and cns-002613) . See the **Smartwall TDD Getting Started Guide** for more configuration information.

There are 3 default Flex-Rules:

- **cns-002500 (Block only Flex-Rule)** – Primary rule for filters which block matching traffic. The Rule Action can be set to Block, or Disabled.

- **cns-002501 (Programmable Flex-Rule)** – Primary configurable rule which is reserved for use with SWA and other integrated systems. Adding filters is only available through the REST API. All other configuration is available in the Web UI and CLI. The Rule Action can be set to Block, Detect, or Disabled.
- **cns-002502 (Detect only Flex-Rule)** – Primary rule for filters which detect matching traffic. The Rule Action can be set to Detect, or Disabled.

There are 4 TDD specific Flex-Rules:

- **cns-002621 (NTP Monlist Response TDD Flex-Rule)** – Contains two filters which are used by the TDD system to block NTP Monlist Response attack traffic
- **cns-002622 (SSDP Reflection TDD Flex-Rule)** – Contains two filters which are used by the TDD system to block SSDP Reflection attack traffic
- **cns-002623 (Empty UDP data TDD Flex-Rule)** – Contains two filters which are used by the TDD system to block Empty UDP data attack traffic
- **cns-002624 (Memcache TDD Flex-Rule)** – Contains two filters which are used by the TDD system to block Mem-cache attack traffic

There are 3 Flex-Rules reserved for use with the TDD Flexible Configuration Tool:

- **cns-002611 (CORERO_MANUAL_WHITELIST TDD Flex-Rule)** – Contains any egress filters created using the Flexible Configuration Tool in the SWA
- **cns-002612 (CORERO_MANUAL_BLOCK TDD Flex-Rule)** – Contains any block filters created using the Flexible Configuration Tool in the SWA
- **cns-002613 (CORERO_MANUAL_DETECT TDD Flex-Rule)** – Contains any detect filters created using the Flexible Configuration Tool in the SWA

There are 111 additional Flex-Rules you can add to provide space for additional filters:

- **100 General Flex-Rules (cns-002503 to cns-002512 and cns-002611 to cns-002700)** – Configurable rules for filters which need a different Match Rate Limit to the default rules or which you want to report on separately. The Rule Action can be set to Block, Detect, Egress, or Disabled.
- **11 Programmable Flex-Rules (cns-002600 to cns-002610)** – Configurable rules which are reserved for use with SWA and other integrated systems. Adding filters is only available through the REST API. All other configuration is available in the Web UI and CLI. The Rule Action can be set to Block, Detect, or Disabled.

Flex-Rule Filters

For a Flex-Rule to affect traffic, you need to create filters that define the traffic types the Flex-Rule should block or detect. Flex-Rule filter definitions must be written as a Berkeley Pack Filter (BPF) syntax expression.

You can have up to 200 filters per Flex-Rule. However, the total number of filter description characters available for each Flex-Rule is 7000. Therefore, the amount of filters available for a rule can depend on the size of the filter descriptions already on that rule.

Tip: Each rule has a revision number which is incremented each time you make a change to the rule's filters, and that revision number is cited in relevant syslog messages.

Evaluation order

Flex-Rules are evaluated in order; first by Rule Action, then by rule number and finally by filter order on the rule:

- **General Flex-Rules with the rule action Egress** – The filters from top to bottom on each General Flex-Rules set to Egress, in rule number order.
- **Block Only Flex-Rule** – The filters on rule cns-002500, from top to bottom.
- **General Flex-Rules with the rule action Block** – The filters from top to bottom on each General Flex-Rules set to Block, in rule number order.
- **Programmable Flex-Rules with the rule action Block** – The filters from top to bottom on each Programmable Flex-Rules set to Block, in rule number order.
- **Programmable Flex-Rules with the rule action Detect** – The filters from top to bottom on each Programmable Flex-Rules set to Detect, in rule number order.
- **Detect Only Flex-Rule** – The filters on rule cns-002502, from top to bottom.
- **General Flex-Rules with the rule action Detect** – The filters from top to bottom on each General Flex-Rules set to Detect, in rule number order.

Once a packet matches a Flex-Rule filter, it is not inspected by any subsequent filters on that rule, or on any subsequent Flex-Rules.

Enable/Disable a Flex-Rule

A Flex-Rule is enabled when it has a Rule Action of **Block**, **Detect**, or **Egress**. When a Flex-Rule is enabled, you can enable/disable individual filters on that rule. To disable all the filters associated with a Flex-Rule, set the Flex-Rule Rule Action to **Disabled**. When you disable a Flex-Rule, none of the filters will function, even if they are individually enabled.

Managing Flex-Rules



TDD Deployments: All Flex-Rules should be disabled except for the TDD specific Flex-Rules (cns-002621, cns-002622, cns-002623, and cns-002624) and the TDD Flexible Configuration Tool Flex-Rules (cns-002611, cns-002612, and cns-002613) . See the **Smartwall TDD Getting Started Guide** for more configuration information.

You can configure Flex-Rule level settings that affect all filters on that rule. Until you add a filter to the Flex-Rule, they won't affect your defense Policy.


There are multiple Flex-Rules you can configure; however, some Flex-Rules are managed in different ways:



- **Block Only** (1 rule) – Primary rule for filters which block matching traffic. Can be set to Block or Disabled.
- **Detect Only** (1 rule) – Primary rule for filters which detect matching traffic. Can be set to Detect or Disabled.
- **General** (100 rules) – Configurable rules for filters which need a different configuration to the primary rules or which you want to report on separately. Can be set to Block, Detect, Egress, or Disabled.
- **Programmable** (1 primary rule and 11 additional rules) – Configurable rules which are reserved for use with SWA and other integrated systems. Adding filters is only available through the REST API. All other configuration is available in the Web UI and CLI. Can be set to Block, Detect, or Disabled.

To configure an existing Flex-Rule

1. Use the left-hand menu to navigate to **Policy > Flex-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Make sure the **RULES** tab is selected.
4. From the Rules table, click  the edit button next to the Flex-Rule you want to edit.
5. Select a **Rule Action** for this Rule. To disable a Flex-Rule and all filters on that rule, set this to Disabled. Otherwise select the appropriate Rule Action from Block, Detect, or Egress.
6. (Optional) Enable **Packet Rate** Threshold and Rate Limit:
 - a. From the drop-down, select **enabled**.
 - b. Set the **Packet Threshold** for the filters on this rule; this is the rate of packets per second which need to match the filter before the Rule Action is triggered.
 - c. You can optionally also set the **Packet Rate Limit**; this is the rate of packets per second which are allowed to pass unaffected by the Rule Action, once the Threshold has been reached.
7. (Optional) Enable **Bit Rate** Threshold and Rate Limit:
 - a. From the drop-down, select **enabled**.
 - b. Set the **Bit Threshold** for the filters on this rule; this is the rate of bits per second which need to match the filter before the Rule Action is triggered.
 - c. You can optionally also set the **Bit Rate Limit**; this is the rate of bits per second which are allowed to pass unaffected by the Rule Action, once the Threshold has been reached.
8. [Add or edit the Flex-Rule filters](#) on this rule. Return to the Edit Flex-Rule dialog.
9. Click **Save**.
10. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

To create a new General or Programmable Flex-Rule

1. Use the left-hand menu to navigate to **Policy > Flex-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Make sure the **RULES** tab is selected.
4. At the Rules table, click **Add**.
5. Type a **Name** for the new Flex-Rule.
6. From the Rule drop-down, select from the available rule numbers. Select from **cns-002503 to cns-002512** or **cns-002611 to cns-002700** to create a General Flex-Rule, or select from **cns-002600 to cns-002610** to create a Programmable Flex-Rule.
7. Select a **Rule Action** for this Rule. To disable a Flex-Rule and all filters on that rule, set this to **Disabled**. Otherwise select the appropriate Rule Action from **Block**, **Detect**, or **Egress**. Note: Egress is not available for Programmable Flex-Rules.
8. (Optional) Enable **Packet Rate** Threshold and Rate Limit:
 - a. From the drop-down, select **enabled**.
 - b. Set the **Packet Threshold** for the filters on this rule; this is the rate of packets per second which need to match the filter before the Rule Action is triggered.
 - c. You can optionally also set the **Packet Rate Limit**; this is the rate of packets per second which are allowed to pass unaffected by the Rule Action, once the Threshold has been reached.
9. (Optional) Enable **Bit Rate** Threshold and Rate Limit:
 - a. From the drop-down, select **enabled**.
 - b. Set the **Bit Threshold** for the filters on this rule; this is the rate of bits per second which need to match the filter before the Rule Action is triggered.
 - c. You can optionally also set the **Bit Rate Limit**; this is the rate of bits per second which are allowed to pass unaffected by the Rule Action, once the Threshold has been reached.
10. (General Flex-Rules only) [Add Flex-Rule filters](#) on this rule. Return to the Edit Flex-Rule dialog.
11. Click **Save**.
12. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Rules table you can use the following action buttons to edit  or delete  filters. On the Flex-Rules table, you can also view the filters on each rule by expanding the table rows.

CLI Commands (All Flex-Rules)

Create a new General or Programmable Flex-Rule

Tip: You can also use this method to rename a General or Programmable Flex-Rule.

```
configure
set policy protection-profile <ppName> flex-rule-blocking
[programmable|general] <ruleNumber> name <ruleName>
commit
```

Note: When creating a new General or Programmable Flex-Rule, you must provide an unused <ruleNumber>. If you provide one already allocated to a Flex-Rule, you will edit the existing Flex-Rule rather than create a new one.

Set the Rule Action for a Flex-Rule

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] rule-action
[block|detect|disabled|egress]
commit
```

Note: For the block-only Flex-Rule, you can only choose block or disabled. For the detect-only Flex-Rule you can only choose detect or disabled. For Programmable Flex-Rules you can choose block, detect, or disabled. For a General Flex-Rule you can choose block, detect, egress, or disabled. Selecting any Rule Action except disabled, will enable the Flex-Rule.

Change the Packet Threshold and Rate Limit for a Flex-Rule

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] packet-rate
admin-state [disabled|enabled] threshold <ppsRate> rate-limit <ppsRate>
commit
```

Change the Bit Threshold and Rate Limit for a Flex-Rule

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] bit-rate
admin-state [disabled|enabled] threshold <bpsRate> rate-limit <bpsRate>
commit
```

Delete configuration of a General or Programmable Flex-Rule

```
configure
```

```
edit policy protection-profile <ppName> flex-rule-blocking
delete [programmable|general] [ruleNumber|ruleName]
commit
exit
```

Types of Flex-Rule Filters

Caution: It is Corero's recommendation to craft destination specific rules, to limit the impact of these rules to the intended destinations only.

To write a filter definition, you need to first use the historic attack data in SmartWall SecureWatch Analytics to identify a common type of attack traffic for your network. You then need to craft a definition that will target only that specific type of attack traffic and not anything else; perhaps a specific combination of destination IP address, TCP port, and packet length. Finally, you can write that definition out as a BPF syntax expression. For example, if you used the following definition to create a filter on the Block-only rule, you could block a common type of SSDP reflection attack:

```
udp and (udp[8:4]=0x48545450 and (udp[12:4]=0x2f312e31 or udp[12:4]=0x2f312e30))
```

Caution: Flex-Rules are very powerful tools capable of blocking finely-targeted attacks. Therefore, pay careful attention when defining a Flex-Rule filter, as a simple mistake in typing the filter syntax can have unintentionally damaging effects on other traffic you want to continue receiving. A simplistic example is that of using the Boolean operator "OR" instead of "AND", but more subtle mistakes, such as misplaced parentheses or an incorrect port ID, can have significant unintended consequences, also. Even if you are defining a Flex-Rule in response to an ongoing attack, take time to define it carefully.

There are three types of Flex-Rule filters which each require slightly different use of syntax in the definition:

- **Fixed pattern match** – If you need to look for expected and fixed packet characteristics and patterns, you can use the standard BPF syntax
- **Flexible pattern match** – If you need to search the packets content looking for patterns which could appear in different parts of each packet, you also need to use Corero specific search syntax.
- **Flex-Rule IP table filters** – You can write a filter which can check SIPs or DIPs from incoming packets, against a table of IP addresses stored in the CMS.

Flexible pattern match

If you want to use a Flex-Rule to target packets which contain a specific pattern that can appear at any point in the packet, you can use additional syntax created by Corero as an extension to the BPF library. For example, you may

experience attack traffic where each packet contains similar but not identical URLs (e.g. each has a different prefix). You can use the search syntax to look for the common section of the URL which can be found in all related packets.

The search syntax uses the following structure to find a pattern inside a specified block within the packet:

```
<protocol>["<pattern>":<offset>:<size>]
```

You would need to replace the following placeholders:

- *<protocol>* – The protocol of the packets you're targeting. Can be: `udp`, `tcp`, `icmp`, or `setp`.
- *<pattern>* – The pattern you want to search for. If it is a string value it must be within the quotation marks (e.g. `"company.com"`).

Caution: Instead of searching for a string, you could use the following syntax to include a regular expression. However, this can adversely affect your performance speed. *<protocol>*

```
[re"<regex>":<offset>:<size>]
```

- *<offset>* – The number of bytes after the IP header you want to skip before beginning the search. If you don't specify a value, the default is 0. For example, `udp["company.com"]` uses the default offset and size values.
- *<size>* – The size (in bytes) of the block in the packet you want to search for the pattern. If you don't specify a value, the default is 64. If there is not offset value set, the block begins after the IP header.



For example, to target all UDP packets which contain `"company.com"` in a 50 byte block starting 8 bytes in from the IP header, you would add the following to a Flex-Rule:

```
udp["company.com":8:50]
```

Tip: If the pattern you want to search for is a hex value, you must use specific formatting to stop the filter converting it. For example to search for a hex value containing `"58575655"`, you need to format it like this: `"\x58\x57\x56\x55"`. A flexible pattern match filter looking for that hex value in `udp` packets would look something like: `udp["\x58\x57\x56\x55":8:50]`

Flex-Rule IP table filters

You can create Flex-Rule filters, which can compare a SIP or DIP on an incoming packet against a list of stored IP addresses. You can store up to three tables of IP addresses as Flex-Rule IP Address Tables. Each Flex-Rule IP Address Tables is comprised of one or more [Address Groups](#).

To write these IP table filters, you need to use additional syntax created by Corero as an extension to the BPF library:

iptables

This allows an ip-address to be checked against a table of addresses and returns true if a match is found and false if not. For example, a filter with this definition `ip and src iptable botnet_table`, would match traffic with a source IP address that matched any of the IP addresses in the IP Address Table named "botnet_table".

```
[src|dst] iptable <tableName>
```

You would need to replace the following placeholders:

- `[src|dst]` – Replace with `src` to compare the packet SIP to the IP Address Table, or replace with `dst` to compare the packet DIP to the IP Address Table
- `<tableName>` – Replace with the name of the Flex-Rule IP Address table you want to reference

tablesize

This returns the size (number of entries) currently present in the table and can be compared to a value using the binary comparison operators (>, <=, etc). For example this can be an important safety guard against a mis-populated table, especially for a negative check. The following filter will fail safely in the case where the "Australia" IP Address table did not get populated: `ip and udp and tablesize Australia > 0 and not src iptable Australia`

```
tablesize {tableName} {>|<|==|!=|>=|<=} {value}
```

You would need to replace the following placeholders:

- `tableName` – Replace with the name of the Flex-Rule IP Address table you want to reference
- `[>|<|==|!=|>=|<=]` – Replace with one of the possible operators
- `<value>` – Replace with a value representing the number of table entries you want to compare with the current table size

Managing Flex-Rule Filters


TDD Deployments: Do not edit the default Flex-Rule Filters on a TDD system. Changing these filters can result in false positives in the attack detection engine in the SWA. The Flex-Rule Filters implemented when you first configured the TDD Policy should be sufficient for most deployments. If you do not want to use them, [disable the Flex-Rule](#) or contact your support representative. See the **Smartwall TDD Getting Started Guide** for more configuration information.

For a Flex-Rule to affect traffic, you need to create filters on that Flex-Rule, which define the traffic types the Flex-Rule should block/detect. Filter definitions must be written using Berkeley Pack Filter (BPF) syntax. In addition to the BPF syntax you can use Corero specific syntax to search packets.

You can add filters to any of the Flex-Rules, however some Flex-Rules are managed in different ways:


- **Block Only** (1 rule) – Primary rule for filters which block matching traffic. Can be set to Block or Disabled.
- **Detect Only** (1 rule) – Primary rule for filters which detect matching traffic. Can be set to Detect or Disabled.
- **General** (100 rules) – Configurable rules for filters which need a different configuration to the primary rules or which you want to report on separately. Can be set to Block, Detect, Egress, or Disabled.
- **Programmable** (1 primary rule and 11 additional rules) – Configurable rules which are reserved for use with SWA and other integrated systems. Adding filters is only available through the REST API. All other configuration is available in the Web UI and CLI. Can be set to Block, Detect, or Disabled.



To create a Flex-Rule filter (except Programmable Flex-Rules)

1. Use the left-hand menu to navigate to **Policy > Flex-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Make sure the **RULES** tab is selected.
4. From the Rules table, click  the edit button next to the Flex-Rule you want to add a filter to.
5. At the Filters table, click **Add**.
6. Type a **Name** for the new filter. You must only use alphanumeric, spaces, or `.-&()/_/@:=` symbols.
7. Select the Admin State:
 - **Enable** – To enable the Flex-Rule filter, and either block/detect/egress (depending on the Flex-Rule's Rule Action) the traffic which matches this filter
 - **Disable** – To disable the Flex-Rule filter
8. [Write a Definition for the filter](#). This must be a Berkeley Packet Filter (BPF) syntax expression which defines the characteristics of the packets you want the Defense device to affect.
9. Click **Save**.

10. Check that the new filter is compatible with the current Flex-Rule configuration:
 - If a Threshold and Rate Limit is set, check it is sensible for this new filter
 - Check that the Rule Action is correct for this new filter

If the filter is not compatible with this Flex-Rule, delete it and recreate it on a [new Flex-Rule](#) configured as you require.

11. Click **Save**.
12. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Filter table, in the Edit Flex-Rule dialog, you can use the following action buttons to edit  or delete  filters. On the Flex-Rules table, you can also view the filters on each rule by expanding the table rows.

CLI Commands

View current filters

```
show configuration policy protection-profile <ppName> flex-rule-blocking
[block-only|detect-only|general|programmable]
```

Create a new filter (Not available for Programmable Flex-Rules)

Tip: The filter must be within quotation marks or you won't be able to commit the change.

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|general <ruleNumber>] filter <filterName> admin-state
[disabled|enabled] definition "<bpfFilter>"
commit
```

Edit an existing filter

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] filter
<filterName> definition "<bpfFilter>"
commit
```

Rename a filter

```
configure
request policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] filter
<filterName> rename name <newName>
commit
```

Delete a filter



```
configure
edit policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>]
delete filter <filterName>
commit
exit
```

Enable/Disable a filter

```
configure
set policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable <ruleNumber>|general <ruleNumber>] filter
<filterName> admin-state [disabled|enabled]
commit
```

To re-order Flex-Rule filters

Note: In the CMS Web UI, rearranging the table using column sort does not affect the evaluation order. After sorting by column, you can refresh the page to see the evaluation order again.

1. Use the left-hand menu to navigate to **Policy > Flex-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Make sure the **RULES** tab is selected.
4. From the Rules table, click  the edit button next to the Flex-Rule you want reorder filter on.
5. In the filters table, filters are evaluated from top to bottom. Use the Priority column to drag and drop filters into the order you want them evaluated.
6. If you want to save the new configuration, and push your changes to any affected Defense devices, click  . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands


```
configure
edit policy protection-profile <ppName> flex-rule-blocking [block-
only|detect-only|programmable|general <ruleNumber>]
move filter <filterName> [after|before|first|last]
commit
```

Tip: If you have a long list of filters to reorder, it helps to write out the new order, then set the filter you want to begin with to `first`. Then you can set each following filter as `after` the one before it in the list.

Troubleshooting

Flex-Rule filters are not blocking/detecting traffic

There are a few things to check:

- Check that the filter is enabled. Select the correct rule tab and locate the filter in the table. To enable a filter, click  the edit button.
- Check that [the Flex-Rule itself is enabled](#). Select the correct rule tab and check the **Rule Action** is **block** or **detect**.
- Check that the [Match Rate for this rule](#) isn't too high for your current traffic to start matching the filter. Select the correct rule tab and check the **Match Rate Limit**. If only one or two filters require a different Match Rate Limit, you can [configure a new General Flex-Rule](#) to hold just those filters with the altered Match Rate Limit.
- If you're using a [Flex-Rule Lookup Table](#), check that the name is correct and that it is populated with the correct list of IP addresses. Editing the associated [Address Groups](#), will affect your Flex-Rule Lookup Tables.
- Check that your filter order makes logical sense. You can see which filters are being matched with traffic using SecureWatch Analytics. Search for `cat=security,type=rule-stats` and look for the `cfg-frn` field for the filter name being matched for each event logged.

If everything else looks correct, you may have an issue with your filter definition. Contact Support for more specific assistance.

Managing Flex-Rule IP Tables



You can create Flex-Rule filters that compare incoming traffic against a list of IP addresses stored in a Flex-Rule IP Table. The tables must be stored and maintained in the CMS.

Note: You can create three Flex-Rule IP Tables per Protection Profile.

Prerequisites



- [Import lists of known IP addresses as one or more Address Groups](#). This could be a geographical grouping, a suspected botnet, a trusted set of destination IPs, etc. Each Flex-Rule IP Table can contain multiple Address Groups, and Address Groups can be referenced by more than one Flex-Rule IP Table.

To create a Flex-Rule IP Table

1. Use the left-hand menu to navigate to **Policy > Flex-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **IP TABLES** tab.
4. At the filter table, click **Add**.
5. Type a **Name** for the new table. The name can only include letters and numbers and must start with a letter.
6. Click **Add**.
7. Select an **Address Group** from the drop-down.
8. Click **Save**.
9. You can use a single Address Group, or you can continue to add them to the table in the same way. You can also use  the delete button to modify your list.
10. When you're happy with your table, click **Save**.
11. If you want to save the new configuration, and push your changes to any affected Defense devices, click  **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Next Step

- [Create a Flex-Rule filter which references this table](#)

Tip: On the IP Tables table, you can use the following action buttons to edit  or delete  Flex-Rule IP Tables.

CLI Commands

View Address Groups in a Flex-Rule IP Table

```
show configuration policy protection-profile <ppName> flex-rule-blocking ip-
table <tableName>
```

Create a new Flex-Rule IP Table

```
configure

set policy protection-profile <ppName> flex-rule-blocking ip-table
<tableName> address-group <agName>

commit
```

Edit a Flex-Rule IP Table

```
configure

edit policy protection-profile <ppName> flex-rule-blocking ip-table
<tableName>
```

Tip: Use the `set address-group <agName>` command to add another Address Group or the `delete address-group <agName>` command to remove an Address Group.

```
commit

exit
```

Rename a Flex-Rule IP Table

```
configure

request policy protection-profile <ppName> flex-rule-blocking ip-table
<tableName> rename name <newName>

commit
```

Delete a Flex-Rule IP Table

```
configure

edit policy protection-profile <ppName> flex-rule-blocking

delete ip-table <tableName>

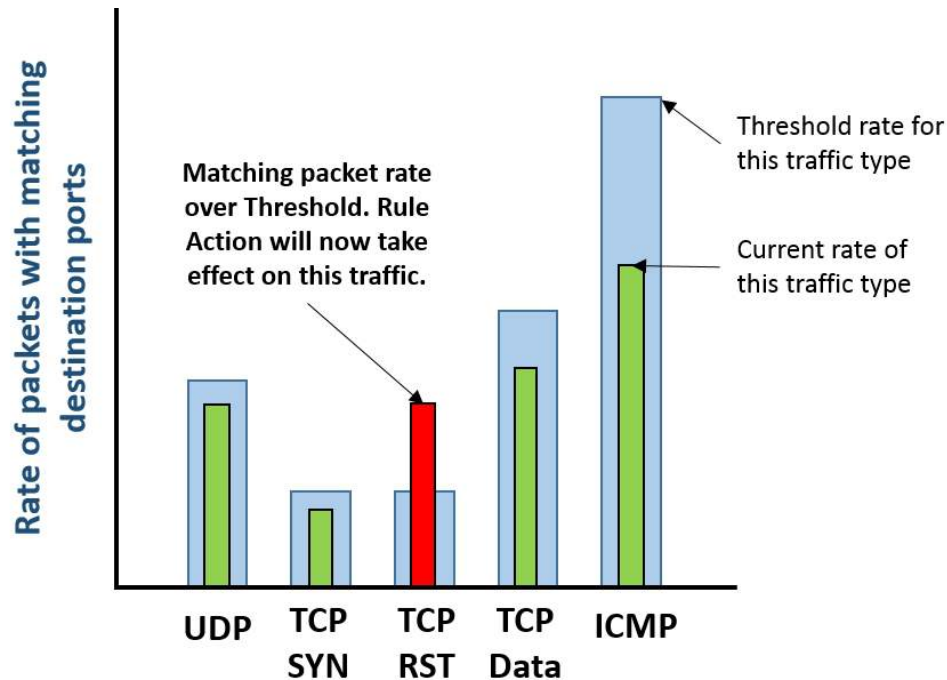
commit

exit
```


Smart-Rules

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Smart-Rules Screen reference topic](#).

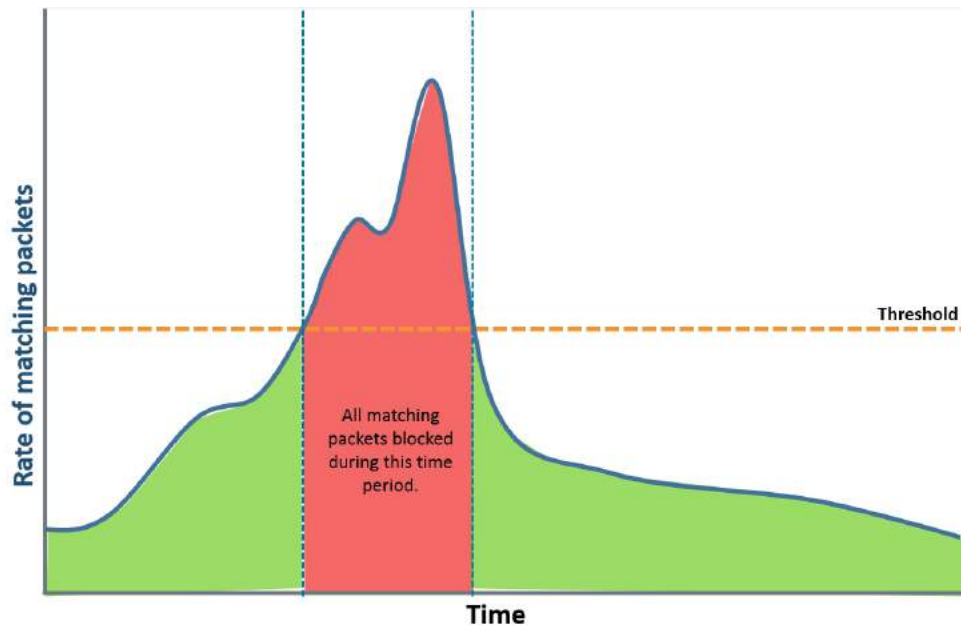
Smart-Rules is an attack mitigation feature. For each traffic type, a Smart-Rule looks for a large number of packets with similar characteristics. Once the number of these packets passes a set threshold, which denotes a flood attack is happening, the Smart-Rule can surgically block just the packets which match those attack characteristics.



Smart-Rule Thresholds

TDD Deployments: Smart-Rules cannot be set to Detect for TDD Deployments. See the **Smartwall TDD Getting Started Guide** for more configuration information.

For each Smart-Rule, a proprietary algorithm monitors that rule's related fields in every incoming packet. When a high number of packets arrive with the same value in those fields, the rule sees this as an attack and can drop all the packets which match the Smart-Rule. Most Smart-Rules only act on one traffic type; therefore, if a flood of packets with the same source IP address triggers the Reflection TCP SYN Smart-Rule, the Defense device can drop those packets but it won't drop a normal volume of UDP packets, with the same source IP, which came through at the same time. However, if the volume of UDP packets with matching source IP addresses later rose and passed the threshold for the Reflection UDP Smart-Rule, they would be dropped by the Defense device.



For each Smart-Rule, you need to set a threshold value and an action the system should perform once that threshold is passed. You can use SmartWall SecureWatch Analytics to determine what your average rate is for each traffic type, then set the Smart-Rule threshold to around three times that. This ensures that the Smart-Rule action only triggers when an abnormal amount of matching traffic, of that type, is seen.

There are two types of detection method you can use to measure thresholds:

- **Bit rate (bps)** – Use the size (in bits) of this traffic type to determine traffic rate
- **Packet rate (pps)** – Use the number of packets of this traffic type to determine traffic rate

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.

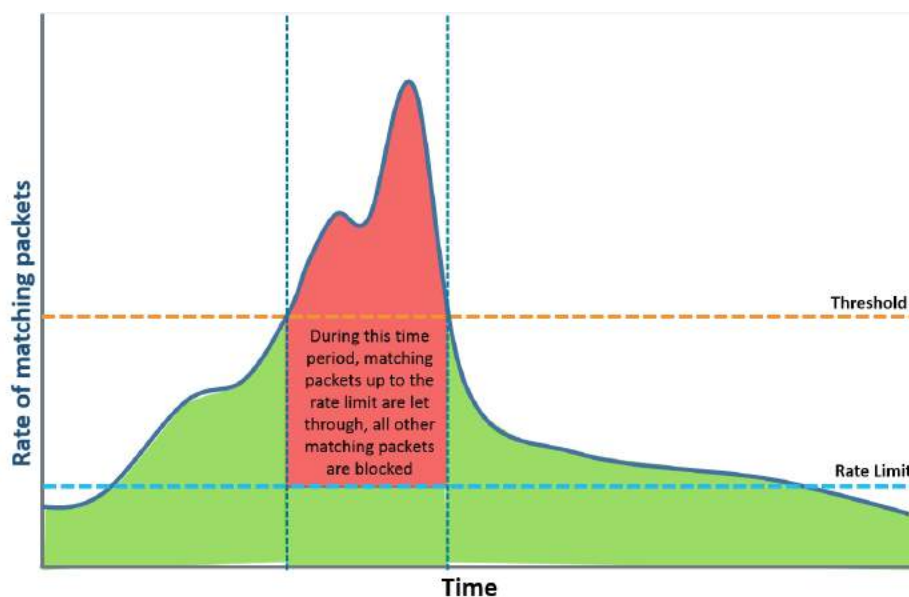
Once the volume of traffic with matching fields, of a specific traffic type, passes the threshold value, there are three action types a Smart-Rule can perform:

- **Block** – The Defense device blocks all traffic matching the rule definition
- **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
- **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.

There can be a short delay (around a second) between the traffic passing a threshold and the Smart-Rule triggering. This is because the Smart-Rule, takes an average traffic rate and if traffic rises slowly, the Smart-Rule doesn't see the threshold has been crossed straight away. However, when traffic rises sharply, the rule triggers almost immediately, providing a fast response against large attacks.

Rate Limits

A Rate Limit tells the Defense device to let a certain rate of traffic through once the Threshold has been crossed. For example, if you set the Rate Limit to 5000pps then once the Threshold is crossed, the Defense device allows 5000 matching packets through every second and drops the rest. If you set the Rate Limit to 0, it will drop all matching traffic once the Threshold is crossed.



Tip: The Thresholds and Rate Limits of Smart-Rules can be scaled up or down for selected destination IP addresses using the [Smart-Rule Scale](#) feature in Inspection Control override entries.

Smart-Rule Types

There are five Smart-Rules categories. Each category looks for matching values in different fields and, in each category, there are Smart-Rules which act on specific traffic types:

Service

TDD Deployments: All Service Smart-Rules must be set to **block** and a custom Smart-Rule created for **destination port 53**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

The Service Smart-Rules look for a flood of packets with the same destination port, where an attacker could be targeting a specific service in your network.

- **UDP Any Destination Port** – This Smart-Rule looks for all UDP packets with matching destination ports
- **TCP SYN** – This Smart-Rule looks for TCP SYN packets with matching destination ports
- **TCP RST** – This Smart-Rule looks for TCP RST packets with matching destination ports
- **TCP Data** – This Smart-Rule looks for all other TCP packets with matching destination ports
- **TCP PSH/ACK** – This Smart-Rule looks for TCP PSH ACK packets with matching destination ports
- **ICMP Any Type** – This Smart-Rule looks for all ICMP packets with matching destination ports

Reflection

TDD Deployments: All Reflection Smart-Rules must be set to **block** except for DNS Query Response. See the **SmartWall TDD Getting Started Guide** for more configuration information.

The Reflection Smart-Rules look for a flood of packets with the same source port. An attacker could have made a spoofed request, with your IP range, to an internet server which then reflects the attack back to your network, causing a packet flood.

- **UDP or ICMP Any Source Port** – This Smart-Rule looks for all UDP or ICMP packets with matching source ports
- **UDP Source Port 53** – This Smart-Rule looks for all UDP packets containing source port 53. Port 53 is generally used for DNS and often sees a lower volume of traffic.
- **UDP Source Port 4500** – This Smart-Rule looks for all UDP packets containing source port 4500. Port 4500 is generally used for VPN and often sees a higher volume of traffic.
- **TCP SYN/ACK** – This Smart-Rule looks for TCP SYN ACK packets with matching source ports
- **TCP RST** – This Smart-Rule looks for TCP RST packets with matching source ports
- **TCP PSH/ACK** – This Smart-Rule looks for TCP ACK PSH packets with matching source ports
- **DNS Query Response** – This Smart-Rule looks for all DNS Query Response packets with matching source ports. This could be the result of an Amplification attack, where the attacker has taken advantage of a recursive DNS request to reflect a flood of responses to your network.

Group traffic using DNS Query Response parameters

You can further refine the Reflection DNS Query Response Smart-Rule by selecting or deselecting signature parameters, which the Defense device can look for on the incoming packets.

Selecting a parameter modifies how the traffic is grouped together when applying Thresholds and Rate Limits. For example, when **DNS Signature is Fragmented** is not selected, grouping does not depend on whether the packet is a fragment or not. However, when **DNS Signature is Fragmented** is selected, whether a packet is fragment is used, in addition to the default criteria used to split the traffic into groups. The result is that packets which are fragmented are

measured in one group, while non-fragmented packets are measured in another group. The rate of packets assigned to a single group must exceed the configured Threshold to trigger the Rule Action.

Note: If you select an option to separate traffic into smaller groups or deselect an option to aggregate the traffic into a large group, you should adjust your Thresholds to reflect the change.

You can use this feature to separate traffic in the following ways:

- **DNS Signature Any** – The traffic is separated into two further groups; one for the rate of packets with the request type "ANY" and one for the rate of packets where it is not "ANY".
- **DNS Signature is Fragmented** – The traffic is separated into two further groups; one for the rate of packets which are fragments and one for the rate of packets which are not fragments.
- **DNS Signature Packet Length** – The traffic is further refined into multiple groups; one for each packet length. The rate of packets which all have the same packet length must cross a Threshold to trigger the Rule action.
- **DNS Signature Recursive** – The traffic is separated into two further groups; one for the rate of packets with "recursion desired" and one for the rate of packets without it.

Caution: Each option you select further refines your traffic into smaller groups. For example, if you selected **DNS Signature is Fragmented** and **DNS Signature Any** then, for each source port value, you would have four further sub-groups: fragmented with request type any, fragmented without request type any, non-fragmented with request type any, and non-fragmented without request type any.

Server

TDD Deployments: All Server Smart-Rules must be set to **block**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

The Server Smart-Rules look for a flood of packets with the same destination IP address, where an attacker could be targeting one of your assets.

- **UDP Any Port** – This Smart-Rule looks for UDP packets with matching destination IP addresses
- **UDP Fragment Under Attack** – This Smart-Rule looks for all UDP fragmented packets with matching destination IP addresses
- **TCP SYN** – This Smart-Rule looks for TCP SYN packets with matching destination IP addresses
- **TCP RST** – This Smart-Rule looks for TCP RST packets with matching destination IP addresses
- **TCP Data** – This Smart-Rule looks for all other TCP packets with matching destination IP addresses
- **ICMP Any Type** – This Smart-Rule looks for all ICMP packets with matching destination IP addresses
- **ANY Protocol** – This Smart-Rule looks for any other packets with matching destination IP addresses, which did not match the other Server Smart-Rules

Source

TDD Deployments: All Source Smart-Rules must be set to **disabled**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

The Source Smart-Rule looks for a flood of packets with the same source IP address, where an attacker could be sending a flood of traffic from a single source.

- **IP Any Source Address** – This Smart-Rule looks for any type of packets with matching source IP addresses

ICMP

TDD Deployments: All ICMP Smart-Rules must be set to **block**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

The ICMP Smart-Rules look for a flood of packets with ICMP error messages, where an attacker may have attempted a reflection attack, but sent the query to a disabled server, resulting in a flood of errors coming back to you.

- **ICMP Failed Reflectors** – This Smart-Rule looks for ICMP packets with matching destination ports

You can further refine the ICMP Smart-Rule to include or exclude packets which contain the following features:

- **UDP Destination Port** – The ICMP packet contains the original destination port (of the internet server now sending you the ICMP messages). By default, all ports in the table are enabled. This means that ICMP traffic, whose original destination port is listed on the table, will be counted by the Smart-Rule as potential attack packets. If you disable a port, then ICMP traffic with that original destination port number will not trigger the Smart-Rule, even if the rate goes above the Threshold. The following ports are listed and enabled by default:
 - **CHARGEN** – Default port number is 19
 - **DNS** – Default port number is 53
 - **LDAP** – Default port number is 389
 - **NETBIOS** – Default port number is 137
 - **NTP** – Default port number is 123
 - **RIP** – Default port number is 520
 - **RPC** – Default port number is 111
 - **SNMP** – Default port number is 161
 - **SSDP** – Default port number is 1900
 - **TFTP** – Default port number is 69

You can provide a description of each port, change the port number, or create a new table entry to reflect the types of attack you're seeing.

- **ICMP v4 Type** – By default, the types listed in the table are enabled. If the ICMP packet is one of the ICMP v4 types listed it will be counted by the Smart-Rule as a potential attack packet. If you disable a type, the ICMP packets matching that type will not trigger the Smart-Rule, even if the rate goes above the Threshold. The following types are listed and enabled by default:

- **Destination Unreachable** – Default ICMP v4 type number is 3 (type number can be between 0-63)
- **Time Exceeded** – Default ICMP v4 type number is 11 (type number can be between 0-63)

You can provide a description of each type, change the type number, or create a new table entry to reflect the types of attack you're seeing.

- **ICMP v6 Type** – By default, the types listed in the table are enabled. If the ICMP packet is one of the ICMP v6 types listed it will be counted by the Smart-Rule as a potential attack packet. If you disable a type, the ICMP packets matching that type will not trigger the Smart-Rule, even if the rate goes above the Threshold. The following types are listed and enabled by default:

- **Destination Unreachable** – Default ICMP v6 type number is 1 (type number can be between 0-191)
- **Time Exceeded** – Default ICMP v6 type number is 3 (type number can be between 0-191)

You can provide a description of each type, change the type number, or create a new table entry to reflect the types of attack you're seeing.

Custom Smart-Rules

A custom Smart-Rule enables you to specify the Smart-Rule configuration (threshold, rate limit, and rule action) for traffic with a specific protocol or a specific port. When you create a custom Smart-Rule which provides specific configuration for a traffic type, that traffic will no longer be affected by any other existing Smart-Rules.

For example, in the Server category the existing Smart-Rules enable you to set Thresholds for traffic with the same destination IP addresses of any protocol type. If you create a custom Smart-Rule specifically for GRE traffic, then all GRE traffic with matching destination IP addresses will be subject to the new Smart-Rule configuration and excluded from the existing Smart-Rule.

You can create custom Smart-Rules in the following categories: **Service** (UDP only), **Reflection** (UDP only), and **Server** (any protocol except TCP).

Programmable Smart-Rules

There are additional customizable Smart-Rules which you can configure using the CLI or REST API only. These are generally reserved for use with SWA and other integrated systems.

Caution: Implementing programmable Smart-Rules without assistance from your Support representative can lead to incorrect traffic handling.


Configuring Smart-Rules for Service Floods

TDD Deployments: All Service Smart-Rules must be set to **block** and a custom Smart-Rule created for **destination port 53**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

A service flood can happen during a DDoS attack and when a large number of packets appear with the same destination port, you can configure a Service Smart-Rule to block that packet flood. You can set Smart-Rules for five traffic types; for each type, you can set a Bit Rate and a Packet Rate Threshold.



Tip: If you need to specify Thresholds and Rate Limits for a more specific set of UDP destination ports, you can [create a custom Service Smart-Rule](#) to specify the Smart-Rule configuration (threshold, rate limit, and rule action) for that specific type of traffic and exclude it from the configuration of the more general Smart-Rules.

To configure a Smart-Rule to protect against service floods

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SERVICE** tab.
4. In the table, locate the Smart-Rule you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list of Smart-Rules.
5. Set the **Rule Action** for this Smart-Rule. It is triggered when the Packet Threshold or Bit Threshold is crossed.
 - **Block** – The Defense device blocks all traffic matching the rule definition
 - **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
 - **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.
6. Set the **Threshold** rate for your chosen traffic type/s (**Bit Rate**, **Packet Rate** or both). When the rate of that type of traffic (with the same destination port) goes past the Threshold, the Smart-Rule performs the associated Rule Action.

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.


7. (Optional) Set the associated **Rate Limit** for this traffic type. When the Rule Action is set to **Block**, the Rate Limit sets how much traffic of this type is still allowed through to the internal network.
8. (Optional) If you're not using one of the available traffic types (Bit Rate or Packet Rate), you can use the drop-down to disable that Threshold and Rate Limit.



9. (Custom Smart-Rules only) Use the **Destination Ports** table to create a list of the ports you want this Smart-Rule to specifically affect (ports not specified in a custom Smart-Rule are affected by the existing Smart-Rules). Type a UDP destination port number and click **Add**. You can use  the delete button to remove port numbers from the list.
10. Click **Save**.
11. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

To create a custom UDP Service Smart-Rule

Note: Customer Service Smart-Rules can only be used for UDP traffic.

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SERVICE** tab.
4. Click **Add**.
5. Type a unique **Name** for this Smart-Rule. You must only use alphanumeric, spaces, or `.-&()/_@:=` symbols.
6. Select an available **Rule** to map your new custom configuration to. There are three available rules for Service Smart-Rules.
7. Edit the Smart-Rule configuration (as above) and click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Smart-Rule table, you can use the following action buttons to edit  any Smart-Rules or delete  custom Smart-Rules.

CLI Commands

Tip: While editing the protocols list you can use the following command to remove protocol numbers from the list: `delete <portNumber>`

Edit a built-in Service Smart-Rule

configure

```
set policy protection-profile <ppName> smart-rule service [icmp|tcp-
data|tcp-psh-ack|tcp-rst|tcp-syn|udp] rule-action [block|detect|disabled]
[bit-rate|packet-rate] admin-state [disabled|enabled] threshold <rate>
rate-limit <rate>

commit
```

Edit a custom Service Smart-Rule

```
configure

edit policy protection-profile <ppName> smart-rule service custom service-
[1|2|3]

set name <name> rule-action [block|detect|disabled]

set [bit-rate|packet-rate] admin-state [disabled|enabled] threshold <rate>
rate-limit <rate>

set destination-ports <portNumber>

commit
```

Create a custom Service Smart-Rule

```
configure

set policy protection-profile <ppName> smart-rule service custom service-
[1|2|3] name <name> rule-action [block|detect|disabled] [bit-rate|packet-
rate] admin-state [disabled|enabled] threshold <rate> rate-limit <rate>

edit policy protection-profile <ppName> smart-rule service custom service-
[1|2|3] destination-ports

set <portNumber>

commit
```

Delete a custom Service Smart-Rule

```
configure

edit policy protection-profile <ppName> smart-rule service custom

delete service-[1|2|3]

commit
```


Configuring Smart-Rules for Reflection Floods

TDD Deployments: All Reflection Smart-Rules must be set to **block**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

A reflection flood can happen during a DDoS attack and when a large number of packets appear with the same source port, you can configure a Reflection Smart-Rule to block that packet flood. You can set Smart-Rules for seven traffic types; for each type, you can set a Bit Rate and a Packet Rate Threshold. You can set additional options to define attack packets for the DNS Query Response traffic type.



Tip: If you need to specify Thresholds and Rate Limits for a more specific set of UDP source ports, you can [create a custom Reflection Smart-Rule](#) to specify the Smart-Rule configuration (threshold, rate limit, and rule action) for that specific type of traffic and exclude it from the configuration of the more general Smart-Rules.

To configure a Smart-Rule to protect against reflection floods

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **REFLECTION** tab.
4. In the table, locate the Smart-Rule you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list of Smart-Rules.
5. Set the **Rule Action** for this Smart-Rule. It is triggered when the Packet Threshold or Bit Threshold is crossed.
 - **Block** – The Defense device blocks all traffic matching the rule definition
 - **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
 - **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.
6. Set the **Threshold** rate for your chosen traffic type/s (**Bit Rate**, **Packet Rate** or both). When the rate of that type of traffic (with the same source port) goes past the Threshold, the Smart-Rule performs the associated Rule Action.

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.

7. (Optional) Set the associated **Rate Limit** for this traffic type. When the Rule Action is set to **Block**, the Rate Limit sets how much traffic of this type is still allowed through to the internal network.

8. (Optional) If you're not using one of the available traffic types (Bit Rate or Packet Rate), you can use the drop-down to disable that Threshold and Rate Limit.
9. (DNS Query Response Smart-Rule only) Check the boxes to modify how the traffic is grouped together when applying Thresholds and Rate Limits:
 - **DNS Signature Any** – The traffic is separated into two further groups; one for the rate of packets with the request type "ANY" and one for the rate of packets where it is not "ANY".
 - **DNS Signature Is Fragmented** – The traffic is separated into two further groups; one for the rate of packets which are fragments and one for the rate of packets which are not fragments.
 - **DNS Signature Packet Length** – The traffic is further refined into multiple groups; one for each packet length. The rate of packets which all have the same packet length must cross a Threshold to trigger the Rule action.
 - **DNS Signature Recursive** – The traffic is separated into two further groups; one for the rate of packets with "recursion desired" and one for the rate of packets without it.
10. (Custom Smart-Rules only) Use the **Source Ports** table to create a list of the ports you want this Smart-Rule to specifically affect (ports not specified in a custom Smart-Rule are affected by the existing Smart-Rules). Type a UDP source port number and click **Add**. You can use  the delete button to remove port numbers from the list.
11. Click **Save**.
12. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).



Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

To create a custom UDP Reflection Smart-Rule

Note: Customer Reflection Smart-Rules can only be used for UDP traffic.

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **REFLECTION** tab.
4. Click **Add**.
5. Type a unique **Name** for this Smart-Rule. You must only use alphanumeric characters, spaces, or `.-&()/_@:=` symbols.
6. Select an available **Rule** to map your new custom configuration to. There are three available rules for Reflection Smart-Rules.
7. Edit the Smart-Rule configuration (as above) and click **Save**.

8. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Smart-Rule table, you can use the following action buttons to edit  any Smart-Rules or delete  custom Smart-Rules.

CLI Commands

Tip: While editing the protocols list you can use the following command to remove protocol numbers from the list: `delete <portNumber>`

Edit a built-in Reflection Smart-Rule

configure

```
set policy protection-profile <ppName> smart-rule reflection [dns-query-
response|tcp-ack-psh|tcp-rst|tcp-syn-ack|udp-or-icmp|udp-source-port-53|udp-
source-port-4500] rule-action [block|detect|disabled] [bit-rate|packet-
rate] threshold <rate> rate-limit <rate>
```

Note: For dns-query-response you can also set the following refinements to true or false: dns-signature-any, dns-signature-is-fragmented, dns-signature-packet-length, and dns-signature-recursive.

commit

Edit a custom Reflection Smart-Rule

configure

```
edit policy protection-profile <ppName> smart-rule reflection custom
reflection-[1|2|3]
set name <name> rule-action [block|detect|disabled]
set [bit-rate|packet-rate] admin-state [disabled|enabled] threshold <rate>
rate-limit <rate>
set source-ports <portNumber>
commit
```

Create a custom Reflection Smart-Rule

configure

```
set policy protection-profile <ppName> smart-rule reflection custom
reflection-[1|2|3] name <name> rule-action [block|detect|disabled] [bit-
```

```
rate|packet-rate] admin-state [disabled|enabled] threshold <rate> rate-limit
<rate>

edit policy protection-profile <ppName> smart-rule reflection custom
reflection-[1|2|3] source-ports

set <portNumber>

commit
```

Delete a custom Reflection Smart-Rule

```
configure

edit policy protection-profile <ppName> smart-rule reflection custom
delete reflection-[1|2|3]

commit
```


Configuring Smart-Rules for Server Floods

TDD Deployments: All Server Smart-Rules must be set to **block**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

A server flood can happen during a DDoS attack and when a large number of packets appear with the same destination IP address, you can configure a Server Smart-Rule to block that packet flood. You can set Smart-Rules for different traffic types; for each type, you can set a Bit Rate and a Packet Rate Threshold.


Tip: If you need to specify Thresholds and Rate Limits for a more specific set of protocols, you can [create a custom Server Smart-Rule](#) to specify the Smart-Rule configuration (threshold, rate limit, and rule action) for that specific type of traffic and exclude it from the configuration of the more general Smart-Rules.

To configure a Smart-Rule to protect against server floods


1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SERVER** tab.
4. In the table, locate the Smart-Rule you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list of Smart-Rules.
5. Set the **Rule Action** for this Smart-Rule. It is triggered when the Packet Threshold or Bit Threshold is crossed.
 - **Block** – The Defense device blocks all traffic matching the rule definition
 - **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
 - **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.
6. Set the **Threshold** rate for your chosen traffic type/s (**Bit Rate**, **Packet Rate** or both). When the rate of that type of traffic (with the same destination port) goes past the Threshold, the Smart-Rule performs the associated Rule Action.

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.

7. (Optional) Set the associated **Rate Limit** for this traffic type. When the Rule Action is set to **Block**, the Rate Limit sets how much traffic of this type is still allowed through to the internal network.
8. (Optional) If you're not using one of the available traffic types (Bit Rate or Packet Rate), you can use the drop-down to disable that Threshold and Rate Limit.


9. (Custom Smart-Rules only) Use the **Protocols** table to modify the list of the protocols you want this Smart-Rule to specifically affect (Protocols not specified in a custom Smart-Rule are affected by the existing Smart-Rules). Type an IP protocol number (e.g. 47 for GRE) and click **Add**. You can use  the delete button to remove protocols from the list.



Note: You cannot use TCP protocol (protocol number 6) when creating a Custom Server Smart-Rule. Use [Threat Awareness](#) to handle TCP floods with matching destination IP addresses.

10. Click **Save**.
11. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

To create a custom Server Smart-Rule

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SERVER** tab.
4. Click **Add**.
5. Type a unique **Name** for this Smart-Rule. You must only use alphanumeric characters, spaces, or .-&()/_/@:= symbols.
6. Select an available **Rule** to map your new custom configuration to. There are three available rules for Server Smart-Rules.
7. Edit the Smart-Rule configuration (as above) and click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Smart-Rule table, you can use the following action buttons to edit  any Smart-Rules or delete  custom Smart-Rules.

CLI Commands

Tip: While editing the protocols list you can use the following command to remove protocol numbers from the list: `delete <ipProtocolNumber>`

Edit a built-in Server Smart-Rule

```
configure

set policy protection-profile <ppName> smart-rule server [any|icmp|tcp-
data|tcp-rst|tcp-syn|udp|udp-fragment-under-attack] rule-action
[block|detect|disabled] [bit-rate|packet-rate] admin-state
[disabled|enabled] threshold <rate> rate-limit <rate>

commit
```

Edit a custom Server Smart-Rule

```
configure

edit policy protection-profile <ppName> smart-rule server custom protocol-
[1|2|3]

set name <name> rule-action [block|detect|disabled]

set [bit-rate|packet-rate] admin-state [disabled|enabled] threshold <rate>
rate-limit <rate> protocols

set <ipProtocolNumber>

commit
```

Create a custom Server Smart-Rule

```
configure

set policy protection-profile <ppName> smart-rule server custom protocol-
[1|2|3] name <name> rule-action [block|detect|disabled] [bit-rate|packet-
rate] admin-state [disabled|enabled] threshold <rate> rate-limit <rate>

edit policy protection-profile <ppName> smart-rule server custom protocol-
[1|2|3]

set protocols <ipProtocolNumber>

commit
```

Delete a custom Server Smart-Rule

```
configure

edit policy protection-profile <ppName> smart-rule server custom

delete protocol-[1|2|3]


commit
```

Configuring Smart-Rules for Source Floods


TDD Deployments: All Source Smart-Rules must be set to **disabled**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

A source flood can happen during a DDoS attack and when a large number of packets appear with the same source IP address, you can configure a Source Smart-Rule to block that packet flood. For this type, you can set a Bit Rate and a Packet Rate Threshold

To configure a Smart-Rule to protect against source floods

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SOURCE** tab.
4. In the table, click  the edit button.
5. Set the **Rule Action** for this Smart-Rule. It is triggered when the Packet Threshold or Bit Threshold is crossed.
 - **Block** – The Defense device blocks all traffic matching the rule definition
 - **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
 - **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.
6. Set the **Threshold** rate for your chosen traffic type/s (**Bit Rate**, **Packet Rate** or both). When the rate of that type of traffic (with the same destination port) goes past the Threshold, the Smart-Rule performs the associated Rule Action.

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.

7. (Optional) Set the associated **Rate Limit** for this traffic type. When the Rule Action is set to Block, the Rate Limit sets how much traffic of this type is still allowed through to the internal network.
8. (Optional) If you're not using one of the available traffic types (Bit Rate or Packet Rate), you can use the drop-down to disable that Threshold and Rate Limit.
9. Click **Save**.
10. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

CLI Commands

Edit a Source Smart-Rule

```
configure

set policy protection-profile <ppName> smart-rule source ip-address rule-
action [block|detect|disabled] [bit-rate|packet-rate] admin-state
[disabled|enabled] threshold <rate> rate-limit <rate>


commit
```

Configuring Smart-Rules for ICMP Floods

TDD Deployments: All ICMP Smart-Rules must be set to **block**. See the **Smartwall TDD Getting Started Guide** for more configuration information.

An ICMP flood can happen during a DDoS attack and when a large number of packets appear with ICMP error messages, you can configure an ICMP Smart-Rule to block that packet flood. As well as setting the threshold, you can set additional Smart-Rule refinements for the packet's destination port and message type.

To configure a Smart-Rule to protect against ICMP floods

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **ICMP** tab.
4. In the first table, click  the edit button.
5. Set the **Rule Action** for this Smart-Rule. It is triggered when the Packet Threshold or Bit Threshold is crossed.
 - **Block** – The Defense device blocks all traffic matching the rule definition
 - **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
 - **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.
6. Set the **Threshold** rate for your chosen traffic type/s (**Bit Rate**, **Packet Rate** or both). When the rate of that type of traffic (with the same destination port) goes past the Threshold, the Smart-Rule performs the associated Rule Action.

Tip: You can use one or both rates for each traffic specific setting, but in most situations packet rate is sufficient. If you don't want to use a certain type, you can set its value high so it never interacts with traffic. You can normally use a bit rate of 40,000,000,000bps and a packet rate of 40,000,000pps to accomplish this. If you use both rates, the Threshold that is reached first will trigger the Rule Action.

7. (Optional) Set the associated **Rate Limit** for this traffic type. When the Rule Action is set to Block, the Rate Limit sets how much traffic of this type is still allowed through to the internal network.
8. (Optional) If you're not using one of the available traffic types (Bit Rate or Packet Rate), you can use the drop-down to disable that Threshold and Rate Limit.
9. Click **Save**.
10. You can edit the **UDP Destination Port** table to refine the ICMP Smart-Rule by including or excluding certain ICMP packets as potential attack packets when the Defense device calculates the rate. Each packet has an original destination port (from the server sending the ICMP messages); you can choose to enable/disable the ports that count as potential attack traffic towards the ICMP Smart-Rule Threshold.

11. You can edit the **ICMP V4 Types** and **ICMP V6 Types** tables to similarly include or exclude ICMP packets as potential attack packets, by enabling or disabling ICMP types.
12. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

CLI Commands

Edit an ICMP Smart-Rule

```
configure

set policy protection-profile <ppName> smart-rule icmp icmp-from-failed-
reflectors rule-action [block|detect|disabled] [bit-rate|packet-rate] admin-
state [disabled|enabled] threshold <rate> rate-limit <rate>

edit policy protection-profile <ppName> smart-rule icmp [dest-port|v4-
type|v6-type]

Tip: When your editing the dest-port, v4-type, or v6-type tables, you can type
an existing table entry or create a new one. Then for each entry you can edit
description and port-number and choose if the entry is disabled or
enabled.

exit


commit
```

Edit the Smart-Rule Scale Percentages

Smart-Rule Scale is used in [Inspection Control override entries](#) to scale up or down the Smart-Rule Thresholds and Rate Limits depending on the traffic's destination IP address.

To edit a Smart-Rule Scale percentage

1. Use the left-hand menu to navigate to **Policy > Smart-Rules**.
2. From the **Selected Protection Profile** drop-down, choose the Protection Profile you want to edit.
3. Select the **SCALE** tab.

4. Set the following percentages:
 - **High** – Set the scaling percentage for all Inspection Control override entries set to use a **high** Smart-Rule Scale. The default is 200%.
 - **Medium** – Set the scaling percentage for all Inspection Control override entries set to use a **medium** Smart-Rule Scale. The default is 100%.
 - **Low** – Set the scaling percentage for all Inspection Control override entries set to use a **low** Smart-Rule Scale. The default is 50%.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To return to the default Threshold or Rate Limit value, delete all characters of the current value. To return to the default Rule Action, click the X in that field.

CLI Commands

Edit Smart-Rule Scale percentages

```
configure


set policy protection-profile <ppName> smart-rule scale high
<highPercentage> medium <mediumPercentage> low <lowPercentage>

commit
```

Advanced Settings

For information on the Advanced Settings available in the Policy area of the CMS, access the built in help available in the CMS Web UI.

To open the CMS built in help

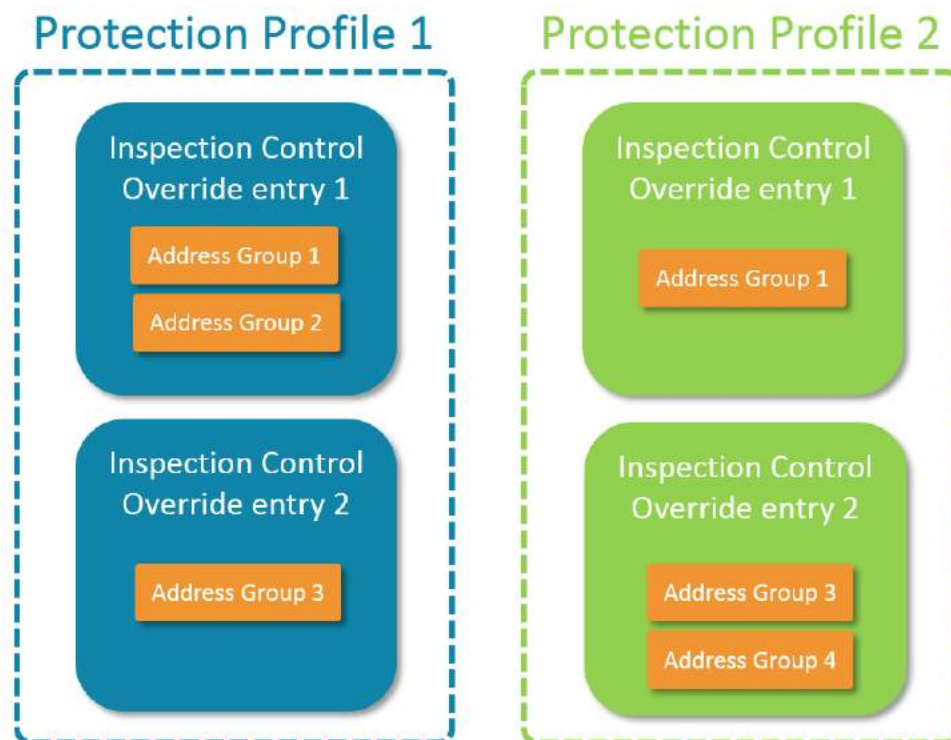
1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

Address Groups

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Address Groups Screen reference topic](#).

An Address Group is a set of related IP addresses which you can use (and reuse) in multiple Protection Profiles. In addition to its use in Protection Profiles, the Address Group associated with an IP address can be made visible as part of any Security Event or sFlow syslog messages sent to SmartWall SecureWatch Analytics (SWA). This enables you to perform searches aimed at a specific Address Group. If you associate a name with an individual IP address it can also appear in the messages.

You can create up to 128 Address Groups.



When you create an Address Group, you don't assign a purpose to the IP addresses/ranges/subnets it contains. This enables you to use them how you want within the Policy and even reuse the same group in different ways or across different Protection Profiles.

If you choose to create Address Groups of related destination IP addresses, you can use them in Inspection Control override entries in multiple Protection Profiles. You can give names to the group and the individual IP addresses/ranges/subnets, so you can quickly see which assets in your network these IP addresses represent.

Equally, you could create groups of related source IP addresses to identify trustworthy or untrustworthy customers, and use those groups, in Source Control entries, to black list or white list the source IP addresses.

You can also use Address Groups in [Flex-Rule Lookup Tables](#), to enable a Flex-Rule filter to compare the IP on an incoming packet with the list of IP addresses in the selected Address Groups.

[Learn more about using IP Address subsets in the CMS.](#)

Note: You can manually add IP addresses to an Address Group or you can import multiple addresses using a .csv file.

Syslog messages



When the CMS generates a syslog message, if the IP address in the message is contained in an Address Group, then the group name and the IP entry name (if used) can also be included in the message. This enables you to query specific Address Groups or IP entries in SmartWall SecureWatch Analytics. To include the Address Group name and IP names, you need to [enable analytics IP Reporting](#) for that group.

Creating Address Groups

Rather than managing IP addresses individually, you can group like addresses into Address Groups. For example, you may group the destination IP addresses of your assets into location based groups. You can create up to 128 Address Groups.

Tip: You can use Address Groups in Inspection Control and Source Control.


To create a new Address Group



1. Use the left-hand menu to navigate to **Policy > Address Groups**.
2. At the table, click **Add**.
3. Type a **Name** for the new Address Group. You must only use alphanumerics, spaces, or `.-&()_/@:=` symbols.
4. (Optional) Type a **Description** of this Address Group.
5. Click **Add** to add an IP address, range, or subnet to the group. Type an **IP** address, range (e.g. `10.10.10.0-10.10.10.100`) or subnet (e.g. `10.10.10.0/24`) and, optionally, a **Name** (which will appear in syslog messages with the Address Group name). Then click **Save**.
6. You can use a single IP address/range/subnet, or you can continue to add them to the Address Group in the same way. You can also use  the delete button to modify your group.
7. When you're happy with the group, click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click  **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Caution: The same IP address cannot exist in more than one Address Group which is used for [IP Reporting](#). If you add an IP address which already exists in another group, you won't be warned at this stage.

To import an Address Group

Tip: [Learn more about importing and exporting Address Groups.](#)

1. Use the left-hand menu to navigate to **Policy > Address Groups**.
2. At the table, click **Import**.
3. Locate and select the .csv file and click **Open**.
4. (Optional) Edit the **Name** for the new Address Group.
5. (Optional) Type a **Description** of this Address Group.
6. Click **Save**.
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: From the Address Groups table, you can edit  or delete  existing Address Groups.

CLI Commands

Create a new Address Group

```
configure
set policy address-group <agName> description "<description>" ip <ipAddress>
name <ipName>
commit
```

Import an Address Group

```
configure
request policy import address-group name <agName> description
"<description>" remote-uri <remoteUri> remote-password <remotePassword>
commit
```

Edit an existing Address Group

```
configure
edit policy address-group <agName>
```

Tip: Use the `set` command to edit the `description`, or add a new `ip` (and optionally a `name`). Use the `delete` command to remove an existing `ip`.

```
commit
```

```
exit
```

Rename an Address Group

```
configure
```

```
edit policy address-group <agName> rename name <newName>
```

```
commit
```

Delete Address Group

```
configure
```

```
edit policy address-group
```

```
delete <agName>
```



Note: You can only delete an Address Group if it isn't referenced by an attack mitigation feature (i.e. Source Control or Inspection Control).

Exporting and Importing Address Groups

As well as importing a .csv file to create a new Address group you can use them to edit existing groups. You can export address groups to store externally, edit externally, or import into another CMS.

Caution: The same IP address cannot exist in more than one Address Group which is used for [IP reporting](#). If you import an IP address which already exists in another group, you won't be warned at this stage.


To add multiple IP addresses to an existing group

1. Use the left-hand menu to navigate to **Policy > Address Groups**.
2. At the table, locate the Address Group you want to edit and click  the edit button.
3. Click **Import**.
4. Locate and select the .csv file and click **Open**.
5. Select a **Method**:
 - **Merge** – Keep all existing IP addresses in this group and add any new ones from the .csv file
 - **Replace** – Delete all existing IP addresses in this group and replace with the list of IP addresses in this .csv file
6. Click **Import**.
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

```
configure
request policy address-group <agName> import method [merge|replace] remote-
uri <remoteUri> remote-password <remotePassword>
commit
```

To export an Address Group as a .csv file

1. Use the left-hand menu to navigate to **Policy > Address Groups**.
2. At the table, locate the Address Group you want to export and click  the export button.
3. The addresses and their names will be downloaded as a .csv file in your browser

CLI Commands

```
request policy address-group <agName> export remote-uri <remoteUri> remote-
password <remotePassword>
```

To format a .csv file for import

If you want to create a .csv file containing a list of IP addresses, or want to export it from another system, it must be formatted in the following way:

```
"address1", "name1"
"address2",
"address3", "name3"
"address4", "name4"
```

You must:

- Use a new line for each entry.
- Surround each address in quotes and surround each name in quotes.
- Not have any whitespaces around the comma.
- Include a comma after an address, even if you don't want to provide a name for it. No name can be represented by empty quotes or by nothing.
- Not have any empty lines.
- Save the file with a .csv extension.

Example in text editor

```
"1.1.1.1", ""
"2.2.2.2-2.2.2.19", "name2"
"3.3.3.0/24", "name3"
```

Example in Excel

If you are creating the .csv file in excel, you do not need to use quotes or commas. Put all addresses in column A and their corresponding names in column B. Then save the file as a .csv file.

	A	B	C	D
1	1.1.1.1			
2	2.2.2.2-2.2.2.19	name2		
3	3.3.3.0/24	name3		
4				
5				
6				
7				


Enabling IP Reporting for an Address Group

You can configure the CMS to send Address Group and IP address names in event syslog messages. This can enable you more easily search and identify trends in the analytics application. You must enable this feature for each Address Group.

Caution: The same IP address cannot exist in more than one Address Group which is used for IP reporting.

To enable an Address Group for Analytics IP Reporting

1. Use the left-hand menu to navigate to **System > Analytics & Syslog**.
2. Select the **IP REPORTING** tab.
3. Click **Add**.
4. Select an **Address Group**.
5. Click **Save**.
6. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the table, you can use  the delete button to disable IP reporting for an Address Group.

CLI Commands

Enable IP reporting for an Address Group

```
configure
set analytics ip-reporting group2 <agName>
commit
```

Disable IP reporting for an Address Group

```
configure
delete analytics ip-reporting group2 <agName>
commit
```


SECTION 3

Manage Network

The CMS defines the attack mitigation Policy for each Defense device and enables you to push updates and changes to those devices without having to touch the device itself. The CMS also manages the connected Defense devices.

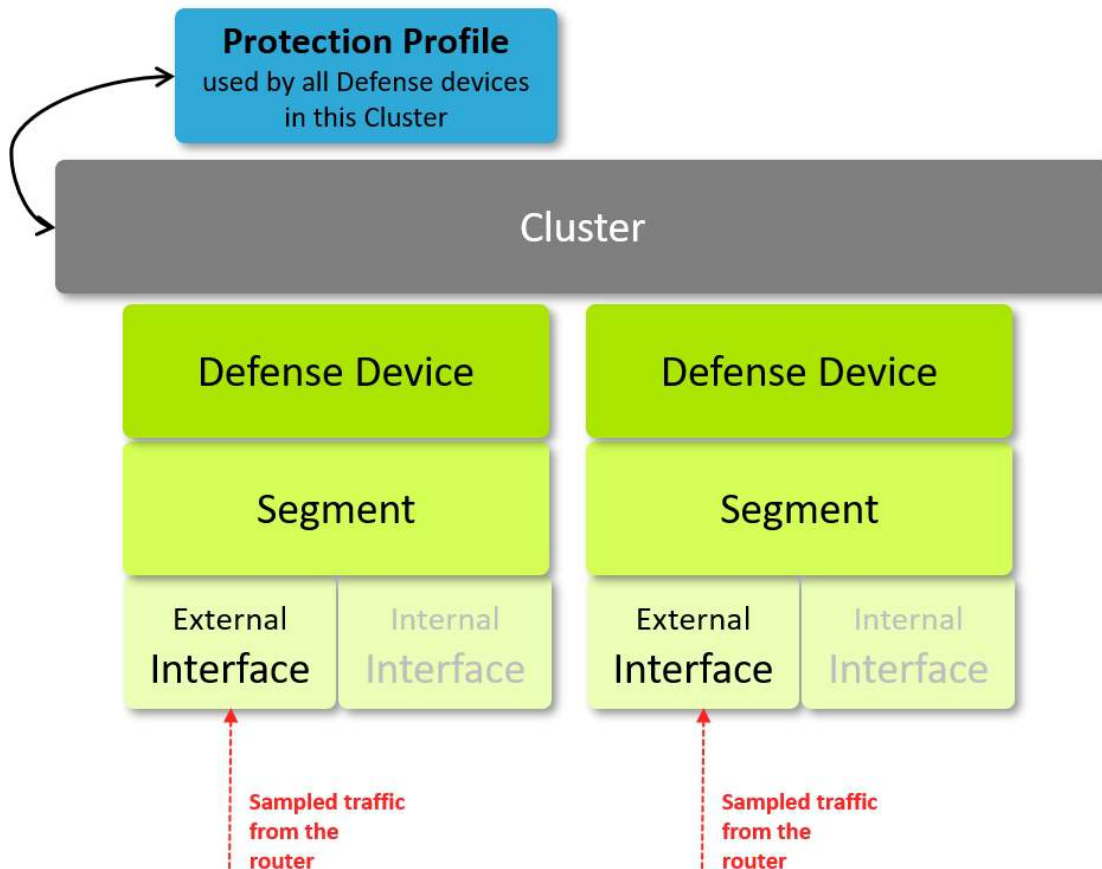
This section discusses the following:

SmartWall Network	97
Clusters	99
Deployment Options and Clusters	100
Analytics reporting per cluster	101
Managing Clusters	101
Devices	105
Clusters	105
Authentication Groups	105

SNMP	106
Viewing Device Status	107
Adding a Device to the CMS	112
Managing Authentication Groups	113
Changing Device Credentials	116
Enabling SNMP for a Defense device	116
Disabling an Interface	117
Upgrading a Device's Software	118
Changing a Device's IP Address	120
Syncing a Device	121
Rebooting a Device	123
Redeploying a Device	123
Segments	125
Link State Propagation	125
Analytics reporting per Segment	126
Viewing Segment Status	126
Configuring a Segment	126
Connecting a Bypass Device to a Segment	128
Enabling Link State Propagation	128
Operating Modes	130
To open the CMS built in help	130

SmartWall Network

Your SmartWall Threat Defense Director (SmartWall TDD) is made up of a SmartWall Central Management Server (CMS), a SmartWall SecureWatch Analytics (SWA) application and multiple Defense devices. You can manage these devices using the CMS.



Protection Profiles

A Protection Profile is a container for a configuration of the attack mitigation features (Policy) in the CMS. When you associate a Protection Profile with a Cluster, it provides the Defense devices in that Cluster with the Policy for handling incoming traffic. You can create one Protection Profile for your network or multiple Protection Profiles each containing a different Policy.

Clusters

A Cluster is a set of identically configured Defense devices. When you create a new Cluster you must associate it with a Protection Profile; which controls how the devices in that Cluster respond to traffic. A single CMS can control up to 16 Clusters.

Devices

There are two types of devices in the SmartWall TDD system:

- **Defense devices** – This is broader term for the vNTDs (SmartWall Network Threat Defense Virtual Edition devices) which are used purely as Detection Engines in a SmartWall TDD deployment.
- **Remote Devices** – This is a broader term for the Juniper Networks MX Series router used to mitigate DDoS attack traffic. These are managed in the SWA and will not appear in the CMS.

Segments

A Segment is a linked external and internal network interface defined from a front-panel port pair on a Defense device. The first time you connect a device to the SmartWall Central Management Server (CMS), it identifies the available interfaces and records them as Segments.

Interfaces

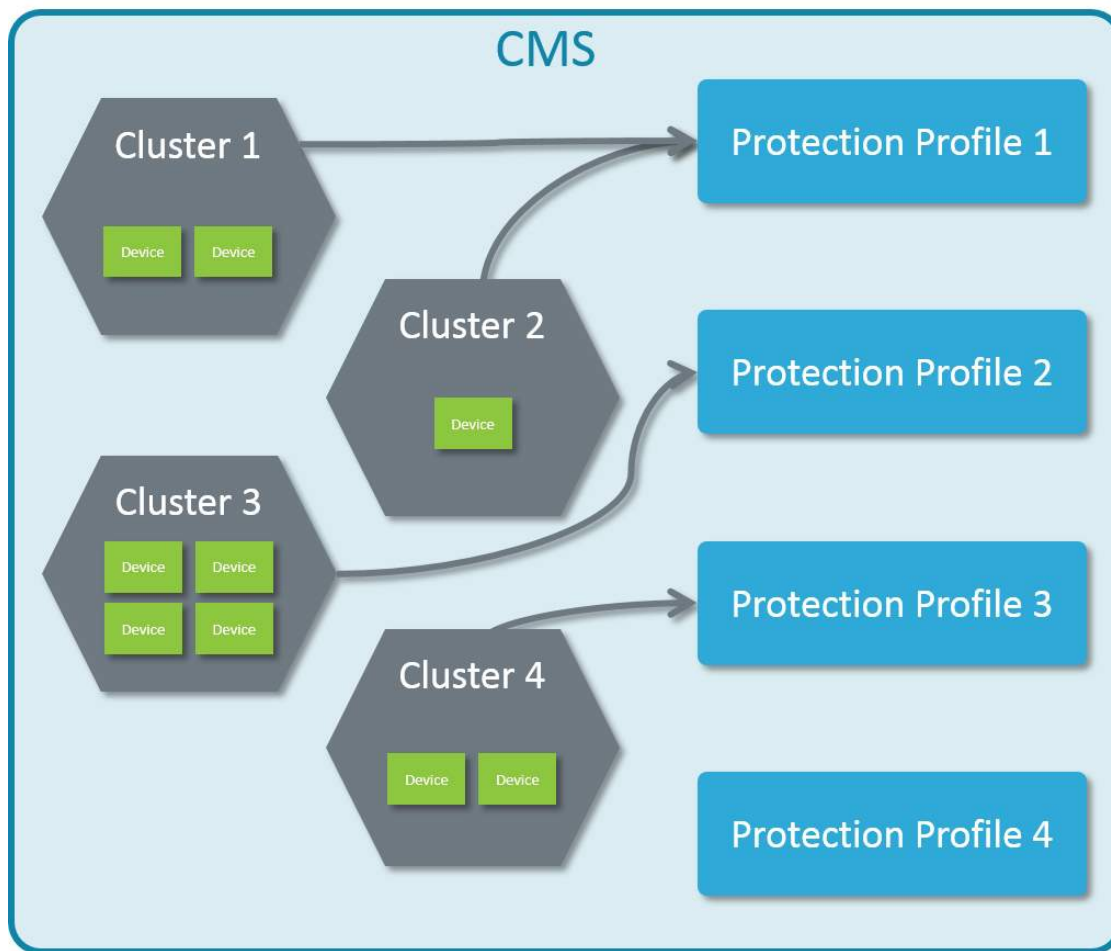
Interfaces are the physical ports on a device where traffic passes into and out of the device.

Each default segment is made of two interfaces so, for a Segment on a Defense device, you will see data for two interfaces per segment.

Clusters

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Clusters Screen reference topic](#).

A Cluster is a set of identically configured Defense devices. When you create a new Cluster, you must associate it with a Protection Profile; this Protection Profile contains a Policy which controls how the devices in that Cluster respond to traffic. A single SmartWall Central Management Server (CMS) can control up to 16 Clusters. After installation, the CMS initially has a single default Cluster which is associated with the default Protection Profile and default Authentication Group.



How you choose to group your Defense devices depends on your deployment:

- If you want to use multiple Protection Profiles (to have some Defense devices treat traffic differently to others), you need to have a new Cluster for each Protection Profile you want to use.

- If you want to use a single Protection Profile for all your Defense devices, you may choose to have a single Cluster. However multiple Clusters can use the same Protection Profile, so you could continue to use a single Protection Profile while you group your devices into logical arrangements, such as by location or link type. Having devices grouped in that way can improve the usefulness of SmartWall SecureWatch Analytics because every syslog message sent from the CMS contains a Cluster name. You could use this to view more specific queries on a specific group of Defense devices, such as reports on all the devices in a single location.
- Or you may choose a mixture of both, using multiple Protection Profiles where each has multiple Clusters. However, a Cluster can only be associated with one Protection Profile at a time. For example, if you want to separate your Defense devices by their locations in your New York and Boston data centers but you have two Protection Profiles which you use in both locations, you would need to have four clusters: "Protection Profile 1 (New York)", "Protection Profile 1 (Boston)", "Protection Profile 2 (New York)", and "Protection Profile 2 (Boston)".

Note: You cannot add a [Bypass device](#) to a Cluster. To associate a Bypass device with a Defense device, you must assign the Bypass device to the [Segment](#) it is physically connected to.

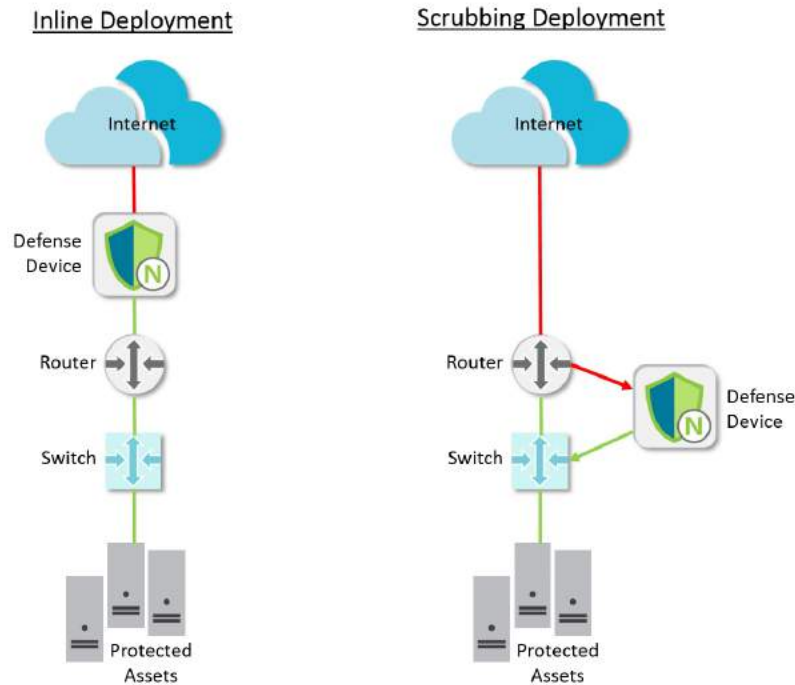
A Defense device can only belong to one Cluster at a time. If you want to move a Defense device to a new Cluster, you must first remove it from the current Cluster before you can add it to the new one.

Until you add a new Defense device to a Cluster, it can only work in pass-through mode (sending all traffic on to the internal network without inspecting or blocking). When you remove an existing Defense device from a Cluster, it retains the last Policy it synced from the CMS. It will continue to mitigate traffic in that way until you add it to a new Cluster. Once you add it to a new Cluster, the Policy associated with that new Cluster will overwrite the device's stored Policy.

Deployment Options and Clusters

There are multiple ways to deploy your Defense devices to provide the best DDoS mitigation for your network. The two most common are:

- **Inline DDoS Mitigation** – The Defense devices are deployed physically inline on the incoming fiber connection, in front of your edge router.
- **Scrubbing DDoS Mitigation** – Traffic requiring DDoS protection is logically rerouted by your router through the Defense devices.



When you use Inline DDoS Mitigation, the Defense devices must be placed before the edge router in your network. However, if you use Scrubbing DDoS Mitigation, the Defense devices can be deployed in various locations within your network.

Analytics reporting per cluster

The syslog messages sent from the CMS to SmartWall SecureWatch Analytics contain Cluster names. This enables you to aggregate device information for all devices in a Cluster and view reports on the group. For multiple Clusters, this enables you create more specific reports on your device groups. For Clusters that use different Protection Profiles, this enables you to more clearly see which Protection Profile might need tuning.

Managing Clusters

TDD Deployments: For Clusters of TDD vNTDs, you must set the **Ingress Sample Rate** to the same value as the Port-Mirroring Sample rate on the routers those vNTDs are connected to. If you have more than one Port-Mirroring Sample rate on your routers, you will need a Cluster of vNTDs configured for each rate.




If you want to use multiple Protection Profiles (to have some Defense devices treat traffic differently to others), you need to have a new Cluster for each Protection Profile you want to use. Alternatively, you may want to use the same Protection Profile for all devices but separate them into Clusters for more easily searchable analytics.



Caution: The more Clusters you use, the more copies of the Protection Profile must be sent down to the Defense devices. This can increase your device syncing time.

Prerequisites

You must have at least one [Protection Profile](#) and one [Authentication Group](#) before you can create a Cluster. When you first install the CMS you have a default Protection Profile and a default Authentication Group.



To create a new Cluster


1. Use the left-hand menu to navigate to **Network > Clusters**.
2. At the table, click **Add**.
3. Type a **Name** for Cluster. You must only use alphanumeric, spaces, or `.-&()/_/@:=` symbols.
4. (Optional) Type a **Description**.
5. (Optional) If the devices are part of a TDD deployment you will need to set an **Ingress Sample Rate**. Otherwise leave it at the default value of 1.
6. Select the **Protection Profile** you want the devices in this Cluster to use.
7. In the **Available Devices** box, check the box next to the devices you want to add to the new Cluster and click  the right arrow. You can remove devices by selecting them in the **Devices in Cluster** box and using  the left arrow.
8. Click **OK**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click  **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).


Tip: On the Clusters table, you can use the following action buttons to edit  or delete  a Cluster.

To add a Defense device to a Cluster

Note: You cannot add a Bypass device to a Cluster. You must [associate a Bypass device with the Segment](#) on the Defense device it is physically connected to. The Bypass device will then inherit the Cluster of that Defense device.

1. Use the left-hand menu to navigate to **Network > Clusters**.
2. From the table, locate the Cluster you want to add the device to, and click  the edit button. You can type a text string into the Search field to narrow down the list.
3. In the **Available Devices** box, check the box next to the device you want to add to the new Cluster and click  the right arrow.

4. Click **OK**.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To remove a device from a Cluster, follow the same process but use  the left arrow to remove the device. When you remove a Defense device from a Cluster, it will have the deployment state **not-in-cluster** and will retain its last Policy configuration. If you add the device to a new Cluster, the Policy associated with the new Cluster overrides the device's previous Policy.

CLI Commands

Create a new Cluster

```
configure

set clusters cluster <clusterName> description "<description of cluster>"
protection-profile <ppName> device <deviceName>

commit
```

Edit an existing Cluster

```
configure

edit clusters cluster <clusterName>

set protection-profile <ppName> description "<descriptionText>"

commit

exit
```

Rename a Cluster

```
configure

request clusters cluster <clusterName> rename name <newName>

commit
```

Add a Defense device to a Cluster

```
configure

set clusters cluster <clusterName> device <deviceName>

commit
```

Remove a Defense device from a Cluster

```
configure

delete clusters cluster <clusterName> device <deviceName>
```


```
commit
```

Delete a Cluster

```
configure
edit clusters
delete cluster <clusterName>
commit
exit
```

Troubleshooting

The Defense devices in this Cluster aren't handling traffic as I expected

Check the Cluster has the correct Protection Profile associated with it. That Protection Profile is what the Defense devices in this Cluster use to define how they handle incoming traffic. Locate the Cluster in the table and click  the edit button.

If the Protection Profile is correct, check there are no Operating Mode overrides on this Cluster or its devices: **Network > Operating Modes**.

Devices

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Devices Screen reference topic](#).

The CMS manages your Defense devices, which are virtual Network Threat Defense devices (vNTDs). These devices act as Detection Engines and detect DDoS attack traffic in mirrored samples sent from the edge routers.

While the SmartWall TDD only uses vNTDs, in the user interface and documentation you should be aware that device can refer to any of the Defense devices compatible with the SmartWall TDS system (virtual or physical) or a Bypass Device.

Note: The SmartWall TDD system also includes Remote Devices (which are your edge routers). These are managed by the SWA and are not part of the devices managed by the CMS. See the **SmartWall TDD User Guide** for more information.

Clusters

When you physically add a new Defense device to your network, you need to also add it to the CMS before it can begin to mitigate attacks. When you add a new Defense device to the CMS, you must also assign it to a [Cluster](#). The Cluster is associated with a [Protection Profile](#) which contains the Policy that your new device will use to identify good and bad traffic.

When you add a new external Bypass device to the CMS, you do not need to add it to a Cluster, but you must assign it to the Segment on the Defense device it is physically connected to.

Authentication Groups

An Authentication Group manages the authentication credentials which the SmartWall Central Management Server (CMS) uses to connect with the SmartWall devices. All devices must be associated with an [Authentication Group](#) containing the correct access credentials for that device, to enable the CMS to communicate with the device.

Default Authentication Group

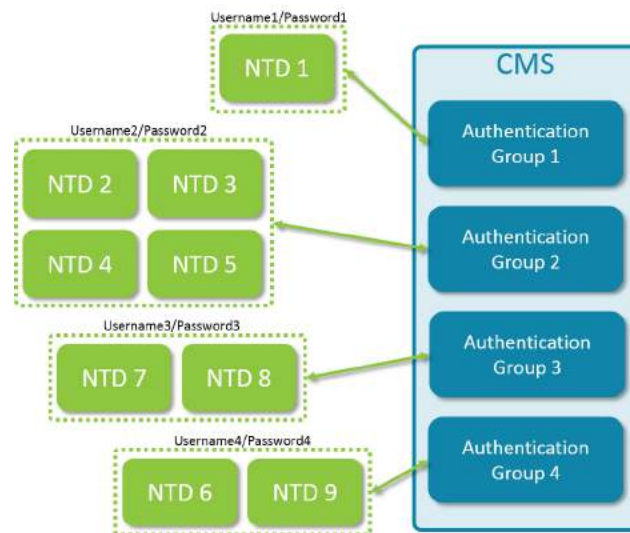
When you first deploy a SmartWall device, it has a default username and password associated with it (admin/smartwall). When you first deploy the CMS, it uses the default Authentication Group to connect with the new devices.

When you change the username and password on your devices to one specific to your organization, you must either update the default Authentication Group to match or create a new Authentication Group with the updated credentials.

Note: If your CMS authentication credentials do not match the expected credentials on a device, the Deployment State will appear as **authentication-failed** and you can't change any device configurations until you fix the authentication.

Using multiple Authentication Groups

Depending on your organization's security policy, all your devices may use the same username/password, or your devices may need to have a range of authentication credentials. If you have devices with different credentials in your network, you must create an Authentication Group for each set of credentials, then add the devices using those credentials to the relevant groups. This way the CMS knows which username/password to send to which device.





SNMP

You can use the CMS SNMP (Simple Network Management Protocol) to collect information and view alerts from your SmartWall devices, using your own network management system.

You can [enable basic SNMPv2c for the Defense device](#). This allows you to query basic network layer information from the [IF MIB](#). You can download the MIB files from the support portal.

Viewing Device Status

If you see a device status alert on the Status bar (when  the in-sync or  the reachable icon turns orange) or want to view information about your devices, you can view that information on the Devices screen and the Home screen.

To view the status of a device

1. Use the left-hand menu to navigate to **Network > Devices**.
2. At the table, you can see the current status of all your connected devices.
3. (Optional) Type a text string into the Search field to narrow down the list of devices. For example, you could search for all devices in a specific Cluster, or of a specific device type, or in a particular defense mode etc.

Corresponding CLI commands

```
show devices device status
```

Reading the Devices table

The Devices table shows the current status of every device connected to your CMS. For each device you can see its basic information (**Name**, **Cluster**, **deviceType**, **Bypass Mode**, **Defense Mode**, **IP Address**, **Uptime** since last restart, and **Software Version**) and the current state of the device in three columns: **Deployment State**, **Deployment Action**, and **Status**.

Caution: The Devices table is updated every 10 seconds, so the state may be up to 10 seconds old. If a device quickly changes state and returns within that 10 second window, you won't see the change.

Deployment State

This column shows the current state of the device. It can display the following:

- **in-sync** – The device is connected and its configuration matches the current configuration stored in the CMS for this device.
- **sync-required** – The device is connected but its configuration does not match the current configuration stored in the CMS for this device. The device could have become out of sync if it was unavailable when a change was committed in the CMS or if you have replaced a connected device with a new version (with the same IP address). Use the **Sync** option to push the Policy changes to the device.

- **force-sync-required** – The device is connected but there has been an unexpected error in the configuration. Use the **Force sync** option to wipe the old configuration from the device and replace it with the current version stored in the CMS.
- **unexpected-device-type** – The selected device type does not match the information on the actual device when queried. Edit the device and give it the correct Device Type. If you have added a remote device to the devices table, it will appear as an unexpected device. You must delete it and add it to the Remote Devices screen in the SWA.
- **not-in-cluster** – (Defense device only) The Defense device is connected but it is not in a Cluster so has no Policy associated with it. Add the device to an existing Cluster or create a new Cluster for it.
- **initial-sync-pending** – The device is connected but it is new and the CMS has not yet sent its configuration. Alternatively, an unlicensed device has just been given a license.
- **deploy-pending** – The device is connected but is waiting for the CMS to complete a configuration deployment. If the deployment is successful the state will change to in-sync.
- **unsupported-version** – The device is connected but the software version on the device is not compatible with this version of the CMS.
- **invalid-modules-detected** – The Defense device contains an unsupported module configuration. Physically correct the modules, then redeploy the device.
- **unknown** – The CMS has not yet attempted a connection to a new device or is unable to report the state for another reason.
- **no-connection** – (Connection State) The CMS is unable to connect to the device or discover the device model.
- **connection-refused** – (Connection State) The CMS successfully sent a request to the device but the device refused to send a response. Check you have the correct IP address for the device in the Devices table, and check that there isn't a firewall blocking the connection.
- **connection-timed-out** – (Connection State) The CMS attempted a connection but the attempt timed out. Check you have the correct IP address for the device in the Devices table, and check that there isn't a firewall blocking the connection.
- **authentication-failed** – (Connection State) The CMS attempted a connection but the authentication credentials on the CMS did not match the credentials on the device. Check that the device is in the correct Authentication Group in the CMS and that the credentials associated with that group are correct.

Note: In the CLI there are two columns for this information: **Connection State** and **Deployment State**. Connection State covers the six connection states and, when the device is **Connected**, Deployment State shows whether the device is **In sync**, **Sync**

required, Force sync required, Not in cluster, Initial sync pending, or Deploy pending.

Deployment Action



This column shows if the device is currently performing an action. It can display the following:



- **none** – The device is not performing any deployment action
- **deploy-in-progress** – The device is currently being deployed.
- **upgrade-in-progress** – The device is currently being upgraded by the CMS
- **commit-in-progress** – The device is currently receiving a committed configuration change from the CMS
- **sync-to-in-progress** – The device is currently syncing with the CMS
- **force-sync-in-progress** – The device is currently being force synced by the CMS

Note: You can use the **Reboot** option, on the Devices table, to restart a device. If you commit any changes in the CMS while the device is restarting, you may have to **Sync** the device when it comes back online.

Status

This column shows whether traffic is running to the device as normal or if there is currently a problem with the device which may affect traffic or its connection to the CMS. The Status field can display either **normal** or it can show one or more of the other states:

- **normal** – Traffic is running normally.
- **not-in-sync** – The device is not currently in sync. This could be for a number of reasons. Check the Deployment State to see if an action is required.
- **not-in-cluster** – (Defense device only) The Defense device is not in a Cluster. Go to **Network > Clusters** and edit a Cluster to include this device.
- **not-licensed** – (vNTD only) The vNTD does not currently have a license associated with it. If you have available license capacity, click  and select **License**. If you need additional license capacity, contact your Corero representative.
- **connection-issue** – This device is experiencing a connection issue. See the Deployment State column for the specific connection issue (i.e. no-connection, connection-refused, connection-timed-out, authentication-failed, unsupported-version, or unknown)
- **authentication-failed** – The CMS does not have the right authentication credentials for this device. Click  to check the device is in the correct Authentication Group.

- **device-unreachable** – The device cannot be reached at all. Check the device has the correct IP and all physical connections are working as expected.
- **link-down** – A link on this device is currently down. This status appears even if the link is brought down due to Link State Propagation.
- **uncleared-alarms** – There are one or more uncleared alarms associated with this device. Click  the Alarm icon in the status bar to see the list of alarms.
- **heartbeat-failed** – (Defense device Only) The Bypass device, associated with this Defense device, has been unable to reach the Defense device and if it was in Automatic mode has now started bypassing the Defense device and sending traffic directly to the internal network.
- **Invalid-modules-detected** – The Defense device contains an unsupported module configuration. Physically correct the modules, then redeploy the device.
- **unexpected-device-type** – The device has the wrong device type selected (e.g. it is a Bypass device but has defense type selected). Click  to change the device type.
- **unsupported-version** – The software version on this device is incompatible with the software currently on the CMS. You need to upgrade the device software to a supported version.
- **no-sflow** – CMS is not currently receiving sFlow samples from the device.
- **no-syslog** – CMS is not currently receiving syslog messages from the device.

Note: When a Defense device is showing heartbeat-failed, the associated Bypass device will most likely be showing as normal. This is because the Bypass device is behaving as expected in this situation and only the Defense device has an issue.

For more information about this table, see the [Devices Screen reference](#).

To view the current status of an interface on a device

Each Segment on a device is made of two interfaces; one internal and one external. You can check the status of a device's interfaces using CMS.

1. Use the left-hand menu to navigate to **Network > Devices**.
2. Click the **INTERFACES** tab.
3. From the **Device(s)** drop-down, choose the device where this interface is located.
4. From the **View** drop-down, select **Summary**, **Packet Statistics**, or **Diagnostics**.
5. In the table you can see the selected information on the selected device.

Corresponding CLI commands

```
show devices device <deviceName> interfaces interface <interfaceName>
commit
```

Resetting interface counters

Caution: Resetting counters can affect your analytics information in SWA and should only be done when recommended by Corero Customer Support.

To investigate packet or byte counts, you can reset interface counters to measure inbound and outbound packets/bytes over any period of time you require.

Reset counters for all interfaces shown


1. Use the left-hand menu to navigate to **Network > Devices**.
2. Click the **INTERFACES** tab.
3. From the **Device(s)** drop-down, choose the device or devices you want to reset counters on.
4. From the **View** drop-down, select **Packet Statistics**.
5. The table should now display the current counters for all selected devices.
6. To reset all displayed counters in the table, click **Reset All Counters**.
7. Click **OK** to confirm.

Corresponding CLI commands

Caution: The CLI command resets the interfaces for all devices connected to the CMS. There is no way to select a subset of devices like there is in the GUI.

```
request devices device <deviceName> interfaces reset interface-counters
commit
```

Reset counters for a single interface

1. Use the left-hand menu to navigate to **Network > Devices**.
2. Click the **INTERFACES** tab.
3. From the **Device(s)** drop-down, choose the device where this interface is located.
4. From the **View** drop-down, select **Packet Statistics**.
5. From the table, locate the interface you want to reset counters for and click  the reset button.
6. Click **OK** to confirm.


Corresponding CLI commands



```
request devices device <deviceName> interfaces interface <interfaceName>
reset interface-counters
commit
```

Adding a Device to the CMS

Once you physically install a new device, you need to connect it to a CMS.

To add a device to the CMS

1. Use the left-hand menu to navigate to **Network > Devices**.
2. At the table, click **Add**.
3. Type a **Name** for this device. You must only use alphanumeric, spaces, or .-&()/_@:= symbols.
4. (Optional) Type a **Description** of the device.
5. Type the IP **Address** (IPv4) of the device (you will have set this up when you installed the device. See the **Getting Started Guide** for more information)
6. For Defense devices, select the **Cluster** you want to add this device to. The device's defense Policy is determined by the Protection Profile associated with the Cluster.
7. (Optional) If your device does not use the credentials in the Default Authentication Group, from the **Authentication Group** drop-down, select the Authentication Group which corresponds to the authentication credentials on this device.
8. Click **OK**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Devices table, you can use the following action buttons to edit  or remove  a device.

CLI Commands

Add a device to the CMS

```
configure

set devices device <deviceName> description "<Description Text>" address
<ipAddress> authgroup <authName>

set clusters cluster <clusterName> device <deviceName>

commit
```

Edit a device

```
configure

edit devices device <deviceName>

set address <ipAddress>
```



```
set authgroup <groupName>
set description "<description>"
commit
exit
```

Note: Changing a device's IP address in the CMS only changes the IP address the CMS uses to locate the device. If you want to give the device a new IP address, you must [access the device's pCLI on the console port](#).

Remove a device from the CMS

```
configure
edit devices device
delete <deviceName>
commit
exit
```

Troubleshooting

New vNTD device showing as not-licensed

If the device is a SmartWall Network Threat Defense Virtual Edition (vNTD), you must have at least 10Gbps available license capacity for the device to automatically license and connect to the CMS. If you don't, you will have to create some space by delicensing an old vNTD or buying additional license capacity from your Corero representative. You can then [license the device](#) manually.


Next steps



- For a Defense device:
 - [Disable unused interfaces](#)
 - NTD1100 Only: [Set ethernet mode for interfaces](#)
 - Split-fiber deployments: [Disable Link State Propagation for Segments](#)
- For a Bypass device:
 - [Connect a Bypass device to a Segment](#)

Managing Authentication Groups

Unless all your devices use the same credentials, you will need to create additional Authentication Groups to connect them to the CMS.



To create an Authentication Group

1. Use the left-hand menu to navigate to **Network > Devices**.
2. Click the **AUTHENTICATION GROUPS** tab.
3. At the table, click **Add**.
4. Type a **Name** for the group. You must only use alphanumerics, spaces, or .-&()/_/@:= symbols.
5. Type the **Device Username**.
6. Select from the following verification options:
 - **SSH Key** – Not available for physical devices. For vNTD's only, use the drop-down to select the private key from the [SSH Keys](#) table that corresponds to the devices public key
 - **Device Password/Confirm Password** – Enter the Password for this device's administrator credentials
7. Click **OK**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Authentication Groups table, you can use the following action buttons to edit  or remove  Authentication Groups.

To change a device's Authentication Group

If you edit a device's credentials in the device pCLI, you will either need to [create a new Authentication Group](#) for this device or move the device into an existing Authentication Group which has those credentials already.

1. Use the left-hand menu to navigate to **Network > Devices**.
2. From the table, locate the device you want to edit and click the  edit button. You can type a text string into the Search field to narrow down the list.
3. From the **Authentication Group** drop-down, select the new group.
4. Click **OK**.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

Create a new Authentication Group
configure

```
set devices authgroups <authName> group <groupName> default-map remote-name
<username> remote-password <password>

commit
```

Tip: If you're using the Public Key authentication option, after `default-map` use the command `public-key private-key name <keyName>`.

Edit an Authentication Group

```
configure

edit devices authgroups <authName>
```

Tip: Use the `set default-map` command to edit the `remote-name` and `remote-password` or the `public-key`.

```
commit

exit
```

Rename an Authentication Group

```
configure

request devices authgroups group <authName> rename name <newName>

commit
```

Delete an Authentication Group

```
configure

edit devices authgroups

delete group <authName>

commit

exit
```

Change a device's Authentication Group

```
configure

edit devices device <deviceName>

set authgroup <authName>

commit

exit
```

Changing Device Credentials

In the CMS, you can only change the credentials that the CMS uses to connect to a device. To change the device's authentication credentials, you need to access it through the device console, and use the pCLI.

To change a Defense device's credentials


1. Connect to the device's console. For physical devices, you can connect using the device's IP address to SSH through an SSH client (e.g. `ssh -p 2222 admin@10.10.100.100`):
 - For **NTD1100** or **NTD280**, ssh on port 2222
 - For **NTD120** or **Bypass device**, ssh on port 22
 - For **vNTD**, you can ssh on port 2222 or open a console window for the VM in vsphere
2. Log in to the pCLI (using the same authentication credentials stored in the CMS for this device)
3. Type the following command: `setup aaa`
4. Follow the instructions to setup the new username and password.
5. When complete, return to the CMS.
6. If you already have an Authentication Group using the device's new credentials, skip this step. Otherwise, navigate to **Network > Authentication Groups** and [create a new Authentication Group](#) for the new device credentials.
7. Navigate to **Network > Devices**. The device will show a Deployment State of **sync-required**; this is expected.
8. [Change the device's Authentication Group](#).
9. [Sync the device](#). The device should now show a Deployment State of **in-sync**.


Enabling SNMP for a Defense device

By default, SNMPv2c is disabled for all new Defense devices. You can choose to enable SNMPv2c for your Defense devices.

Note: This feature is not available for NTD120 or Bypass device.

To enable SNMPv2c for a Defense device

1. In the CMS, use the left-hand menu to navigate to **Network > Devices**.
2. Select the **SNMP** tab.
3. From the table, locate the device you want to enable SNMP for and click  the edit button. You can type a text string into the Search field to narrow down the list.
4. At the **Admin State** drop-down, select **enabled**.
5. The default UDP port is 161. To change this, type a new port number in the **UDP Port** field.
6. The default community string is `smartwall`. To change this, type a new string in the **Community** field.
7. (Optional) Add a **System Location**. This can be any text string, for example, the city you're located in, or a building name.



8. (Optional) Add a **System Contact** email address. This should be someone able to manage the CMS SNMP settings.
9. Click **Save**.
10. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Disabling an Interface

By default, all Defense device interfaces are enabled. If you're not planning to connect an interface to your network, you can disable it, so it doesn't affect your traffic statistics, or generate alarms. If you later choose to use this interface, you can enable it using the same method.

To enable/disable a Defense device interface

Caution: When Link State Propagation (LSP) is enabled, you cannot disable an interface. You must [disable LSP for this Segment](#) before you can continue.

1. Use the left-hand menu to navigate to **Network > Devices**.
2. Click the **INTERFACES** tab.
3. From the **Device(s)** drop-down, choose the device where this interface is located.
4. From the **View** drop-down, make sure **Summary** is selected.
5. From the table, locate the interface you want to edit, click  the edit button. You can type a text string into the Search field to narrow down the list.
6. Choose to **Enable** or **Disable** this interface.
7. Click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

```
configure
set devices device <deviceName> interfaces interface <interfaceName> admin-
state [disabled|enabled]
commit
```

Upgrading a Device's Software

Caution: Device will restart during the upgrade process.

Once you upgrade the CMS version, you may also need to upgrade the software on your devices. You can manage this process entirely through the CMS. You must first import a device software package to the CMS, then you can push the upgrade software to your devices one at a time.

During the upgrade, the device will lose contact with the system while it restarts. You can monitor the progress of the upgrade from the Devices table. After the device has restarted, the CMS automatically updates any Policy associated with that device.

Device software packages

When you upload a file to the Software Packages table, the CMS first checks to make sure it is for a supported device type and a supported software version for your system. If it passes those checks, the file is added to the list and stored in the CMS. You can view the list of available software packages and how many devices are running each software version.

Before the CMS uses a device software package to upgrade a device, it checks that the software in the package is compatible with the selected device. It also checks that the device is currently running an older version of the software. If it passes these checks, the software package is sent to the device and the upgrade begins.

Tip: If you need to send software of the same version or earlier to a device, you can **force** the "upgrade" but you can never send an incompatible file.

Prerequisites

- [Upgrade the CMS](#) to the required software version


Caution: Do not upgrade a device without first upgrading the CMS to that version. If you do not first upgrade the CMS, you will not be able to reach your upgraded device from the CMS.

- Recommended: As the device may be down for a couple of minutes during upgrade, you should re-route the traffic to take the device out of line of active network traffic.

To upload a new software package

1. Use the left-hand menu to navigate to **System > Software Upgrade**.
2. Select the **DEVICES** tab.
3. Click **Upload**.
4. Select a device upgrade package and click **Open**.

To upgrade the software on a device

1. Use the left-hand menu to navigate to **System > Software Upgrade**.
2. Select the **DEVICES** tab.
3. In the Devices table, locate the device you want to upgrade and click  the upgrade button.
4. From the **Package version** drop-down, select the software version you want to upgrade this device to.
5. Click **Upgrade**.
6. Click **OK**.
7. To monitor the upgrade navigate to the **Home** screen:
 - On the **Devices** table:
 - The **Deployment Action** goes from **none** > **upgrade-in-progress** > **none**
 - The **Status** goes through the following transition: **normal** > **uncleared-alarms** > **connection-issue, no-sflow, no-syslog, unclear-alarms** > **uncleared-alarms** > **normal**
 - On the **Segments** table, you will see the **External** and **Internal** interfaces go from **Up** > **Unknown** > **Up**
 - During the upgrade, in the Status panel you will see **Errors detected** for the Device status and **Warnings detected** for the Network status
8. Repeat for each device you need to upgrade.

Tip: You can also locate a package version from the Software Packages table, click the upgrade button, then select the device you want to use that package. Both methods will upgrade the device.

CLI Commands

Import the package file:

```
request devices software import remote-uri <fullPackagePath> remote-password
<password>
```

Note: <fullPackagePath> should follow a structure similar to this example: *sftp://user1@1.2.1.2/downloads/corero-ntd-combined-vm-dpdk-9.0.0.0351-signed.pkg* and in this case, the password you enter should correspond to the *user1* account.

Once the import is complete, push the software to each device you want to update:

```
request devices software packages package <packageType> <softwareVersion>
install device <deviceName>
yes
```

To check that the device is now running the new software:

```
show devices device status
```



Next steps

Put the upgraded device back inline with active network traffic.

Changing a Device's IP Address

You cannot change a device's IP address from within the CMS, but when you change a device's IP address on the device, you need to update the information in the CMS so that the CMS can reach the device on the new IP address.

To change a device's IP address

1. Connect to the device's console. For physical devices, you can connect using the device's IP address to SSH through an SSH client (e.g. `ssh -p 2222 admin@10.10.100.100`):
 - For **NTD1100** or **NTD280**, ssh on port 2222
 - For **NTD120** or **Bypass device**, ssh on port 22
 - For **vNTD**, you can ssh on port 2222 or open a console window for the VM in vsphere
2. Log in to the pCLI (using the same authentication credentials stored in the CMS for this device)
3. Type the command: `setup network`
4. Follow the steps in the wizard to change the device IP address.
5. In the CMS, use the left-hand menu to navigate to **Network > Devices**.
6. From the table, locate the device whose IP address you changed and click  the edit button. You can type a text string into the Search field to narrow down the list.
7. At the **Address** field, type the new IP address of the device.
8. Click **OK**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

These commands correspond to steps 5-9 above:

```
configure
edit devices device <deviceName>
```



```
set address <newIP>
commit
exit
```

Syncing a Device

If the Devices table shows the deployment actions **sync-required** (a commit was made when the device was unreachable and the devices policy no longer matches the CMS) or **force-sync-required** (an error occurred and the device's policy cannot be synced to the CMS), you must perform a CLI command to return the device to the in-sync state. Until you perform this command, the device won't receive any committed Policy updates.

To sync a device

1. Use the left-hand menu to navigate to **Network > Devices**.
2. From the table, locate the device you need to sync (the Deployment State displays **sync-required**) and click the **...** button. You can type sync-required into the Search field to narrow down the list.
3. Click **Sync Device**.
4. Click **OK**.

Note: If, after syncing a device, the Deployment State is **authentication-failed**. The credentials on your device do not match the stored credentials in the CMS. This can happen after you change a device's IP address. It may be in the wrong Authentication Group, or the Authentication Group may have a mistake in the credentials. Make sure the Authentication Group contains the correct credentials for this device then try syncing again.

To force sync a device

1. Use the left-hand menu to navigate to **Network > Devices**.
2. From the table, locate the device you need to force sync (the Deployment State displays **force-sync-required**) and click the **...** button. You can type force-sync-required into the Search field to narrow down the list.
3. Click **Force Sync Device**.
4. Click **OK**.

CLI Commands

Sync a device

```
request devices device <deviceName> sync-to-device
commit
```

Force-sync a device

```
request devices device <deviceName> force-sync-device  
commit
```

Rebooting a Device


If you need to, you can use the CMS to restart a device.

Caution: When you reboot a device you can briefly interrupt your network traffic while it is offline. You should always reroute the traffic before rebooting a device.

Prerequisites

Reroute traffic around the device.

To reboot a device

1. Use the left-hand menu to navigate to **Network > Devices**.
2. From the table, locate the device you want to reboot and click the  button. You can type a text string into the Search field to narrow down the list.
3. Click **Reboot**.
4. Click **OK**.

CLI Commands

```
request devices device <deviceName> restart action [application-
only|operating-system]
yes
```

Note: Choose `application-only`, to just restart the application on the device, or choose `operating-system` to restart the application and the operating system on the device.

Next steps

Place device back inline.

Redeploying a Device

Redeploying a device resets the hardware capabilities. For example, if you add a new module to an NTD280 Defense device, you must then redeploy the device before the CMS will see the new segments.


Caution: If the Defense device is not in a Cluster, redeploying will clear the Policy from the device. If the Defense device is in a Cluster, it will automatically re-sync the Policy associated with the Cluster.

Prerequisites

Reroute traffic around the device manually or using your connected Bypass device.

Caution: When you redeploy a device, you may briefly interrupt your network traffic unless you're using a connected Bypass device.

To redeploy a device

1. Use the left-hand menu to navigate to **Network > Devices**.
2. From the table, locate the device you want to reboot and click the  button. You can type a text string into the Search field to narrow down the list.
3. Click **Redeploy**.
4. Click **OK**.

CLI Commands

```
request devices device <deviceName> redeploy-device
yes
```

Next steps

Place device back inline or change Bypass Mode to send traffic to the Defense device.

Segments

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Segments Screen reference topic](#).

A Segment is a linked external and internal network interface defined from a front-panel port pair on a Defense device. The first time you connect a device to the SmartWall Central Management Server (CMS), it identifies the available interfaces and records them as Segments.

Note: As well as the identification number, you can use the CMS to provide a name for each Segment.

Each Segment should have external traffic coming in to the external interface and have its internal interface connected to the internal network to allow traffic to continue once it has been through the Defense device. If you don't intend to use one of the segments on your device, you can [disable the interfaces in that segment](#) to avoid any alarms being generated.

Link State Propagation

Note: Link State Propagation (LSP) is only available for Segments using the Dual-Interface Transparent Segment Mode.

For each supported Segment you can choose to enable or disable **Link State Propagation** (by default, this is enabled for all Segments). When Link State Propagation is enabled, if one interface in a Segment goes down then the other interface is also brought down. This prevents an interface from continuing to receive traffic after its linked interface has gone down.

Each interface in the Segment has its own status:

- **Up** – The interface is able to receive traffic
- **Down** – The interface is unable to receive traffic
- **Disabled** – The interface is purposefully disabled by a CMS user
- **Down link state propagation** – The Link State Propagation feature brought this interface down because the status of the partner interface in its Segment is "**Down**"

In the CLI, you can also set the `wait-time`, which is the number of seconds the system should wait before propagating a link state change to the partner interface.

Caution: Split-fiber deployments cannot support Link State Propagation. If your Defense device uses split-fiber, you must [disable Link State Propagation](#).

Analytics reporting per Segment

The CMS sends per segment syslog messages to SmartWall SecureWatch Analytics, where you can query these to view detailed reports. The CMS sends interface statistics which contain a field identifying the Segment associated with each statistic. You can query this field to view reports about an individual Segment on a device. Additionally, you can view a Segment's current and historic status (interface status, link speed, Defense Mode, Bypass Mode, etc).

Note: When a Segment has a Bypass device attached, the bypass mode, bypass state and port status displayed for that Segment are taken directly from the Bypass device rather than the Defense device.

Viewing Segment Status

If you want to view information about a Segment, you can view that information on the Segments screen and on the Home screen.

To view a segment's status

1. Use the left-hand menu to navigate to **Network > Segments**.
2. At the Segments table, you can see the current state of all the Segments in your network.
3. (Optional) Type a text string into the Search field to narrow down the list of Segments. For example, you could search for all Segments in a specific Defense device, or find the Segment using a specific Bypass device, or all Segments in a particular defense mode etc.
4. For more information about this table, see the [Segments Screen reference](#).


CLI Commands


```
show segments
```

Configuring a Segment

Default Segments are generated by the CMS the first time it connects to a new Defense device. By default, dual-interface Segments are created and are given generic names for identification. However, for a TDD deployment, only the 1st interface is required. Follow these steps to disable Link State Propagation (LSP) and to disable the additional interface for the vNTD segment.

To configure a Segment for TDD

1. Use the left-hand menu to navigate to **Network > Segments**.
2. From the Segments table, locate the Segment you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list.

3. (Optional) Edit the **Name**. This must be unique among Segments. You must only use alphanumerics, spaces, or `.-&()/_@:=` symbols.
4. (Optional) Type a **Description** of up to 265 characters.
5. The **External** Interface on the vNTD will already be selected.
6. In the **Internal** Interface drop-down, select **none-detector**.
7. (Optional) For networks using a tunnel to send traffic samples to the vNTD:
 - a. Set the External **IPv4 Address** to the IP address of the external interface on the vNTD (the tunnel endpoint)
 - b. Set the External **Peer IPv4 Address** to the IP address of the interface which is the last hop before the traffic arrives at the vNTD (e.g the interface on the router which has received the sampled traffic and is directly connected to the vNTD)
8. Under **Link State Propagation**, at the **Admin State** drop-down, select **disabled**.
9. Click **Save**.
10. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

```
configure
delete segments segment <deviceName><segmentID> internal
edit segments segment <deviceName><segmentID>
set name <segmentName> description "<descriptionText>"
set segment-mode detector
set external interface <interfaceID> inet <IPv4Address>
set external interface <interfaceID> inet peer-address <IPv4Address>
set link-state-propagation admin-state disabled
commit
exit
```



Connecting a Bypass Device to a Segment

If you use an external Bypass device, you must physically connect it to a Segment on a Defense device and also connect it to the Segment within the CMS. This enables you to manage the Bypass Mode for the external Bypass device attached to that Segment.

Prerequisites

- [Add a Defense device to the CMS](#)
- [Add a Bypass device to the CMS](#)
- Use cables to physically connect the Bypass device to a Segment on the Defense device

To connect an external Bypass device to a Segment

1. Use the left-hand menu to navigate to **Network > Segments**.
2. From the Segments table, locate the Segment you want to edit and click the  edit button. You can type a text string into the Search field to narrow down the list.
3. From the **Bypass Device** drop-down, select an available Bypass device.
4. Click **OK**.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click  **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).



CLI Commands

```
configure
set segments segment <defenseDeviceName> <segmentName> bypass-device
<bypassDeviceName>
commit
```

Enabling Link State Propagation

For each supported Segment you can choose to enable or disable **Link State Propagation (LSP)**. By default, this is enabled for all new Segments. When Link State Propagation is enabled, if one interface in a Segment goes down then the other interface is also brought down. This prevents an interface from continuing to receive traffic after its linked interface has gone down.

To enable/disable Link State Propagation

1. Use the left-hand menu to navigate to **Network > Segments**.
2. From the Segments table, locate the Segment you want to edit and click  the edit button. You can type a text string into the Search field to narrow down the list.
3. Select the required option from the **Link State Propagation** drop-down.
4. Click **Save**.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands


```
configure
set segments segment <deviceName> <segmentName> link-state-propagation
admin-state [disabled|enabled] wait-time <timeInSeconds>
commit
```

Note: In the CLI, you have the additional options of editing the number of seconds the system should wait before propagating a link state change to a partner (`wait-time`); by default, this is 1 second but can be set anywhere between 0-360.

Operating Modes

For information on changing your Operating Mode, access the built in help available in the CMS Web UI.

To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

SECTION 4

Manage Services

The SmartWall Central Management Server (CMS) provides support for additional DDoS protection services which use the SmartWall Threat Defense Director in conjunction with external devices:

- **BGP Mitigation** – Use the SmartWall system to detect when the rate of traffic going to one of your protected servers crosses a set threshold and send BGP routing updates for your Internet Service Provider to black-hole that DIP.

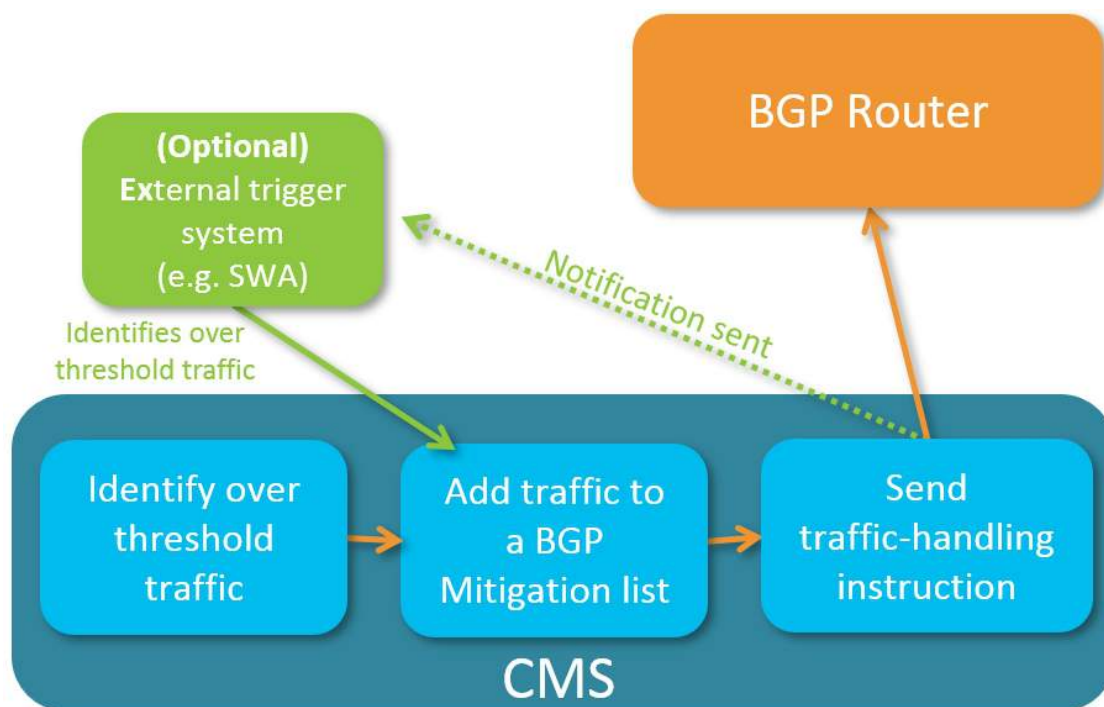
This section discusses the following:

BGP Mitigation	132
Connect to BGP routers	133
Entry states	134
ExaBGP strings for FlowSpec routes	136
Configuring a Direct BGP Connection for RTBH	137
Configuring a BGP Connection for RTBH via REST API	140
Configuring a BGP Connection for FlowSpec	144
Configuring BGP Mitigation DIP Thresholds	146
Managing the Black Hole Address List	148
Managing the FlowSpec routes List	150

BGP Mitigation

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [BGP Mitigation Screen reference topic](#).

When the rate of traffic going to one of your protected servers crosses a set threshold, the CMS can use Border Gateway Protocol (BGP) routing updates for your Internet Service Provider to black-hole specific traffic for a set period of time. For example, a particular server in your network is being attacked and the CMS has identified the traffic is at a rate which could start overwhelming your Internet connections. The CMS could then send a message to the upstream routers to black hole just the traffic heading to that Destination IP (DIP) until the attack was over. This stops the attack traffic filling your Internet connections and enables good traffic to continue to reach your other servers, without impact.



There are two types of BGP Mitigation available from the CMS:

- **Remote Triggered Black Hole (RTBH)** – Black holes traffic going to a specified destination IP address
- **FlowSpec** – Performs a specified action on traffic which is identified based on one or more match fields (DIP, SIP, destination port, source port, TCP flags etc)

There are three ways a BGP Mitigation can be activated:

- **Manually** – Use the CMS Web UI or CLI to add a RTBH address or FlowSpec route
- **Automatic CMS DIP threshold** – Traffic exceeds the specified rate thresholds to a single DIP, and the CMS performs the specified BGP Mitigation action (RTBH or FlowSpec action)
- **Automatic external trigger** – An external application (e.g. SWA), which monitors traffic levels, sends the command to apply a BGP Mitigation. For information on how to set up this type of BGP Mitigation integration, contact your support representative.

Note: RTBH and FlowSpec track the traffic rate of the top 32 DIPs in your network and can only announce routes for those 32 DIPs.

Connect to BGP routers

Different settings are required depending on the type of BGP Mitigation you want to configure.

Caution: You cannot use enable BGP CLIENT settings and RTBH REST CLIENT settings at the same time. You can enable RTBH with BGP CLIENT and FlowSpec at the same time. You cannot use RTBH with REST CLIENT and FlowSpec at the same time.

BGP connection for RTBH:

- Direct to BGP Router – Configure settings on BGP CLIENT and RTBH PATH ATTRIBUTES tabs
- Via an orchestrator REST API – Configure settings on RTBH REST CLIENT and RTBH PATH ATTRIBUTES tabs

BGP connection for FlowSpec:

- Configure settings on BGP CLIENT tab

Editing your BGP connection settings

You can follow the same steps above to edit your configuration. If you already have active black holes, you will see the following behavior when you commit a change to the BGP connection settings:

- If using a **BGP Client** connection (FlowSpec and/or RTBH) – The update will take immediate effect on the existing black holes and any future activations
- If using **BGP REST** connection (RTBH only) – Any future activations will use the updated configuration, but existing black holes will not. If you cannot wait for an existing black hole to auto-withdraw, you can manually withdraw and re-announce a black hole to apply the new configuration.

Changing the RTBH BGP configuration type (BGP Client or REST Client)

Before changing your BGP configuration type for RTBH, you should always withdraw all active black holes. If you change which BGP configuration type while you have active black holes, you will be unable to send a withdraw

instruction for that active black hole route. You will also be unable to delete the black hole from the Current Addresses table.

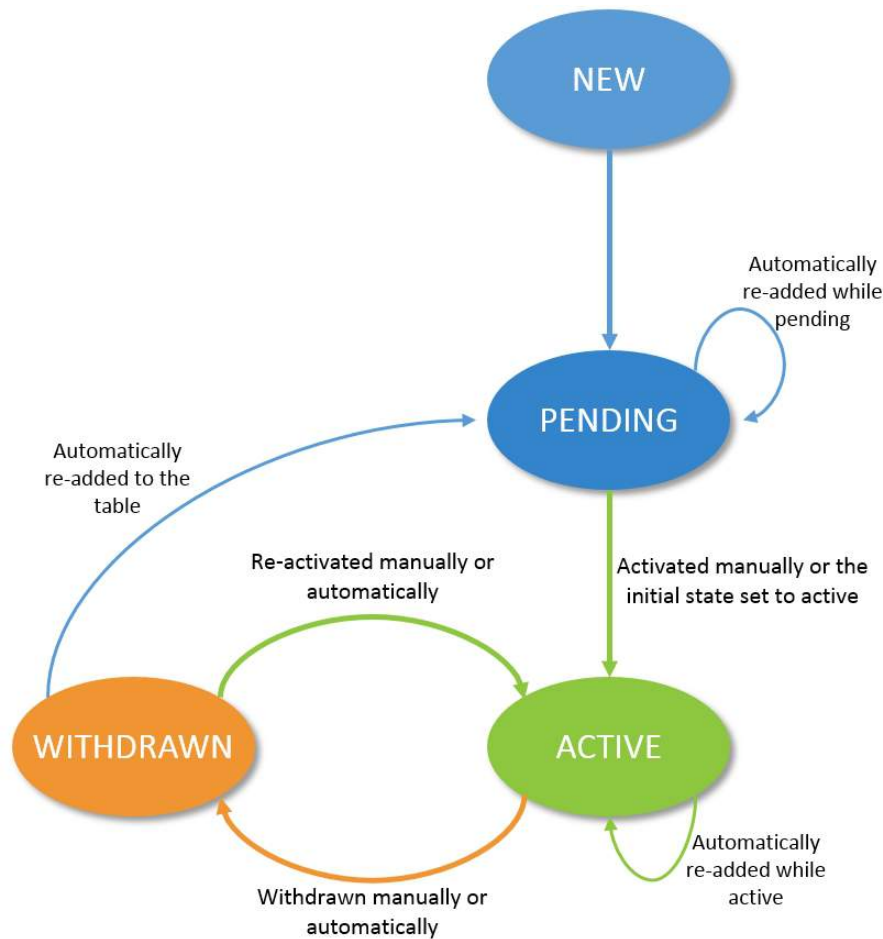
You need to reconnect the CMS to the original configuration type or access the black hole routes from another system to withdraw it.

Entry states

Entries on the RTBH and FlowSpec tables can exist in one of three states:

- **Pending** – The entry has been added to the table but not activated. This could be a new entry or one which has been re-added while in the Pending or Withdrawn state.
- **Active** – The entry is active. It could have been activated manually, automatically, or been re-added while the entry was in the Active state.
- **Withdrawn** – The entry was active but is now withdrawn. It could have been withdrawn manually, or automatically.

Note: When an entry is first added to a table it temporarily exists in the **new** state with the state reason **new-entry**. You may not see this in the table.



As well as showing the **State** of an entry (**pending**, **active**, or **withdrawn**), the tables also provides information on why this state has occurred in the **State Reason** column:

- **new-entry** – A temporary state while a new entry is added to the table.
- **re-added** – Traffic to the DIP has crossed the threshold rate and the entry has been re-added to the table.
- **activation-failed** – The CMS was unable to activate the entry. Check the BGP connection details are correct, and that there are no current network anomalies which could interrupt the connection.
- **withdraw-failed** – The CMS was unable to withdraw the entry. Check the BGP connection details are correct, and that there are no current network anomalies which could interrupt the connection.
- **activated-manually** – The initial state is set to pending and the entry was successfully activated by a CMS operator.
- **activated-automatically** – The initial state is set to active and the entry was successfully activated when it was added to the table.
- **withdrawn-manually** – The entry was successfully withdrawn by a CMS operator.
- **withdrawn-automatically** – The entry was successfully withdrawn by the Auto Withdraw Delay function.

- **withdrawn-snapshot-restore** – A snapshot has been restored on the CMS and active entries in the table have been withdrawn.

ExaBGP strings for FlowSpec routes

You can use the following semi-colon separated statements to create the Match and Action strings used for FlowSpec routes. You can use a single statement or multiple where appropriate.

Match string:

```
source <ip-address>/<prefixlength>;
destination <ip-address>/<prefixlength>;
port <portnumber>;
source-port <portnumber>;
destination-port <portnumber-expression>;
protocol [ udp | tcp ];
next-header [ udp | tcp ];
tcp-flags [ fin | syn | rst | push | ack | urgent ];
icmp-type [ echo-reply | echo-request | info-reply |
info-request | mask-reply | mask-request |
parameter-problem | redirect | router-advertisement |
router-solicit | source-quench | time-exceeded |
timestamp | timestamp-reply | unreachable ];
icmp-code [ communication-prohibited-by-filtering |
destination-host-prohibited |
destination-host-unknown |
destination-network-unknown |
fragmentation-needed | host-precedence-violation |
ip-header-bad | network-unreachable |
network-unreachable-for-tos | port-unreachable |
redirect-for-host | redirect-for-network |
redirect-for-tos-and-host |
redirect-for-tos-and-net |
required-option-missing | source-host-isolated |
source-route-failed |
ttl-eq-zero-during-reassembly |
ttl-eq-zero-during-transit ];
```



```
fragment [ not-a-fragment | dont-fragment | is-fragment |
first-fragment | last-fragment ];
dscp <dscp-value>;
traffic-class <traffic-class>;
packet-length <packet-length-expression>;
flow-label <flow-label-expression>;
```

Action string:

```
accept;
discard;
rate-limit <ratelimit>;
redirect ( <route-distinguisher> | <ip-address> );
copy <ip-address>;
mark <mark>;
action ( sample | terminal | sample-terminal );
community [...];
large-community [...];
extended-community [...];
```

Configuring a Direct BGP Connection for RTBH


Before you can use RTBH, you must connect the CMS to your BGP router. There are two ways to connect to the BGP client: a direct connection to the BGP client or [via an orchestrator REST API](#). You can only enable one method of communication between the CMS and your BGP router.

You can use RTBH on its own or alongside a FlowSpec connection. However, FlowSpec can only be used with RTBH when it is configured to use a direct BGP connection. You cannot use FlowSpec with an RTBH connection which uses the REST client.


Prerequisites

You must have a BGP router on your network edge which can announce and withdraw black hole routes. The router must be accessible from the CMS over a TCP connection.

To configure a direct BGP connection for RTBH

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Add the BGP Router's path attributes:
 - a. Select the **RTBH PATH ATTRIBUTES** tab.
 - b. Type the **IPv4 Next-Hop** and **IPv6 Next-Hop** for the black-hole route. These must be individual IP addresses without CIDR prefixes.
 - c. Add an entry for each route parameter required:
 - i. At the Entries table, click **Add**.
 - ii. Type a **Name** for this route parameter entry.
 - iii. For each BGP community needed, click **Add** and type a **BGP Community** name, then click **Save**.
You can also use  the delete button to modify your list.
 - iv. When you're happy with your route parameter entry, click **Save**.
3. Configure the direct connection to the BGP router:
 - a. Select the **BGP CLIENT** tab.
 - b. Change the **Admin State** to **enabled**.
 - c. Type the **Router ID** IP address of your local BGP router. This router must be positioned to enable a TCP connection with the CMS.
 - d. Type your **Local AS** for this router.

Note: The CMS only supports a 2-byte AS. It does not support a 4-byte AS.

- e. Add an entry for every neighbor (peer) of your local BGP router which may be contacted:
 - i. In the Neighbors table, click **Add**.
 - ii. Type the **Address** of the neighbor.
 - iii. (Optional) If you don't want to use this neighbor yet, change the **Admin State** to **Disable**. Otherwise, leave as **Enable**.
 - iv. Type the **Remote AS** of this neighbor.
 - v. Type the **MD5 Password** to access this neighbor.
 - vi. Click **Save**.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click  **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Next Steps

- (Optional) [Configuring BGP Mitigation DIP Thresholds](#)
- [Manage the Black Hole Address List](#)

CLI Commands

View BGP configuration

```
configure
show bgp-mitigation bgp-client
```

Path Attributes: Configure next hops

```
configure
set bgp-mitigation rtbh path-attributes ipv4-next-hop <ipv4Address> ipv6-
next-hop <ipv6Address>
commit
```

Path Attributes: Add a new entry or add a new community to an existing entry

```
configure
set bgp-mitigation rtbh path-attributes entry <entryName> community
<communityName>
commit
```

Path Attributes: Delete an entry

```
configure
edit bgp-mitigation rtbh path-attributes entry
delete <entryName>
commit
```

Path Attributes: Delete a community from an entry

```
configure
edit bgp-mitigation rtbh path-attributes entry <entryName>
delete community <communityName>
commit
```

BGP Client: Configure BGP router details

```
configure
set bgp-mitigation bgp-client admin-state [disabled|enabled] router-id
<routerIP> local-as <localASNumber>
commit
```

BGP Client: Add a new neighbor or edit an existing neighbor

```
configure
set bgp-mitigation bgp-client neighbor <neighbourName> admin-state
[disabled|enabled] remote-as <remoteASNumber> md5-password <password>
commit
```

BGP Client: Delete a neighbor

```
configure
edit bgp-mitigation bgp-client neighbor
delete <neighbourName>
commit
```

Configuring a BGP Connection for RTBH via REST API


Before you can use RTBH, you must connect the CMS to your BGP router. There are two ways to connect to the BGP client: [a direct connection to the BGP client](#) or via an orchestrator REST API. You can only enable one method of communication between the CMS and your BGP router.

You can use RTBH on its own or alongside a FlowSpec connection. However, FlowSpec can only be used with RTBH when it is configured to use a direct BGP connection. You cannot use FlowSpec with an RTBH connection which uses the REST client.

Prerequisites

You must have a BGP router on your network edge which can announce and withdraw black hole routes. The router must be accessible from the CMS via your own orchestrator REST API.

To configure a REST API BGP connection for RTBH

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Add the BGP Router's path attributes:
 - a. Select the **RTBH PATH ATTRIBUTES** tab.
 - b. Type the **IPv4 Next-Hop** and **IPv6 Next-Hop** for the black-hole route. These must be individual IP addresses without CIDR prefixes.
 - c. Add an entry for each route parameter required:
 - i. At the Entries table, click **Add**.
 - ii. Type a **Name** for this route parameter entry.
 - iii. For each BGP community needed, click **Add** and type a **BGP Community** name, then click **Save**.
You can also use  the delete button to modify your list.
 - iv. When you're happy with your route parameter entry, click **Save**.

3. Configure an indirect connection to the BGP router via orchestrator REST API:
 - a. Select the **BGP REST CLIENT** tab.
 - b. Change the **Admin State** to **enabled**.
 - c. Type your REST API **Username** and **Password**.
 - d. Select the **Content Type** required.
 - e. Configure the **Announce** endpoint:
 - i. Type your announce endpoint **URL**.
 - ii. Select a HTTP **Request Method** from the drop-down.
 - iii. Type the **Body** content required for your announce endpoint. Use the [required tokens](#) as placeholders for the information generated by the CMS for each new black hole.
 - f. Configure the **Withdraw** endpoint:
 - i. Type your withdraw endpoint **URL**.
 - ii. Select a HTTP **Request Method** from the drop-down.
 - iii. Type the **Body** content required for your withdraw endpoint. Use the [required tokens](#) as placeholders for the information generated by the CMS for each black hole which needs withdrawn.
 - g. (Optional) If there are any additional **HTTP Headers** required for your REST requests:
 - i. Click **Add**.
 - ii. Type the HTTP **Header** you want to add to the REST requests.
 - iii. Type the **Value** for that header.
 - iv. Click **Save**.

Caution: There are three headers you must be cautious of adding to the HTTP headers table.

- `accept` is by default set to `all`. Adding it to the HTTP Headers table will overwrite `all` with your chosen value.
- `authorization` is set by the **Username** and **Password** fields on this page. Using these fields overwrites an `authorization` header in the table. You must clear the Username and Password fields to use your own `authorization` value in the HTTP Headers table.
- `content-type` is set by the **Content Type** field on this page. Using this field overwrites a `content-type` header in the table. You must clear the Content Type field to use your own `content-type` value in the HTTP Headers table.

4. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: You can use the CLI to debug the REST API configuration, by viewing the exact REST configuration sent for an announce or withdraw request. The following command enables

you to announce or withdraw a DIP and then returns the HTTP request sent: `request bgp-mitigation rtbh rest [announce-api|withdraw-api] test address <dipaddress>`. **Caution:** Using the command to send an announce request will blacklist the specified DIP, just like manually adding a black hole.

Next Steps

- (Optional) [Configuring BGP Mitigation DIP Thresholds](#)
- [Manage the Black Hole Address List](#)

BGP REST endpoints: Body and URL tokens

The URL and Body fields accept the following tokens as placeholders for variable information. The CMS replaces each token with the appropriate information for each new black hole being announced or withdrawn.

The CMS replaces the following tokens with:

- `{ip}` – The section of the DIP CIDR *before* the slash. For example, if the DIP being black-holed is 192.168.10.10/32 this token is replaced with 192.168.10.10.
- `{mask}` – The section of the DIP CIDR *after* the slash. For example, if the DIP being black-holed is 192.168.10.10/32 this token is replaced with 32.
- `{nexthop}` – The next hop for this black hole route. Can be IPv4 or IPv6.
- `{community-n}` – The community represented by the index value (e.g. 6500:1234). To use the token, you need to replace `n` with the index value (1-16) representing the one of the communities associated with this black hole route.
- `{communities-space-separated}` – All communities associated with this black hole route, separated by spaces (e.g. 6500:1234 6500:1235 6500:1236).
- `{communities-comma-separated}` – All communities associated with this black hole route, separated by spaces (e.g. 6500:1234, 6500:1235, 6500:1236).
- `{id}` – A numeric hash of IP and mask values to identify the black hole. The ID will be the same every time this CIDR is announced.
- `{time}` – The current UTC time, formatted as the number of milliseconds since Epoch (e.g. 1525174499000).

Note: The `{time}` token is replaced by the time at the moment the REST request is sent and will not be the same for an announce and withdraw request for the same black hole.

In the event that there is no value available for a token, the token is removed from the URL or Body and replaced with nothing. For example, if you only have one community configured, `{community-2}` would be removed and replaced with nothing. If text other than a valid token is surrounded by braces `{ }`, it will not be removed or replaced. It will appear as entered in the URL or Body (e.g. `{community-pool}` would not be valid and would appear unedited in the request).

Note: Text in the URL field is altered by URL encryption when a request is generated, so may appear slightly different in the request.

CLI Commands

Path Attributes: Configure next hops

```
configure

set bgp-mitigation rtbh path-attributes ipv4-next-hop <ipv4Address> ipv6-
next-hop <ipv6Address>

commit
```

Path Attributes: Add a new entry or add a new community to an existing entry

```
configure

set bgp-mitigation rtbh path-attributes entry <entryName> community
<communityName>

commit
```

Path Attributes: Delete an entry

```
configure

edit bgp-mitigation rtbh path-attributes entry

delete <entryName>

commit
```

Path Attributes: Delete a community from an entry

```
configure

edit bgp-mitigation rtbh path-attributes entry <entryName>

delete community <communityName>

commit
```

BGP REST API: Configure connection

```
configure

set bgp-mitigation rtbh rest admin-state [disabled|enabled] content-type
<contentType> basic authentication username <RESTusername> password
<RESTpassword>

commit
```

Tip: In the CLI, you can also set the connection and read timeouts for contacting the REST API. The default for both is 5 seconds. `set rtbh bgp rest connection-timeout <seconds> read-timeout <seconds>`

BGP REST API: Configure announce and withdraw endpoints

```
configure
set bgp-mitigation rtbh rest announce-api url <endpointURL> request-method
[CONNECT|DELETE|GET|HEAD|OPTIONS|PATCH|PUT|TRACE] body "<body>"
set bgp-mitigation rtbh rest withdraw-api url <endpointURL> request-method
[CONNECT|DELETE|GET|HEAD|OPTIONS|PATCH|PUT|TRACE] body "<body>"
commit
```

Caution: The entire body string must be surrounded with quotes or the command won't be accepted e.g: body '{"items":[{"adminState":"enabled", "definition": "hostabc{ip}", "name": "name{ip}"}]}'

BGP REST API: Add a new HTTP header or edit the value of an existing HTTP header

```
configure
set bgp-mitigation rtbh rest http-headers <headerName> value <headerValue>
commit
```

BGP REST API: Delete a HTTP header

```
configure
edit bgp-mitigation rtbh rest http-headers
delete <headerName>
commit
```

Configuring a BGP Connection for FlowSpec

Before you can use FlowSpec, you must connect the CMS to your BGP client.

You can use FlowSpec on its own or alongside a RTBH connection which uses direct BGP connection. If you have RTBH (using a direct BGP connection) already configured, then your CMS BGP client is configured and you can skip this step and move on to [Manage the FlowSpec Routes List](#) or [Configuring BGP Mitigation DIP Thresholds](#).

Note: You cannot use FlowSpec with an RTBH connection which uses the REST client.

Prerequisites

You must have a BGP router on your network edge which can send FlowSpec instructions. The router must be accessible from the CMS over a TCP connection.

To configure the CMS BGP client for FlowSpec

1. Open the CMS in a browser and log in.
2. Use the left-hand menu to navigate to **Services > BGP Mitigation**.

3. Configure the connection to the BGP router:

- a. Select the **BGP CLIENT** tab.
- b. Change the **Admin State** to **enabled**.
- c. Type the **Router ID** IP address of your local BGP router. This router must be positioned to enable a TCP connection with the CMS.
- d. Type your **Local AS** for this router.

Note: The CMS only supports a 2-byte AS. It does not support a 4-byte AS.

e. Add an entry for every neighbor (peer) of your local BGP router which may be contacted:

- i. In the Neighbors table, click **Add**.
- ii. Type the **Address** of the neighbor.
- iii. (Optional) If you don't want to use this neighbor yet, change the **Admin State** to **Disable**. Otherwise, leave as **Enable**.
- iv. Type the **Remote AS** of this neighbor.
- v. Type the **MD5 Password** to access this neighbor.
- vi. Click **Save**.

4. If you want to save the new configuration, and push your changes to any affected Defense devices, click

Commit

. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Next Steps

- (Optional) [Configuring BGP Mitigation DIP Thresholds](#)
- [Manage the FlowSpec Routes List](#)

CLI Commands

View BGP configuration

```
configure
show bgp-mitigation bgp-client
```

BGP Client: Configure BGP router details

```
configure
set bgp-mitigation bgp-client admin-state [disabled|enabled] router-id
<routerIP> local-as <localASNumber>
commit
```

BGP Client: Add a new neighbor or edit an existing neighbor

```
configure
```

```
set bgp-mitigation bgp-client neighbor <neighbourName> admin-state
[disabled|enabled] remote-as <remoteASNumber> md5-password <password>
commit
```

BGP Client: Delete a neighbor

```
configure
edit bgp-mitigation bgp-client neighbor
delete <neighbourName>
commit
```

Configuring BGP Mitigation DIP Thresholds

If you want to enable the CMS to send RTBH or FlowSpec routes when the traffic rate to a Destination IP address goes too high, you need to configure the BGP Mitigation DIP Thresholds.

Note: Only individual /32 or /128 DIPs are mitigated automatically. To mitigate a larger CIDR, you need to [manually add the CIDR](#) to the black hole addresses table.

Prerequisites

You must have at least one of the following connections established with your BGP router:


- [Configuring a direct BGP connection for RTBH](#)
- [Configuring a BGP connection for RTBH via REST API](#)
- [Configuring a BGP connection for FlowSpec](#)

To configure BGP Mitigation Thresholds

Caution: You do not have to commit changes made to the Current Addresses table. As soon as you make the change it is pushed to your BGP router.

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Configure the traffic threshold which trigger a black-hole:
 - a. Select the **DIP THRESHOLDS** tab.
 - b. Set the maximum rate of **blocked** traffic to a DIP:
 - i. Set the blocked **Admin State** to **enabled**.
 - ii. Type a **Blocked Traffic Threshold** for a single DIP (in Mbps). The threshold is crossed when the average rate of blocked traffic, over the **Threshold Trigger Period**, is more than this threshold value.
 - c. Set the maximum rate of **allowed** traffic to a DIP:
 - i. Set the allowed **Admin State** to **enabled**.
 - ii. Type an **Allowed Traffic Threshold** for a single DIP (in Mbps). The threshold is crossed when the average rate of allowed traffic, over the **Threshold Trigger Period**, is more than this threshold value.
 - d. Select the action to be performed when a DIP Threshold is exceeded:
 - e. In **Threshold Trigger Period**, set the number of seconds over which the average traffic rates are calculated to see if any single DIPs are above blocked or allowed traffic thresholds. The default time is 60 seconds. You can select a time between 10 and 300 seconds.
 - f. In **Auto Withdraw Delay**, set the number of minutes the DIP should be should be in a table before it is automatically withdrawn (default is 0). If an attack is still in progress, once withdrawn the traffic will re-trigger the threshold and be re-added to the table in the **Initial State**.

Tip: By default, the **Auto Withdraw Delay** is disabled by having it set to **0**. In this configuration, you must manually withdraw any black holes.

3. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Next Steps

Set the initial state for new routes added to tables:

- [Manage the Black Hole Address List](#)
- [Manage the FlowSpec Routes List](#)

CLI Commands

Configure DIP thresholds
configure

```
set bgp-mitigation dip-thresholds allowed admin-state [disabled|enabled]
threshold <allowedTraffic>

set bgp-mitigation dip-thresholds blocked admin-state [disabled|enabled]
threshold <blockedTraffic>

set bgp-mitigation dip-thresholds threshold-trigger-period <seconds>
set bgp-mitigation dip-thresholds auto-withdraw-delay <minutes>

commit
```

Managing the Black Hole Address List

You can manage the RTBH Address table manually or via REST API. This topic covers manual operations. For more information on announcing and withdrawing black holes using the REST API (for example, from an analytics application like SWA), contact your Corero representative.

Caution: You do not have to commit changes made to the Current Addresses table. As soon as you make the change it is pushed to your BGP router through your enabled connection method (BGP Client or BGP REST API). You must commit changes to the Initial State drop-down.

Manage RTBH address table

As well as automatically adding DIPs to the black hole addresses table using the CMS DIP thresholds or an external trigger, you can manually add an address, with CIDR prefix, to the list. You might want to do this to test your BGP configuration is working as expected or, to black hole DIPs which don't meet the current automatic threshold configuration.

Note: Black holes added manually will not be automatically withdrawn. You must manually withdraw these black holes when ready.

Prerequisites

- [Set up a connection to your BGP server](#)

To set the initial state

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Select the **BLACK HOLE ADDRESSES** tab.

3. Set the **Initial State**:


- **pending** – (default) All new black holes announced are added to the Current Addresses table but not activated. An operator can be prompted of a new black hole announcement and can access CMS to manually activate this.
- **active** – All new black holes announced are added to the Current Addresses table and are immediately activated.

4. If you want to save the new configuration, and push your changes to any affected Defense devices, click




Commit

. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

To manually black hole a DIP

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Make sure the **BLACK HOLE ADDRESSES** tab is selected.
3. Make sure the **Initial State** field is [set as required](#). This field also applies to black holes added to the table using automatically added RTBH addresses.
4. Click **Add**.
5. Type the Destination IP **Address** you want to black hole. This must be formatted to include the subnet (e.g. 1.2.3.0/24). The subnet can be any size.
6. (Optional) Type a **Description** of this black hole.
7. Click **Save**
8. Activate the black hole:
 - If the **Initial State** is **active**, the black hole will now be active (for the length of time given in the **Auto Withdraw Delay** field on the **DIP THRESHOLDS** tab).
 - If the **Initial State** is **pending**, you need to click  the activate button to announce the black hole.

Tip: While an IP address is in the Current Addresses table, you can:

-  deactivate a black hole
-  reactivate a black hole
-  deactivate the black hole (if active) and delete the entry from the table
- **Purge Withdrawn** – delete all withdrawn entries from the table

Deleting RTBH entries

The CMS can store up to 1000 black hole entries. If another entry is added (manually or automatically) the oldest inactive entry is deleted to make room. If all 1000 entries are active, the CMS deletes the entry with the oldest "last updated" time field.

Note: In the unlikely event that you need to force the CMS to delete an entry from the table (without withdrawing the route), you can use the CLI command: `request bgp-mitigation rtbh blackhole-addresses entry <entryAddress> remove force`

CLI Commands

Set the initial state

```
configure
set bgp-mitigation rtbh blackhole-addresses initial-state [active|pending]
commit
```

View black hole addresses

```
show bgp-mitigation rtbh blackhole-addresses
```

Manually add a black hole address

```
request bgp-mitigation rtbh blackhole-addresses add address <dipCIDR>
description "<description>" source [dip-threshold-trigger|manual|rest]
```

Manage an existing black hole

```
request bgp-mitigation rtbh blackhole-addresses entry <entryAddress>
[activate|remove|withdraw]
```

Note: `remove` is the same as deleting an entry in the Web UI. It withdraws the black hole then removes the entry it from the table.

Purge all withdrawn black holes

```
request bgp-mitigation blackhole-addresses purge
```

Managing the FlowSpec routes List

You can manage the FlowSpec Route table manually or via REST API. This topic covers manual operations. For more information on using the REST API (for example, from an analytics application like SWA), contact your Corero representative.

Caution: You do not have to commit changes made to the Current Routes table. As soon as you make the change it is pushed to your BGP router through your enabled connection method (BGP Client or BGP REST API). You must commit changes to the Initial State drop-down.

Manage FlowSpec routes table


As well as automatically adding routes to the FlowSpec table using the CMS DIP thresholds or an external trigger, you can manually add a route. You might want to do this to test your BGP configuration is working as expected or, to add routes which don't meet the current automatic threshold configuration.

Note: Routes added manually will not be automatically withdrawn. You must manually withdraw these routes when ready.


Prerequisites

- [Set up a connection to your BGP server](#)



To set the initial state


1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Select the **FLOWSPEC ROUTES** tab.
3. Set the **Initial State**:
 - **pending** – (default) All new routes announced are added to the Current Routes table but not activated. An [operator can be prompted](#) of a new route announcement and can access CMS to manually activate this.
 - **active** – All new routes announced are added to the Current Route table and are immediately activated.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

To manually add a FlowSpec route

1. Use the left-hand menu to navigate to **Services > BGP Mitigation**.
2. Select the **FLOWSPEC ROUTES** tab.
3. Make sure the **Initial State** field is set as required. This field also applies to black holes added to the table using automatically added FlowSpec routes.
4. Click **Add**.
5. Type a **Name** for this route.
6. (Optional) Type a **Description** of this route.
7. Type a **Match** string in [ExaBGP format](#).
8. Type an **Action** string in [ExaBGP format](#).
9. Click **Save**
10. Activate the route:
 - If the **Initial State** is **active**, the route will now be active (for the length of time given in the **Auto Withdraw Delay** field on the **DIP THRESHOLDS** tab).
 - If the **Initial State** is **pending**, you need to click  the activate button to announce the route.

Tip: While a route is in the Current Routes table, you can:

-  withdraw the route
-  reactivate the route

-  withdraw the route (if active) and delete the entry from the table
- **Purge Withdrawn** – delete all withdrawn entries from the table

Deleting FlowSpec entries

The CMS can store up to 1000 entries in the FlowSpec routes table. If another entry is added (manually or automatically) the oldest inactive entry is deleted to make room. If all 1000 entries are active, the CMS deletes the entry with the oldest "last updated" time field.

Note: In the unlikely event that you need to force the CMS to delete an entry from the table (without withdrawing the route), you can use the CLI command: `request bgp-mitigation flowspec-routes entry <entryAddress> remove force`

CLI Commands

Set the initial state

```
configure
set bgp-mitigation flowspec-routes initial-state [active|pending]
commit
```

View FlowSpec routes

```
show bgp-mitigation flowspec-routes
```

Manually add a route

```
request bgp-mitigation flowspec-routes add name <routeName> description
"<description>" action "<actionString>" match "<matchString>"
```

Manage an existing route

```
request bgp-mitigation flowspec-routes entry <entryName>
[activate|remove|withdraw]
```

Note: `remove` is the same as deleting an entry in the Web UI. It withdraws the route then removes the entry from the table.

Purge all withdrawn routes

```
request bgp-mitigation flowspec-routes purge
```


SECTION 5

Manage CMS

The SmartWall Central Management Server (CMS) is the heart of the SmartWall Threat Defense Director. It connects the SmartWall devices in your network, and sends analytics information to SmartWall SecureWatch Analytics.

This section discusses the following:

CMS System	156
Initial CMS System Actions	157
Uploading an HTTPS Certificate	157
Uploading a SecureWatch Package	157
Connecting to SWA or Another Syslog Server	160
Changing the CMS Timezone	164
Users	165
CMS user roles	165

Types of user authentication	166
IP Filters	167
Support login	167
Managing Local Users	168
Configuring LDAP Authentication	170
Configuring RADIUS Authentication	173
Setting the Authentication Order	176
Setting Web UI Timeouts	177
Enabling Support Account	177
Configuring CMS IP Filter Management	178
Snapshots	181
Snapshoting your CMS Configuration	181
Scheduling Backups	183
CMS Software	186
Upgrading the CMS Software Version	186
Rolling Back to an Old CMS Software Version	187
SNMP	188
Supported SNMP versions	188
SNMP traps	188
CMS MIBs	189
Configuring the CMS SNMP Settings	189
Managing SNMP trap destinations	191
CMS Licenses for vNTD	193
Viewing License Capacity	193
Adding a vNTD License	195

Licensing/delicensing a vNTD	197
SSH Keys	198
SSH Keys for Authentication Groups	198
SSH Keys for authenticating Remote devices	198
Importing an SSH Key	198
Support Tasks	200
Viewing the Audit Log	200
Downloading Diagnostic Files	201
Restarting the CMS	203
Resetting the CMS to the Default Configuration	203

CMS System

The CMS system features are for admin accounts only. You can use them to authenticate CMS users, create snapshots, perform software upgrades, configure your analytics settings, upload a new SSL certificate, and other high level administrative tasks.

Initial CMS System Actions

There are four main CMS System configuration actions you should do when you first deploy the CMS:

- Upload a signed SSL certificate
- Upload a SecureWatch package
- Connect the CMS to SWA or other syslog server
- Make sure the CMS is in your correct timezone

Uploading an HTTPS Certificate

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [HTTPS Screen reference topic](#).

The CMS comes with a default self-signed Corero SSL certificate which your browser will list as "not secure". As soon as possible, you should replace this with a signed certificate.

Note: Certificates must be packaged in pkcs12 format and can optionally be password protected. The pkcs file should contain a single private key and certificate pair.

To upload a new SSL certificate to the CMS

1. Use the left-hand menu to navigate to **System > Certificates**.
2. Click **Upload Certificate**.
3. Select a pkcs12 certificate file on your computer, and click **Open**.
4. (Optional) Type in the **Password** for the certificate file.
5. Click **OK**.
6. If necessary, refresh the browser to ensure the new certificate has been loaded.

CLI Commands

```
request system https install-certificate-from-pkcs12 remote-uri <remoteURI>
remote-password <remotePassword> password <pkcs12Password>
```

Uploading a SecureWatch Package

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [SecureWatch Screen reference topic](#).

The SecureWatch Service enables monitoring and remote management from Corero's Security Operations Center. If your SmartWall Central Management Server (CMS) application was not deployed on a SmartWall Management Controller you must configure the CMS to connect to the SecureWatch Service using a SecureWatch package file. You can upload this file to the CMS using the Web UI, CLI or pCLI.

Note: To enable the SecureWatch Service you must also configure your firewall to allow **outbound TCP port 443** traffic to destination DNS **address sw2.-corero-cns.com** and IP address **68.233.164.235**.

Prerequisites

- You should receive a SecureWatch package file (.pkg) from your Corero representative and save this to your PC
- You should also receive an unlock code for that file and have that available

To upload a SecureWatch package

1. Use the left-hand menu to navigate to **System > SecureWatch**.
2. Make sure the **PACKAGE** tab is selected.
3. Click **Upload Package**.
4. Select the SecureWatch package file on your computer, and click **Open**.
5. Type in the **Unlock Code** for the package file.
6. Click **OK**.

CLI Commands

```
request system securewatch upload-package remote-uri <remoteURI> remote-
password <remotePassword> password <pkgUnlockCode>
```

Alternative methods for uploading a SecureWatch package using the CMS pCLI

The CMS pCLI is the provisioning command line interface for the CMS. You can use it to perform some initial tasks during installation, including uploading a SecureWatch package file. There are two ways to upload the package file using the pCLI.

To install the SecureWatch package using a base64 file

1. You will receive the base64 file and unlock code from Corero Customer Support.
2. Open a console connection to your CMS application to access the pCLI. If you're using an ssh client, you can connect using the following command: `ssh -p 2222 <username>@<cmsIPaddress>`
3. Type `package-install base64` and press return.
4. Copy the base64 text and paste into the pCLI. Type **Ctrl-d**.
5. When prompted, copy the unlock code and paste into the pCLI, then press return.
6. To verify you're connected, type: `show securewatch` and press return.

To install the SecureWatch package from a local server

1. You will receive the SecureWatch package and unlock code from Corero Customer Support.
2. Save the package on a local server (HTTP, HTTPS, FTP or SFTP).
3. Open a console connection to your CMS application to access the pCLI. If you're using an ssh client, you can connect using the following command: `ssh -p 2222 <username>@<cmsIPaddress>`
4. Type `package-install` and press return.
5. Type the address of the local server where you saved the package and press return. Then type the password and press return.
6. Type the SecureWatch package unlock code and press return.
7. To verify you're connected, type: `show securewatch` and press return.

Next Steps

- Once you have uploaded a package, the SecureWatch Service will be able to connect to your CMS.
- You also need to upload a SecureWatch Package on your SWA application. You can do this in the SWA application in your browser or from the pCLI. For information on how to do this using the SWA pCLI, see the **Corero SmartWall Getting Started Guide** PDF.


Connecting to SWA or Another Syslog Server



The SmartWall Central Management Server (CMS) collates syslog messages from the SmartWall devices in your network and then it can send a summarized version of that information on to SmartWall SecureWatch Analytics (SWA), where the messages are used to produce real-time and historical analytics.

Before the SWA can display information, you must set up the CMS to forward syslog messages to the SWA. You can also configure the CMS to forward the syslog messages to other applications that process syslog messages.

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Analytics & Syslog Screen reference topic](#). See information on Address Groups to [learn more about IP reporting](#).


To connect to an Analytics or Syslog Server

1. Use the left-hand menu to navigate to **System > Analytics & Syslog**. Make sure the SERVERS tab is selected.
2. Click **Add Server** at one of the following tables:
 - **Analytics Servers** – For SWA applications
 - **Syslog Servers** – For all other applications which process syslog messages
3. Type a **Name** for this server. You must only use alphanumeric, spaces, or .-&()/_/@:= symbols.
4. Type the IP **Address** of the server (or its DNS name).
5. Enable or Disable **Encryption** for this server. The CMS and SWA come with self-signed SSL certificates. You can choose to upload signed certificates to the CMS and SWA- see optional steps below.
6. Type the **Port** you server accepts syslog messages on. The default (9997 for unencrypted and 9998 for encrypted) is the correct port for SWA.
7. Click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).
9. Open your server application and check it is now receiving syslog messages.

Tip: On the servers tables in the CMS, you can use the following action buttons to edit  or delete  a server connection.

Optional– Add a signed certificate to the CMS - SWA connection

By default, the connection between the CMS and SWA uses an in-built self-signed certificate. If you want to use a signed certificate, you need to upload a PKC#S12 certificate to both sides of the connection.

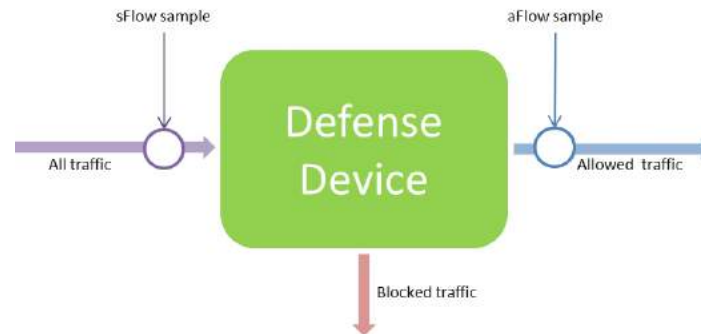
1. Add a signed SSL certificate in the CMS side of the connection:
 - a. Use the left-hand menu to navigate to **System > Analytics & Syslog**.
 - b. Open the **SSL CERTIFICATE** tab.
 - c. Click **Upload Certificate**.
 - d. Select a pkcs12 certificate file on your computer, and click **Open**.
 - e. (Optional) Type in the **Password** for the certificate file.
 - f. Click **OK**.
 - g. If necessary, refresh the browser to ensure the new certificate has been loaded.
 - h. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).
2. Add a signed certificate to the part of the SWA that receives information from CMS:
 - a. Access the SWA pCLI:
 - Open a console session. On an ESXi server, you can use VMware (select the VM and click **Open Console**) or on a KVM server you can use virsh (command: `virsh console <vmName>`).
 - SSH to the pCLI: `ssh -p 2222 admin@<ipAddress>`
 - b. Log in. If you haven't yet changed them, the default username and password is admin/smartwall.
 - c. To load a certificate, type `ssl-certificates forwarder` followed by the URI to the PKCS#12 format certificate file. The supported protocols are FTP, SFTP, HTTP, and HTTPS. For example: `ssl-certificates forwarder sftp://admin@10.20.30.40/certs/my_cert.p12`
 - d. You will be prompted for a password to access the file location. If you password protected the PKCS#12 file, you will also be prompted for that password.

Note: The certificate must be in PKCS#12 format, and include the private key, signed certificate, and CA certificate change to be used for SSL. The common name should match the hostname assigned to the SWA appliance.

To configure syslog message settings

Note: The configuration of syslog message settings in the CMS applies to all syslog and analytics servers.

The CMS analyzes sample packets from the traffic flow to detect attacks and trigger rules. The CMS then sends a sample of those packets on to SWA to provide the data for analytics.



There are two types of samples taken by the CMS:

- **sFlow** – A sample of all traffic coming into the Defense device. Useful for detecting attacks and seeing your incoming traffic stats.
- **aFlow** – A sample of the traffic that the Defense device has allowed through. You can use this to check how well your SmartWall system configuration is working to block unwanted packets.

These are used to report on inbound (coming into the internal network) and outbound (leaving the internal network) traffic.

Note: The default syslog message configuration should work for most systems.

1. Use the left-hand menu to navigate to **System > Analytics & Syslog**.
2. Select the **MESSAGE CONTROLS** tab.
3. You can edit the following options:
 - **sFlow Inbound Limit** – (Default: 5) Change the maximum number of sample inbound packets, sampled from all traffic types, that the CMS will send every second
 - **sFlow Outbound Limit** – (Default: 5) Change the maximum number of sample outbound packets, sampled from all traffic types, that the CMS will send every second
 - **aFlow Inbound Limit** – (Default: 5) Change the maximum number of sample inbound packets, sampled from allowed traffic, that the CMS will send every second
 - **aFlow Outbound Limit** – (Default: 5) Change the maximum number of sample outbound packets, sampled from allowed traffic, that the CMS will send every second
 - **Rule Event Limit** – (Default: 5) Change how many security event messages, per rule, the CMS will send to the SWA every second
 - **Send Events** – (Default: enabled) Choose to send (**enabled**) or stop sending (**disabled**) event messages
 - **Send Detected Events** – (Default: enabled) Choose to send (**enabled**) or stop sending (**disabled**) an event message when a rule detects matching traffic (as opposed to blocking matching traffic)
 - **Send Logs** – (Default: enabled) Choose to send (**enabled**) or stop sending (**disabled**) CMS log entries on to the analytics/syslog server

4. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

Connect to an Analytics or syslog server

```
configure
set analytics [server|syslog-server] name <serverName> address <ipAddress>
port <syslogPort>
commit
```

Edit a server

```
configure
set analytics [server|syslog-server] name <serverName> address <ipAddress>
port <syslogPort>
commit
```

Rename a server

Note: Not currently available in the Web UI.

```
configure
request analytics [server|syslog-server] <serverName> rename name <newName>
commit
```

Delete a server

```
configure
delete analytics [server|syslog-server] name <serverName>
commit
```

Upload an SSL certificate

```
configure
request analytics ssl install-certificate-from-pkcs12 remote-uri <remoteURI>
remote-password <remotePassword> password <pkcs12Password>
commit
```

Configure syslog message setting

```
configure
edit analytics message-controls
```

```

set rule-event-limit <limit>
set send-detected-events [disabled|enabled]
set send-events [disabled|enabled]
set send-logs [disabled|enabled]
set sflow-inbound-limit <limit>
set sflow-outbound-limit <limit>
set aflow-inbound-limit <limit>
set aflow-outbound-limit <limit>
commit
exit

```

Changing the CMS Timezone

You can change the timezone for the CMS system to change the time signature on syslog messages to match the location of your CMS.

Caution: Changing the timezone will restart the CMS.

To change the timezone of the CMS

1. Use the left-hand menu to navigate to **System > System Actions**.
2. At the **Configure System Timezone** drop-down, select the new timezone.
3. Click **Apply**
4. Click **OK**.
5. Once the system restarts, log back in to the CMS.

CLI Commands

```
request system set-timezone timezone <timezone>
```

Tip: Use the tab key after `request system set-timezone timezone` to see a list of available timezones.

```
commit
```

Users

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Authentication Screen reference topic](#).

Note: The Authentication screen is only visible for **cns-admin** users.







When you install the SmartWall Central Management Server (CMS), you will have one administrative user account. You can create more user accounts, either locally or by mapping to an external LDAP server.

Note: If you need assistance from Corero Customer Support, you can enable a support account on the CMS, giving them access to high level settings.

CMS user roles

There are three standard user roles available for the CMS:

- **cns-admin** – The administrative role. An admin user can edit all **Policy**, **Network**, and **System** configurations, including managing users.
- **cns-defense** – A non-administrative role which enables its users to edit all **Policy** options but no Network or System administrative settings
- **cns-monitor** – A primarily read-only role which enables its users to view settings without being able to enact any changes (aside from their own password)

	cns-admin	cns-defense	cns-monitor
Policy (e.g. <ul style="list-style-type: none"> • Protection Profiles • Configuration of attack mitigation features • Address groups) 	 Full access	 Full access	 Read-only access
Devices (e.g. <ul style="list-style-type: none"> • Device Status • Upgrades • Clusters and Segments • Operating Modes • Authentication Groups) 	 Full access	 Read-only access	 Read-only access

	cns-admin	cns-defense	cns-monitor
CMS System (e.g. <ul style="list-style-type: none"> User authentication SSL certificates Analytics settings Snapshots and upgrades) 	 Full access	 Read-only access to some pages	 Read-only access to some pages
Manage own password			

Types of user authentication

There are three types of user authentication available on the CMS:

- **Local Authentication** – Admin users can create and manage local CMS user accounts using the CMS Web UI or CLI
- **RADIUS** – Admin users can configure the CMS to enable users to log into the CMS using their existing organization credentials by connecting to your organization's authentication server over RADIUS
- **LDAP** – Admin users can configure the CMS to enable users to log into the CMS using their existing organization credentials by connecting to your organization's authentication server over LDAP

Note: When you use LDAP or RADIUS authentication, you cannot edit external user details or manage those user passwords from within the CMS. Also, LDAP and RADIUS admin users cannot use their external credentials to access the CMS pCLI.

Authentication order

If you enable one or both types of external authentication, it's possible some of your users may be in more than one database. In that case, you should check you have the correct authentication order for your system:

Option	Authentication Order
External, Local (Default)	<ol style="list-style-type: none"> If enabled, try RADIUS server: <ul style="list-style-type: none"> If accepted: log user in. If rejected: log in denied and no further attempts are made. If server unavailable, try next level of authentication. If enabled, try LDAP server: <ul style="list-style-type: none"> If accepted: log user in. If rejected: log in denied and no further attempts are made. If user does not exist or server unavailable, try next level of authentication. Try local user database: <ul style="list-style-type: none"> If accepted: log user in. If rejected: log in denied and no further attempts are made.
Local, External	<ol style="list-style-type: none"> Try local user database: <ul style="list-style-type: none"> If accepted: log user in. If user does not exist or authentication fails, try next level of authentication. If enabled, try RADIUS server: <ul style="list-style-type: none"> If accepted: log user in. If rejected: log in denied and no further attempts are made. If server unavailable, try next level of authentication. If enabled, try LDAP server: <ul style="list-style-type: none"> If accepted: log user in. If rejected or server unavailable: log in denied and no further attempts are made.

Note: Support accounts are not affected by authentication order.

IP Filters

You can filter which IP addresses are permitted to access the application over the management interface. After you enable IP filtering, you can manage a list of permitted IP addresses. For the CMS, you can manage this list in the [CMS Web UI](#), [CLI](#) or in the [pCLI](#). You can manage IP filters for your devices, on the device pCLI.


Support login



If you require assistance with the CMS, you can allow a Support Engineer to log into your CMS to enact a change. For example, you may require assistance with an upgrade, or help diagnosing an issue. Support accounts can access everything an admin account can, and a few high level support-only options.

Managing Local Users

There are three types of local CMS user account, they all have different levels of access to the CMS.

To create a user account

1. Use the left-hand menu to navigate to **System > Authentication**. Make sure you're on the **USERS** tab.
2. Click **Add User**.
3. Type a user **Name**. The name must only include lowercase letters, numbers and `_`, `-`, and `$` symbols. The `$` symbol can only be the last character. The `-` symbol cannot be the first character.
4. Select a user **Role**:
 - **cns-admin** – The administrative role. An admin user can edit all **Policy**, **Network**, and **System** configurations, including managing users.
 - **cns-defense** – A non-administrative role which enables its users to edit all **Policy** options but no Network or System administrative settings
 - **cns-monitor** – A primarily read-only role which enables its users to view settings without being able to enact any changes (aside from their own password)
5. Type a **Password** for this user and then **Repeat Password** in the field below.
6. Click **Save**.
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Users table, you can use the following action buttons to edit  or delete  a user. When you edit a user's account, you can change their password for them or change their user role.

CLI Commands

Create a new local user

```
configure
set aaa authentication users user <userName> role [cns-admin|cns-
defense|cns-monitor] password <userPassword>
commit
```

Edit a user's role or change password

```
configure
edit aaa authentication users user <userName>
set role [cns-admin|cns-defense|cns-monitor]
```



```
set password <userPassword>
commit
exit
```

Delete a local user


```
configure
edit aaa authentication users
delete user <userName>
commit
exit
```

Configuring LDAP Authentication

There are three main steps to connect an LDAP server to the CMS:

- Configure the LDAP bind account details and attributes which the CMS will use to log in to the LDAP server and attempt to look up user details.
- Add the connection details for your LDAP server(s) to the LDAP Servers list.
- Create a mapping of LDAP groups to the user roles on the CMS. This controls what level of access different users on the LDAP server will receive on successful login to the CMS.

To configure the CMS's LDAP attributes

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **LDAP** tab.
3. At the **Admin State** drop-down, make sure LDAP authentication is **enabled**.
4. Type in a **Bind DN** (Bind Distinguished Name) and **Bind DN Password** for a set of credentials which has read access to the user store. This is used by the CMS to log into the LDAP server.
5. Set the following LDAP User Attributes to identify users within the user store:
 - **User Name Attribute** – (Default: **sAMAccountName**) The LDAP attribute which contains the user's user-name
 - **Real Name Attribute** – (Default: **cn**) The LDAP attribute which contains the user's real name
 - **Email Attribute** – (Default: **mail**) The LDAP attribute which contains the user's email address
 - **User Base DN** – The Base DN used to locate user information in the LDAP schema
 - **User Search Filter** – Optional filter to restrict user search results to a specific object class
6. Set the following LDAP Group Attributes to identify groups within the user store:
 - **Group Name Attribute** – (Default: **cn**) The LDAP attribute which contains the group's name
 - **Group Mapping Attribute** – (Default: **dn**) The LDAP attribute which references a group member
 - **Group Member Attribute** – (Default: **member**) The LDAP attribute which contains a group member
 - **Group Base DN** – The Base DN used to locate group information in the LDAP schema
 - **Group Search Filter** – Optional filter to restrict group search results to a specific object class
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: To enable your users to log in using UPN formatted names, you can enter a UPN in the **Bind DN** field and type `userPrincipalName` in the **User Name Attribute** field.

CLI Commands



```
configure
edit aaa ldap
set admin-state enabled
set bind-dn <bindDN>
set bind-dn-password <bindDNpassword>
set group-attributes group-base-dn <gBaseDN> group-mapping-attribute
<gMapping> group-member-attribute <gMember> group-name-attribute <gName>
group-search-filter <gFilter>
set user-attributes email-attribute <uEmail> real-name-attribute <uRealName>
user-base-dn <uBaseDN> user-name-attribute <uUserName> user-search-filter
<uFilter>
commit
exit
```

To add an LDAP server

Note: In addition to your primary LDAP server, you can add a backup server. The backup server must have the same Directory Information Tree structure as the primary LDAP server and accept the same bind credentials. You can have a maximum of 2 servers in the LDAP servers list.

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **LDAP** tab.
3. At the LDAP Servers table, click **Add Server**.
4. Type a **Name** for this server.
5. Select the **Connection Type** your LDAP server will use to communicate with the CMS. This will auto-fill the **Port** field with the default port number for your selected Connection Type; the default port for LDAP and Start-TLS is **389**, and the default port for LDAPS is **636**.
6. Type the **Host** IP Address.
7. (Optional) If you're not using the default port, you can edit the **Port** number.
8. Type a value for **Connect Timeout**. This is the maximum number of seconds the CMS is permitted to wait for a network response on connecting.
9. Type a value for **Request Timeout**. This is the maximum number of seconds the CMS is permitted to wait for a network response on sending a request.
10. Click **Save**.

11. If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the LDAP Servers table, you can use the following action buttons to edit  or delete  a server.

CLI Commands

Add an LDAP server

```
configure

set aaa ldap servers <serverName> connect-timeout <cTimeout> connection-type
[ldap|ldaps|start-tls] host <hostIPAddress> port <portNumber> request-
timeout <rTimeout>

commit
```

Edit an LDAP server

```
configure

set aaa ldap servers <serverName> connect-timeout <cTimeout> connection-type
[ldap|ldaps|start-tls] host <hostIPAddress> port <portNumber> request-
timeout <rTimeout>

commit
```

Rename an LDAP Server

Note: Not currently available in the Web UI.

```
configure

request aaa ldap servers <serverName> rename name <newName>

commit
```

Delete an LDAP server

```
configure


delete aaa ldap servers <serverName>



commit
```

To add group role mappings

There are 3 CMS user roles you can map an LDAP group to. User's in a mapped group will have the same permissions as their associated role.

Note: If a user is assigned to multiple LDAP groups, and those groups are mapped to different CMS user roles, the user is assigned the role with the highest level of access. For example, if a user was in an LDAP group mapped to `cns-admin` and one mapped to `cns-defense`, they would receive `cns-admin` access when they log in to the CMS.

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **LDAP** tab.
3. At the Group Role Mapping table, click **Add Mapping**.
4. Type the name of an **LDAP Group** from your user store.
5. Select the **Role** you want to map to that group.
6. Click **Save**.
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Group Role mapping table, you can use the following action buttons to edit  or delete  a group role mapping.

CLI Commands

Add a group role mapping

```
configure
set aaa ldap group-role-mappings ldap-groups <groupName> role [cns-
admin|cns-defense|cns-monitor]
commit
```

Edit a group role mapping

```
configure
set aaa ldap group-role-mappings ldap-groups <groupName> role [cns-
admin|cns-defense|cns-monitor]
commit
```

Delete a group role mapping


```
configure
delete aaa ldap group-role-mappings ldap-groups <groupName>
commit
```

Configuring RADIUS Authentication

There are three main steps to connect an RADIUS server to the CMS:

- Enable RADIUS authentication.
- Select a default role for all users. Use the Filter ID attribute to apply other CMS user roles to specific RADIUS groups.
- Add the connection details for an RADIUS server to the RADIUS Servers list. Optionally add a backup server.

To enable RADIUS authentication

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **RADIUS** tab.
3. At the **Admin State** drop-down, select **enabled**.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).


CLI Commands

```
configure
set aaa radius admin-state enabled
commit
```

To provision RADIUS users with CMS user roles

You can use the CMS to provision a default user role for RADIUS authenticated users. To provision specific RADIUS user groups with other CMS roles, use the Filter ID attribute in group configuration on the RADIUS server. Any users who do not have a Filter ID attribute set, or whose Filter ID is not set to a CMS user role, will receive the default user role.

To set a Default Role for all users

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **RADIUS** tab.
3. At the **Default Role** drop-down, select the CMS user role (**cns-admin**, **cns-defense**, or **cns-monitor**) you want to apply to all RADIUS users without a role specified in their Filter ID attributes. The default value is **cns-monitor**.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

```
configure
set aaa radius default-role [cns-admin|cns-defense|cns-monitor]
commit
```


Note: If you don't explicitly set default role, it will remain the default cns-monitor.



To set other CMS roles for specific RADIUS user groups

When configuring a RADIUS user group, use the Filter ID attribute to provision those users with a specific CMS role. You can use one of the three user role names (cns-admin, cns-defense, or cns-monitor) as the Filter ID.

To add a RADIUS Server

Note: In addition to your primary RADIUS server, you can add a backup server. You can have a maximum of 2 servers in the RADIUS servers list.

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **RADIUS** tab.
3. At the RADIUS Servers table, click **Add**.
4. Type a **Name** for this server.
5. Type the IP **Address** of the server.
6. (Optional) If you're not using the default port (1812), you can edit the **Port** number.
7. Type the **Shared Secret** used to communicate with this server.
8. Click **Save**.
9. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the RADIUS Servers table, you can use the following action buttons to edit  or delete  a server.

CLI Commands

Add a RADIUS server

```
configure
```

```
set aaa radius servers <serverName> address <IPaddress> port <portNumber>
shared-secret <secret>

commit
```

Note: If you don't explicitly set the port number, it will remain the default 1812.

Edit a RADIUS server

```
configure

set aaa radius servers <serverName> address <IPaddress> port <portNumber>
shared-secret <secret>

commit
```

Rename a RADIUS server

Note: Not currently available in the Web UI.

```
configure

request aaa radius servers <serverName> rename name <newName>

commit
```

Delete a RADIUS server

```
configure

delete aaa radius servers <serverName>


commit
```

Setting the Authentication Order

There are three types of authentication available on the CMS: local user database, external RADIUS server, and external LDAP server. If you enable one or both of the external authentication types, you may also need to check you have the correct authentication order for your system.

To configure authentication order


1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **SETTINGS** tab.

3. From the **Order** drop-down, select the order you want users to be authenticated on the CMS:
 - **External, Local** – (Default) A user is first checked against enabled external authentication systems; RADIUS first and then LDAP if both are enabled. If the user is rejected by either, login is denied. If the user does not exist in either, or the servers are unavailable, the user is checked against the local user database.
 - **Local, External** – A user is first checked against the local user database. If the user does not have a local account, or local authentication fails, the user is checked against external authentication systems. If both types of external authentication is enabled, RADIUS is checked first and then LDAP.
4. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Setting Web UI Timeouts

You can set the idle timeout and maximum session duration for the Web UI. This applies to all user types regardless of role or authentication type.

To configure Web UI timeouts for all user types

1. Use the left-hand menu to navigate to **System > Authentication**.
2. Select the **SETTINGS** tab.
3. In the **Web UI Idle Timeout** field, you can set the number of minutes a user can be inactive in the Web UI before they are logged out.
4. In the **Web UI Max Session Duration** field, you can set the maximum number of minutes a user can be active in the Web UI before they are logged out.
5. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Caution: When a user is logged out by one of these settings, any un-committed changes are lost.

Enabling Support Account

To allow a Corero Support Engineer to access your CMS, you need to enable the support account. When you enable the support account you are given an 8-character token that you need to send to the Support Engineer to allow them to log in. Once your issue has been resolved, you can disable the support account if you choose.

Note: Once you enable the support user, you can see the support account in the Users table (System > Authentication). You cannot edit or delete the support user from that table.

To view the current support account status and (if enabled) view the support token

1. Use the left-hand menu to navigate to **System > System Actions**.
2. In the Support Account area, you can see a value next to **Support Token**. If you cannot see this value, you must first enable the support account.

To enable the support account

1. Use the left-hand menu to navigate to **System > System Actions**.
2. Click **Enable**.
3. You can now provide the Corero Support Engineer with the support token. They can use that token to log in as the support user and access high-level settings in the CMS.

Tip: To enable the support account with a specific token, you can enter an 8-character token in the field before you click **Enable**.

CLI Commands

View the current support account status

```
request system support-status
```

Enable the support account

```
request system support-enable  
  
commit
```

Tip: You can disable the support account by using the command `request system support-disable`.

Configuring CMS IP Filter Management


Caution: Once you enable IP filtering, all IP addresses not explicitly allowed will be blocked from accessing the CMS. If you have a SecureWatch Service enabled, you must include the SecureWatch VPN IP address as a permitted management IP address.



To restrict access to the CMS, enable IP Filter management and create a list of permitted IP addresses.

To configure CMS IP Filter management

Note: After enabling IP filters, you must create one or more IP entries before you can commit the updated configuration.

1. Use the left-hand menu to navigate to **System > IP Filters**.
2. From the **Admin State** drop-down, select **enabled**.

3. By default, all ICMP traffic is allowed regardless of source IP. To restrict ICMP traffic to only the permitted IP addresses in the table, from the **Always Allow ICMP** drop-down, select **disabled**.
4. Create a permitted IP address entry:
 1. Click **Add**.
 2. Type the permitted IP **Address** CIDR.
 3. (Optional) Type a description of the entry.
 4. Click **Save**.
5. Repeat to add all the IP Addresses which should be permitted to access the CMS.
6. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Entries table, you can use the following action buttons to edit  or delete  an entry.

CLI Commands

View IP filter management

```
configure
show system ip-filter
```

Configure CMS IP Filter management

```
configure
set system ip-filter admin-state [disabled|enabled]
set system ip-filter always-allow-icmp [disabled|enabled]
set system ip-filter entry <entryIP> description "<description>"
commit
```

Edit an entry's description

```
configure
edit system ip-filter entry <entryIP>
set description "<description>"
commit
exit
```

Delete an entry

```
configure
```

```
edit system ip-filter  
delete entry <entryIP>  
commit  
exit
```

Snapshots

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Snapshots Screen reference topic](#).

A snapshot is a package file containing the configuration of the CMS at the moment you create it. You can create one at any time and store multiple snapshots in the CMS. You may want to take a snapshot before you make a large configuration change so you have the option to restore the previous settings.

Note: The Snapshots screen is only visible for **cns-admin** users.

If you choose to restore a snapshot, it deletes the current CMS configuration and replaces it with the saved copy. This excludes the snapshot list, which does not change. This enables you to move back and forth between snapshots. When you restore a snapshot, you also have the option to exclude the user authentication information enabling you to restore the previous configuration without overwriting the user information which may have changed since then.

Caution: Restoring any snapshot will also deactivate all [RTBH instructions](#) in the RTBH DIP table. You can [manually reactivate](#) them as needed or wait for new [automatic triggers](#) to populate the table.

Scheduled backups

The CMS can be configured to create and store a snapshot automatically on a daily or weekly basis. At the time specified, the CMS creates a backup file (.zip) which can contain a snapshot of the current configuration and the CMS log files up to that time. This backup file is stored on a specified location of a remote server.

When the backup file is created, you can choose to store a copy of the snapshot in the CMS snapshot list. You can identify backup snapshots in the list from their auto-generated name which includes the date and time the snapshot was created (e.g. "cms-backup_cms_2017-12-06-05:00:00") and the description which is "Scheduled backup". By default, the CMS stores 10 backup snapshots at a time and will delete older backup snapshots to make room for new ones. It will never delete a manual snapshot to make room for a backup snapshot. You can change the number of stored snapshots using the CLI.

Snapshooting your CMS Configuration

Caution: Snapshots are version specific. After you upgrade the CMS, you will not be able to use any saved snapshots from the previous version. The snapshots remain available in the CMS after an upgrade to enable you to export them if needed.

Periodically, or before you perform a large configuration change, you may want to create a snapshot of the CMS's configuration.

To create a snapshot

1. Use the left-hand menu to navigate to **System > Snapshots**.
2. Click **Create**.
3. Type a **Name** for your new snapshot.


Caution: Snapshot names cannot contain any spaces. Only alphanumeric or .-&()_: symbols.

4. (Optional) Type a **Description** of the snapshot.
5. Click **Save**.

Tip: On the Snapshots table, you can delete  snapshots you no longer need.

To restore CMS configuration from a snapshot


If you want to return to a previous CMS configuration, you can restore an earlier snapshot. Restoring a snapshot does not erase your later snapshots, enabling you to move between snapshots to investigate configuration changes.

1. Use the left-hand menu to navigate to **System > Snapshots**.
2. From the table, locate the snapshot you want to restore and click  the restore button. You can type a text string into the Search field to narrow down the list.
3. Confirm snapshot restore, click **OK**.

Caution: Restoring a snapshot will cause the CMS to restart.

To export your saved configuration

You can export your snapshots to store externally or use with another CMS application. If you choose to password protect a snapshot, you must provide this password when you import the snapshot.

1. Use the left-hand menu to navigate to **System > Snapshots**.
2. From the table, locate the snapshot you want to export and click  the export button. You can type a text string into the Search field to narrow down the list.
3. (Optional) If you want to password protect the snapshot, type in a **Password**.
4. Click **OK**.
5. The snapshot package file is downloaded by your browser.

To import CMS configuration

You can import snapshots you have exported from other CMS applications or which you exported from this CMS application to store externally. Once you import a snapshot you can view it in your snapshot list and use it like any other.

1. Use the left-hand menu to navigate to **System > Snapshots**.
2. Click **Import**.
3. Select the snapshot on your computer and click **Open**.
4. (Optional) If the snapshot is password protected, type in the **Password**.
5. Click **OK**.

CLI Commands

Create a snapshot

```
request snapshots create name <snapName> description "<snapDescription>"
```

Rename a snapshot

Note: Not currently available in the Web UI.

```
configure
request snapshots snapshot <snapName> rename name <newName>
commit
```

Restore a snapshot

```
request snapshots snapshot <snapName> exclude-aa [false|true]
```

Note: In the CLI, you can choose not to overwrite the current authentication information when you restore a snapshot by adding `exclude-aa true`. For local snapshots, you will not see the options to `restore disable-connections`.

Export a snapshot

```
request snapshots snapshot <snapName> export remote-uri <remoteUri> remote-
password <remotePassword> snapshot-password <snapPassword>
```

Import a snapshot

```
request snapshots import remote-uri <remoteUri> remote-password
<remotePassword> snapshot-password <snapPassword>
```

Scheduling Backups

You can use the CLI to create backup files daily or weekly which are stored in a remote server. Backup files can contain a snapshot and the CMS logs. When a backup file with a snapshot is created, the snapshot can also be saved to the CMS.

Tip: You can generate unscheduled backups immediately, in case you need backup the CMS before a large configuration change, or if you need to test the backup process.

To configure how often the CMS creates backup files (CLI only)

You can configure a scheduled back in using one full command. For example, the following command sets up a scheduled backup which runs at 8am every day and includes log files but doesn't include snapshots.

Tip: You can upload scheduled backups to an FTP or SFTP server. This is defined in the command. The examples below use SFTP (e.g. `sftp://<username>@<serverIP>`) but you can also choose to use FTP (e.g. `ftp://<username>@<serverIP>`).

```
configure
```

```
set system backup backup-state enabled remote-uri sftp://<username>@<serverIP> remote-
password <remoteServerPassword> include-log-files true include-snapshots false
frequency daily hour-to-run 08:00
```

```
commit
```

Or you can use the edit command to focus on a specific part of the scheduled backup configuration:

```
configure
```

```
edit system backup
```

```
set backup-state enabled
```

```
set remote-uri sftp://<username>@<serverIP> remote-password <remoteServerPassword>
```

```
set include-snapshots include-log-files
```

Note: You can choose to `include-snapshots` or `include-log-files`, or both. If you do not specify what to include, the backup is created with a snapshot and no log files.

```
set frequency [daily|weekly] day-to-run
[friday|monday|saturday|sunday|thursday|tuesday|wednesday] hour-to-run <hour_
e.g.18:00>
```

Note: If you choose `daily`, you do not have to specify `day-to-run`. If you do not specify a frequency, the backup will run at 00:00 daily. If you specify `weekly`, but then do not specify a day or time, it will run every Saturday at 00:00.

```
set number-of-snapshots <number>
```

Note: This is the number of backup snapshots the CMS will store at one time. Once that number of backup snapshots exist, the CMS will delete older backup snapshots to make room for new ones. If you don't want the CMS to store any backup snapshots, use 0.

```
commit
```

```
exit
```


Tip: To stop the scheduled backups, set the backup-state to disabled.

To create an unscheduled backup file

If you want to immediately create a backup file, rather than wait for the next scheduled time, you can do that with the following CLI command:

```
request system backup execute
```

To revert to a snapshot from backup file

If a backup snapshot is stored in the CMS, you can restore the snapshot as you would any other from the snapshot list. If you want to restore a snapshot stored on your remote server, you must:

1. On the server, unzip the backup file containing your snapshot.
2. In the CMS CLI enter the following commands (where `remote-uri` now includes the snapshot file name):

```
request snapshots import remote-uri <remoteServerLocation> remote-password
<remoteServerPassword>
request snapshots snapshot <snapshotName> restore exclude-aa [false|true]
```

CMS Software

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Software Upgrade Screen reference topic](#). See the devices area for information on [upgrading a device](#).

You can upgrade the CMS from within the application. Once you receive an upgrade package file from Corero customer support, you can upload it to the CMS to perform the upgrade without losing your current CMS configuration. When you upgrade the CMS, you may also need to upgrade your Defense device; you must always upgrade the CMS before upgrading associated devices.

When you upgrade the software on the CMS, it creates a rollback point at the moment before upgrade which enables you to undo that software upgrade and return the CMS configuration to the state it was in prior to upgrade. When you rollback a software update, you lose any changes made since you updated the software. This includes: Policy changes, system configuration changes, device management changes, and any newer rollback points in the installed software list.

Caution: Unlike a snapshot, once you rollback a software upgrade, you cannot then "roll forward" to another saved state.

Upgrading the CMS Software Version


When a new version of the CMS software becomes available, you should receive an upgrade package file from your Corero representative.

Caution: The CMS will restart during the upgrade process.

Prerequisites

- Save the upgrade package file locally
- In SmartWall SecureWatch Analytics, check that there are no ongoing network anomalies
- [Check that all devices are in-sync](#) and all status bar icons in the CMS are green
- Check that you have no outstanding changes to commit

To upgrade the software on the CMS

1. Use the left-hand menu to navigate to **System > Software Upgrade**.
2. Make sure the **CMS** tab is selected.
3. At the Software Pending Upgrade table, click **Upload**.
4. Select a CMS upgrade package file and click **Open**.
5. In the Software Pending Upgrade table, locate the version you want to upgrade the CMS to and click  the upgrade button. You can type a text string into the Search field to narrow down the list.
6. Click **OK**. The CMS will now restart and you will be logged out.

- Once the application has restarted, log back in and check the software version displayed at the top of the Home screen.

Note: If the CMS is unable to validate a successful upgrade, it will automatically rollback to the previous version. If you are unable to complete an upgrade, contact your support representative.

CLI Commands

```
request system software upgrade remote-uri <packageLocation+FileName>
remote-password
<password>
yes
```

Next Steps

[Upgrade the devices](#) connected to this CMS

Caution: Do not upgrade a device without first upgrading the CMS to that version. If you do not first upgrade the CMS, you will not be able to reach your upgraded device from the CMS.

Rolling Back to an Old CMS Software Version


When you upgraded the CMS software, the system created a rollback point enabling you to return the CMS to the state it was in when the upgrade was performed. When you rollback a software update, you lose any changes made since you updated the software (including any snapshots or uploaded upgrade packages).

Caution: The CMS will restart during the rollback process.

Prerequisites


- In SmartWall SecureWatch Analytics, check that there are no ongoing network anomalies
- [Check that all devices are in-sync](#) and all status bar icons in the CMS are green
- Check that you have no outstanding changes to commit

To rollback the software version on the CMS

- Use the left-hand menu to navigate to **System > Software Upgrade**.
- Make sure the **CMS** tab is selected.
- In the Old Software Versions table, locate the version you want to rollback to and click the  rollback button.

You can type a text string into the Search field to narrow down the list.

4. Click **OK**. The CMS will now restart and log you out.

Note: You can delete old versions from this table using  the delete button. This also deletes the saved CMS configuration associated with this software version. You will be unable to rollback to this version once you delete.

CLI Commands

Roll back CMS software to an older version

```
request system software installed <versionNumber> rollback
yes
```

Delete an old software version

```
request system software installed <versionNumber> delete
yes
```

SNMP

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [SNMP Screen reference topic](#).

You can use the CMS SNMP (Simple Network Management Protocol) to collect information and view alerts from your SmartWall devices, using your own network management system.

Supported SNMP versions

The CMS supports version 2c and version 3 SNMP. You can enable both versions at the same time, or just enable the version you plan to use.

The versions require different authentication information:

- For version 2c, you need to provide a Community string. The default string is `smartwall`.
- For version 3, you can create a list of users. For each user, you can choose to set an authentication protocol (md5 or sha) and with a password, and an authentication privacy (aes or des) with a password. Additionally, version 3 requires an Engine ID to identify the system. By default, this is 27 characters of your CMS UUID but you can provide a different ID.

SNMP traps

If you want to send alerts to other locations in your network, you can create SNMP traps. A trap sends a CMS or device alert to a specified IP address in your network. If you are using v3 SNMP, you also have the option to send

inform type traps. These require the SNMP trap receiver to acknowledge the alert within 1.5 seconds otherwise it re-sends up to 3 more times.

CMS MIBs


You can download the CMS MIB files from the support portal. For more information on using the MIB files and a reference table of OIDs, see the CMS User Guide PDF reference information.

Configuring the CMS SNMP Settings

Once you set the general SNMP settings and enable SNMP for the CMS, you can choose to enable version 2c and/or version 3 SNMP. If you need to disable SNMP, you can use the **Admin State** drop-downs to disable SNMPv2c, SNMPv3, or all SNMP for the CMS using the **Admin State** drop-down under General Settings.

Note: If the **Admin State** drop-down under General Settings is set to **disabled**, even if SNMPv2c or SNMPv3 is individually set to enabled, SNMP for the CMS is turned off. To enable SNMPv2c or SNMPv3 you must also enable SNMP under General Settings.

To configure the general SNMP settings and enable SNMP for the CMS

1. Use the left-hand menu to navigate to **System > SNMP**.
2. Under General Settings, set the **Admin State** drop-down to **enabled**.
3. The default UDP port for SNMP communication is 161. To change this, edit the **UDP Port** field.
4. Type a **System Name** for the CMS.
5. Type a **System Location** for the CMS. This can be any text string, for example, the city you're located in, or a building name.
6. Type a **System Contact** email address. This should be someone able to manage the CMS SNMP settings.
7. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).



To enable v2c SNMP

Note: Once you enable SNMP, v2 is automatically enabled with a community called `smartwall`. Use the following instructions to edit those settings or re-enable v2 SNMP after you previously disabled it.

1. Use the left-hand menu to navigate to **System > SNMP**.
2. Make sure that SNMP is enabled for this CMS and all General Settings fields are filled out.
3. Under SNMPv2c, set the **Admin State** drop-down to **enabled**.
4. The default community string is `smartwall`. To change this, type a new string in the **Community** field.

- If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

To enable v3 SNMP

- Use the left-hand menu to navigate to **System > SNMP**.
- Make sure that SNMP is enabled for this CMS and all General Settings fields are filled out.
- Under SNMPv3, set the **Admin State** drop-down to **enabled**.
- You need to create at least one user, but you can create as many as you require. Once you've created your users, you can use the  edit and  delete buttons to manage your user list.
 - At the SNMP users table, click Add.
 - Type a **Name** for this user. The name must be unique.
 - (Optional) Select an Authentication type (MD5 or SHA) and provide a password.
 - (Optional) Select an Privacy type (AES or DES) and provide a password. You can only select a Privacy type if you have an Authentication type selected.
 - Click **Save**.

Once you've created your users, you can use the  edit and  delete buttons to manage your user list.

- If you want to save the new configuration, and push your changes to any affected Defense devices, click **Commit**. Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

CLI Commands

Configure general SNMP settings for the CMS

```
configure
set system snmp admin-state [disabled|enabled] system-contact
<systemContact> system-location <systemLocation> system-name<systemName>
udp-port <portNumber>
commit
```

Enable SNMP v2

```
configure
set system snmp v2c admin-state enabled community <communityString>
commit
```

Enable SNMP v3c

```
configure
set system snmp v3 admin-state enabled user <userName>
```

Note: You can create as many users as you require. Once you create the user, setting **auth** and **priv** for that user is optional. You can choose to set both, neither, or only **auth**.

```
edit system snmp v3 user <userName>
set auth [md5|sha] <authPassword>
set priv [aes|des] <authPassword>
commit
```

Tip: v3 SNMP requires an engine ID for the system. By default this is 27 characters of your CMS UUID (see the [Home screen](#) to view this number). If you want to change this engine ID use the following command: `set system snmp v3 engine-id <idNumber>`


Managing SNMP trap destinations



You can create an SNMP trap for each destination in your network to which you want the CMS to send alert messages.

Prerequisites

Before you can set up trap destination, you must first [configure SNMP](#) for your network.

To add an SNMP trap destination

1. Use the left-hand menu to navigate to **System > SNMP**.
2. Under **Trap Destinations**, click **Add**.
3. Type a **Name** to identify the target destination.
4. Type the **IP Address** of the target destination.
5. Type the UDP **Port** number you want to use for communications.
6. Select the **SNMP Version** you are using for this trap:
 - **SNMP v2C** – Type your **Community** string
 - **SNMP v3** – Select whether this is a **Trap** or **Inform** and select an **SNMP User**
7. Click **Save**.
8. If you want to save the new configuration, and push your changes to any affected Defense devices, click . Then, on the pop-up dialog, click **Commit** to push the changes (alternatively, you can click **Discard** to discard any uncommitted changes).

Tip: On the Trap Destinations table, you can use the following action buttons to edit  or delete  a trap destination.

CLI Commands

Add a new SNMP trap destination

```
configure

set system snmp trap-destinations <trapName> address <ipAddress> udp-port
<portNumber> [v2c|v3]
```

Note: For v3 only: notification type `[inform|trap]` user `<userName>`
security `[auth-no-priv|auth-priv|no-auth-no-priv]`

```
commit
```

Edit an existing trap destination

```
configure

edit system snmp trap-destinations <trapName>
```

Tip: Use the `set` command to edit the `address`, `udp-port`, `v2c`, or `v3` information.
Use the `delete` command to remove an existing `udp-port` or `v3` notification-type.

```
commit
```

Rename a trap destination

Note: Not currently available in the Web UI.

```
configure

request system snmp trap-destinations <trapName> rename name <newName>

commit
```

Delete an existing trap destination

```
configure

edit system snmp trap-destinations

delete <trapName>

commit
```


CMS Licenses for vNTD

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Licensing Screen reference topic](#).

Note: The Licensing screen is only visible for **cns-admin** users.

If you intend to use SmartWall Network Threat Defense Virtual Edition (vNTD) devices, you must have corresponding vNTD license capacity on the CMS.

If you do not have the required license capacity, you must contact your Corero representative . Licenses are created in increments of 10Gbps; you need 10Gbps license capacity for each vNTD you want to connect to a CMS.

If you have enough available license capacity, when you add a new vNTD the CMS automatically licenses it and you can add the device to a Cluster. However, if you do not have enough spare license capacity, the CMS adds the device to the Devices table but it will transition to a not-licensed state.

When a device is in the not-licensed state, it is unable to receive any further configuration updates from the CMS and will continue to enforce the last policy it received. Devices in the not-licensed state do not send any information via syslog, except for the device status messages. If you later add a new license to the CMS with additional capacity, you can then license the device manually.

When you remove a device from the CMS, it is automatically delicensed and its license capacity becomes available for another vNTD to use. If you have a vNTD which you don't currently want to use, you can delicense it without deleting it and free up that license capacity. A delicensed device returns to the not-licensed state.

For time-based licenses, you can see the license expiring date in the licenses table (System >Licensing). You should purchase and upload a new license before that date. If you are unable to, you will have a grace period after the expiry date, where the vNTD will continue to mitigate attacks.

Viewing License Capacity

Before you add a new vNTD to your CMS, you may need to check that you have enough license capacity available. You need 10Gbps of available license capacity for each vNTD you want to connect to a CMS.

Note: The number of cores allocated to a vNTD device does not affect the license capacity required to license a device. All devices require 10Gbps.

To view the available license capacity

1. Use the left-hand menu to navigate to **System > Licensing**.
2. Above the Licenses table, there are two values displayed:
 - **Total Capacity** – The total available capacity of all your uploaded licenses
 - **In-use** – The license capacity currently allocated to licensed vNTDs

Note: Licenses are associated with the CMS rather than with the vNTD. When you remove a vNTD from one CMS and add it to a new CMS, the license is not transferred. You must have adequate available license capacity in the new CMS to manage the vNTD.

CLI Commands

```
show system licenses
```

Note: You can see each license's available capacity in the table.

Adding a vNTD License

Before you can use SmartWall Network Threat Defense Virtual Edition (vNTD) devices, you must have a vNTD license on the CMS. Licenses have a total available capacity; you need 10Gbps of available capacity to license a new vNTD. If you have less than 10Gbps available you will need to add an additional license.

Prerequisites

1. Contact your SmartWall CMS User Guide representative for an additional license. You will need to provide your CMS UUID. You can find this at the top of the [Home screen](#) or using the following CLI command: `show system uuid`
2. When you receive the license from Corero, save it locally.

Note: Licenses are CMS specific and cannot be transferred or used on multiple CMS applications.

To add a vNTD license to the CMS

1. Use the left-hand menu to navigate to **System > Licensing**.
2. Click **Add**.
3. Either:
 - Select **Copy & paste license** and copy the contents of the license into the field. You must include the license header and footer: `---BEGIN-CORERO-LICENSE---` and `---END-CORERO-LICENSE---`
 - Select **Upload license file** and click **Choose file**. Select the license file you want to import and click **Open**.
4. Click **Save**.

Caution: If the selected license is not configured for this CMS, it will display in the table as invalid and you will not be able to use the additional license capacity.

CLI Commands

```
request system licenses import remote-uri <licenseLocation+FileName> remote-
password
<password>
yes
```

Next steps

- You can now [view the available license capacity](#).
- [License an unlicensed vNTD](#)

Note: If you add a new vNTD to the CMS, when there is adequate available license capacity, it is automatically licensed. If you add a vNTD to the CMS when there isn't enough capacity it will remain in an unlicensed state until you manually license it.

Licensing/delicensing a vNTD

When you add a vNTD to the CMS, if there is enough license capacity available, it will be automatically licensed by the CMS. If you do not have enough capacity, the device is still added but it won't be licensed. When you have available license capacity you must manually license the vNTD. One way to create license capacity is to delicense old vNTDs you're no longer using.

Caution: When you delicense a vNTD or add it to the CMS when there isn't enough license capacity available, it enters the not-licensed state. In the not-licensed state, the device is unable to receive any further configuration updates from the CMS and will continue to enforce the last policy it received. Devices in the not-licensed state do not send any information via syslog message except the device status.

Prerequisites

- [Add a vNTD to the CMS](#)
- [Add a vNTD license to the CMS](#)
- To license a vNTD, you must have at least 10Gbps available license capacity on the CMS

To license a vNTD

Note: You can only license a vNTD which is in the not-licensed state.

1. Use the left-hand menu to navigate to **Network > Devices**.
2. On the Devices table, locate the vNTD you want to license or delicense.
3. In the Actions column, click ******* and select **License** or **Delicense**.

SSH Keys

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [SSH Keys Screen reference topic](#).

SSH Keys for Authentication Groups

For some deployment of SmartWall Network Threat Defense Virtual Edition devices, it is possible to authenticate using SSH keys rather than device username and password.

Note: For instructions on adding SSH Keys to vNTDs, contact your Corero representative.

SSH Keys for authenticating Remote devices


SmartWall Threat Defense Director deployments leverage certain edge routers to pre-filter DDoS attacks, at the perimeter. The authentication credentials for connecting to these edge routers is stored in the CMS and can either be Password or an SSH Key authentication. SSH Keys must be stored in the Keys table.



Note: See your SmartWall TDD User Guide for more information about using the CMS for TDD deployments. Alternatively, contact your support representative to find out more about SmartWall Threat Defense Director.

Importing an SSH Key

If you want to use an SSH key to authenticate that connection, you must store the key in the CMS. SSH Keys can be used in [Authentication Groups](#) to authenticate vNTD Defense devices or in [Remote Mitigation](#) to authenticate Remote devices.

To import an SSH Key

1. Use the left-hand menu to navigate to **System > SSH Keys**.
2. At the table, click **Import**.
3. Type a **Name** for this key. You must only use alphanumerics, spaces, or .-&()/_/@:= symbols.
4. Add an SSH key by either:
 - **Copy & paste SSH Key text** into the field. This must be in PKCS#8 format.
 - Or **Upload SSH Key file** by clicking Choose File and selecting an SSH key file from your local computer.
5. (Optional) Type a **Key Passphrase** for this SSH Key.
6. Click **Save**.
7. Click . Then, on the pop-up dialog, click **Commit** to push the changes.

Tip: On the devices table, you can use the following action buttons to edit  or remove  a remote device.

CLI Commands

Import an SSH Key

```
configure
set aaa ssh private-key <keyName> key-data <SSHkeyText> passphrase
<keyPassphrase>
commit
```

Note: The `key-data` must be valid binary data for the private key, in PEM format (text starting with '-----BEGIN DSA PRIVATE KEY-----' or '-----BEGIN RSA PRIVATE KEY-----').

Remove an SSH Key

```
configure
delete aaa ssh private-key <keyName>
commit
```

Support Tasks

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [System Actions Screen reference topic](#). See the Users area for information on [enabling the Support account](#).

Note: The System Actions screen is only visible for **cns-admin** users.

The tasks in this section are usually only undertaken if you encounter problems with the CMS and are asked to perform some troubleshooting tasks by a Corero Support Engineer.

Viewing the Audit Log

The CMS records every action and which user account performed that action. You can use the CLI to view this audit log.

Tip: Alternatively, you can use SmartWall SecureWatch Analytics to view the audit log in a series of log messages. To do that use the Search screen to perform the following search: `index=*source=/var/log/corero/audit.log`.

To view the audit log in the CLI

```
request log view name audit
```

Reading the Audit log

After the time and date of the action, each audit log message has the following fields:

- **address** – The IP address the user accessed the CMS from
- **if** – Whether the action was performed using the CLI or Web UI interface
- **user** – The username of the user account who performed the action
- **sid** – The session ID for this session (this changes every time you log out)
- **op** – The operation performed, e.g. log-in, start-session, set, create, etc
- **tid** – If applicable, the transaction ID for the changes made in this commit
- **path** – If applicable, the model path to the option what was changed or action requested
- **value** – If applicable, the new value for the changed option
- **msg** – If applicable, the message associated with the action. This most commonly in the either "action invoked with parameters [...]" to log the request for an action, or "action completed with result [...]" to log the result of the action.

For example, these two log entries show first, the user requesting to download the diagnostics package from a device, and second, the successful result of that request:

```
<INFO> 2017-05-11T06:23:24.344-
04:00,address=10.10.11.12,if=cli,user=admin,sid=172,op=action,path=/file-copy/from-
```



```
device,msg="action invoked with parameters [file:'diagnostics-package', remote-
uri:'sftp://user@10.10.11.12/issues/ntd-test-diag.zip', remote-password:'****',
device-name:'ntd-1']",
<INFO> 2017-05-11T06:23:41.783-
04:00,address=10.10.11.12,if=cli,user=admin,sid=172,op=action,path=/file-copy/from-
device,msg="action completed with result [result:'Success', message:'Copy
succeeded']",
```

Downloading Diagnostic Files

Tip: For information on specific fields, tables, or buttons in the Web UI, see the [Diagnostics Screen reference topic](#).

A Corero Support Engineer may ask you to download the CMS or device diagnostic log files when they are troubleshooting an issue.

Note: This feature is only available for defense and admin users.

To download a CMS diagnostic file

1. Use the left-hand menu to navigate to **System > Diagnostics**.
2. Under **Download file from CMS appliance**, use the **Source** drop-down to select a file to download:
 - diagnostics-package
 - app-log
 - audit-log
 - system-log
3. Click **Download File**.
4. A zip file will download in your browser.

To download a device diagnostic file

1. Use the left-hand menu to navigate to **System > Diagnostics**.
2. Under **Download file from device**, use the **Source** drop-down to select a file to download:
 - me-log
 - diagnostics-package
3. From the **Device** drop-down, select the device you want to download a log file from.
4. Click **Download File**.
5. A zip file will download in your browser.

CLI Commands

Download CMS diagnostics file

```
request file-copy from-cms file [app-log|audit-log|diagnostics-
package|system-log] remote-uri <remoteUri> remote-password <remotePassword>
```

Tip: The remote-uri must end with **.zip**.

Download a device diagnostics file

```
request file-copy from-device file [diagnostics-package|me-log] device
<deviceName> remote-uri <remoteUri> remote-password <remotePassword>
```

Tip: The remote-uri must end with **.zip**.

Restarting the CMS

You can restart the CMS application if you encounter any problems.

Caution: You will be logged out of the CMS and lose any uncommitted changes.

To restart the CMS

1. Use the left-hand menu to navigate to **System > System Actions**.
2. Click **Restart**.
3. Once the CMS restarts, you can log back in.

CLI Commands

```
request system restart
yes
```

Resetting the CMS to the Default Configuration

You can reset the CMS's configuration to factory defaults. This does not reset the underlying CMS application settings (e.g. the CMS IP address) but does return all options, configurable in the Web UI, to their default state.

Caution: When you reset the CMS, you will lose connection with the rest of your SmartWall Threat Defense Director. You must re-add your SmartWall devices and reconnect to the SWA.

To reset the CMS

1. Use the left-hand menu to navigate to **System > System Actions**.
2. Click **Reset**.
3. Once the CMS restarts, you can log back in.

CLI Commands

```
request system reset
yes
```

Next Steps

- [Add your Defense devices to the CMS](#)
- [Connect the CMS to SWA](#)
- [Create a Protection Profile](#)
- [Create a Cluster](#)

SECTION 5

Reference

This section of the CMS User Guide provides reference material to aid in your use of the CMS.

This section discusses the following:


Rules Reference	207
To open the CMS built in help	207
CMS Alarms and SNMP Trap Notifications	207
SNMP Trap Notifications	212
SNMP MIBs	213
Viewing a Corero MIB	213
OID numbers	215
CMS Web User Interface	232
To open the CMS built in help	232

CMS CLI Overview	232
Accessing the CLI	232
CLI Modes	232
View possible completions	232
Commit a change	233
Example: Using Set and Commit commands to Add a new NTD120 and NBA pair	233
Using pipes	234
Viewing tables	235
Example: Using the show command and pipes to view device information	235
pCLI Overview	239
Accessing the pCLI	239
Using the pCLI	239
pCLI Commands	239
CMS REST API Overview	249
Using the REST API	249
Accessing the REST API documentation	253
REST API Examples	255

Rules Reference


For reference information on all the Rules which make up your Defense Policy, including Rule numbers and descriptions, see your built in CMS help.

To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

CMS Alarms and SNMP Trap Notifications

In the SmartWall Threat Defense Director (SmartWall TDD), an alarm is created when something happens which may require your attention. The alarm tells you what has occurred and where in the system it happened (for example, on a specific device). You can use the alarm to investigate any unexpected issues. Once a system has returned to the expected state, the alarm will clear.

You can view your alarms by clicking  the Alarm symbol the Status bar. If the symbol is green, you have no uncleared alarms; if it is orange, an alarm has not yet cleared and may require your attention.

Note: Alarms can also be generated when a previous alarm state has cleared.

Severity	Alarm type	Problem	Alarm Text	What has happened
Critical	CMS alarm	Internal Error	Application timeout. A CMS restart is required.	The CMS application has gotten into a bad state. Restart the CMS.
Warning	CMS alarm	Rollback Error	Various messages (failure reason)	An error occurred while reverting to a previous software version
Warning	CMS alarm	Snapshot Error	Failed to load configuration on startup	An error occurred while loading a snapshot
Warning	CMS alarm	CMS Upgrade	The CMS upgrade was unsuccessful	CMS upgrade has failed
Critical	Analytics alarm	Splunk Universal Forwarder	Splunk Universal Forwarder is not running	Syslog is not being forwarded to the SWA

Severity	Alarm type	Problem	Alarm Text	What has happened
Warning	Analytics alarm	SecureWatch Analytics Connection	No analytics or syslog server has been configured and enabled	You haven't set up an Analytics or Syslog Server in the CMS
Critical	Resource alarm	Low disk space	Path /var/log/corero, free (bytes): <space>	The CMS appliance has low free disk space
Critical	Resource alarm	CPU	Number of CPU cores available (<cores> cores) is below the recommended limit of <core> cores.	The CMS appliance does not have the required number of CPU cores
Critical	Resource alarm	Memory	RAM size under threshold, current size: <memory> GB (<memory> MB), recommended is<memory> GB."	The CMS appliance does not have the recommended system memory
Critical	Resource alarm	Java	Java version: Error, Got: <version>, Expected Oracle java 1.8	The CMS appliance does not have the required Java version installed
Critical	Resource alarm	Filesystem	Maximum number of file descriptors(<descriptors>) is under the recommended limit (<descriptors>).	The CMS appliance file system does not have enough file descriptors
Warning	Resource alarm	SXOS	SXOS Version: No SXOS file found	Unable to determine operating system version on the CMS appliance
Warning	Resource alarm	SXOS	SXOS Version: Wrong version: <version>, expected one of <version>	Incorrect operating system version found on the CMS appliance
Critical	Resource alarm	Apache	Apache httpd: Not running	Apache is not running on the CMS appliance
Warning	Resource alarm	High System Load	System load average over last minute too high: <load>	The CMS appliance is experiencing high system load

Severity	Alarm type	Problem	Alarm Text	What has happened
Warning	Resource alarm	High Memory Usage	Current memory available (total): Swap:<memory> MB (<memory> MB), Ram:<memory> MB(<memory> MB)"	The CMS appliance is experiencing high memory usage
Warning	Device status alarm	Deployment State	Various messages showing deployment state issue	Deployment state of device is not in-sync
Major	Device upgrade alarm	Device Upgrade	Various messages (failure reason)	Device upgrade has failed
Critical	Device status alarm	CMS Address	Device '<device>' has wrong <CMS> address <CMS IP> (expected <CMS IP>)	The CMS address the device is sending information to is incorrect.
Warning	Device Alarm	Device Type Configuration	<Defense/Bypass> device misconfigured as a <bypass/defense> device	The device type set in the CMS does not match the actual device.
Warning	Device Alarm	Restart Reason	Operating System was restarted	(NTD120 only) The device's operating system was restarted for an identified reason
Warning	Device Alarm	Restart Reason	Unknown (could not retrieve restart reason)	(NTD120 only) The device's operating system was restarted for an unidentified reason
Warning	Device Alarm	Restart Reason	Application was restarted	(NTD120 or NBA only) The device application was restarted
Major	Device Alarm	System Boot	<device> is rebooting	The device has been commanded to reboot
Major	Device Alarm	System Boot	<device> is restarting	The device is currently restarting



Severity	Alarm type	Problem	Alarm Text	What has happened
Major	Device Alarm	Auto Bypass Engaged	Various messages (reason)	Automatic Bypass has engaged and traffic is being routed through the Bypass device/module to the internal network without inspection.
Major/ Warning	Device Alarm	Link Down	Various messages (reason)	A link on the device is down (Warning if it is caused by an admin state and Major if it wasn't)
Major	Device Alarm	File_Xfer	Failed to transfer file <file name>	A file transfer to or from the device has failed (e.g. pulling diagnostic files)
Major	Device Alarm	Factory Reset	Resetting management interface configuration	The device is undergoing a factory reset on management interface configuration only
Major	Device Alarm	Factory Reset	Resetting policy configuration	The device is undergoing a factory reset on policy configuration only
Major	Device Alarm	Factory Reset	Resetting policy configuration	(NTD-120 only) The device is undergoing a factory reset on all configuration
Major	Device Alarm	Firmware	Upgrading firmware <filename>	(NTD-120 or NBA only) The firmware is being upgraded
Major	Device Alarm	Firmware	Firmware upgrade has failed, see logs	(NTD-120 or NBA only) The firmware upgrade failed, you can find the reason in the log files
Major	Device Alarm	Firmware	Firmware upgrade failed (<error code>)	(NTD-120 or NBA only) The firmware upgrade failed due to a recognized error
Warning	Device Alarm	License Update	Received new license file <file>	(NTD-120 only) A new device license file has been sent to the device
Critical	Device Alarm	Packets Dropped	Not all packets are recorded.	(NTD-120 only) PCAP line monitoring has identified packet drops

Severity	Alarm type	Problem	Alarm Text	What has happened
Major	Device Alarm	Repository Full	Query results repository is full	(NTD-120 only) PCAP line monitoring has identified the query results repository is full
Major	Device Alarm	Power Supply <A B>	Power Supply <A B> is down	(NBA only) Power supply A or B has gone down
Warning	Device Alarm	PSoC Image	Loading PSoC image <file>	(NTD-120 only) PSoC file is currently being loaded to the device
Major	Device Alarm	PSoC Image	Failed to install image <file> (<error code>)	(NTD-120 only) PSoC file did not install correctly due to an identified error
Major	Device Alarm	Sensor <sensor> reading too high	<sensor> reading too high - <reading>	(NTD-1100 only) An environmental sensor is reporting too high a reading
Major	Device Alarm	Sensor <sensor> reading too low	<sensor> reading too low - <reading>	(NTD-1100 only) An environmental sensor is reporting too low a reading
Critical	Device Alarm	commit-through-queue-failed > [number]	Commit queue item [number] has failed: [device_name]:transport closed	The connection between the CMS and the device isn't working and the commit has failed. Check device credentials and IP address are correct.
Major	Device Alarm	abort-error	[device-name]: transport closed	The connection between the CMS and the device isn't working. Check device credentials and IP address are correct.
Major	Device Alarm	connection-failure	Failed to connect to device NTD-2: host is unreachable	The connection between the CMS and the device isn't working. Check device credentials and IP address are correct.

Severity	Alarm type	Problem	Alarm Text	What has happened
Major	Device Alarm	connection-failure	Failed to connect to device NTD-2: connection refused	The connection between the CMS and the device isn't working. Check device credentials and IP address are correct.

SNMP Trap Notifications

When an alarm is triggered, you can configure the CMS to send SNMP trap notifications to specific locations in your network. The following table shows the possible alarms which the CMS can generate. When the alarm is translated into an SNMP trap it uses the same information fields. For example, if a device is restarting it sends an alarm which looks like this in the CMS:

Major	False	15 Nov 2017, 16:03 PM	ntd-1	/ncs:devices/ncs:device[ncs:name='ntd-1']	cms-alarm:device-alarm	System Boot	NTD is rebooting		
-------	-------	-----------------------	-------	---	------------------------	-------------	------------------	---	---

Where you can see:

- Severity is **Major**
- Device name is **ntd-1**
- Object path is **/ncs:devices/ncs:device[ncs:name='ntd-1']**
- Alarm type is **cms-alarm:device-alarm**
- Problem is **System Boot**
- Alarm Text is **NTD is rebooting**

An SNMP trap created by this alarm would look something like this:

```
SNMPv2-MIB::snmpTrapOID.0 = OID: TAILF-ALARM-MIB::tfAlarmMajor TAILF-ALARM-MIB::tfAlarmType.0 = STRING: device-alarm TAILF-ALARM-MIB::tfAlarmDevice.0 = STRING: ntd-1 TAILF-ALARM-MIB::tfAlarmObject.0 = STRING: "/ncs:devices/ncs:device[ncs:name='ntd-1']" TAILF-ALARM-MIB::tfAlarmObjectOID.0 = OID: SNMPv2-SMI::zeroDotZero TAILF-ALARM-MIB::tfAlarmObjectStr.0 = "" TAILF-ALARM-MIB::tfAlarmSpecificProblem.0 = STRING: "System Boot" TAILF-ALARM-MIB::tfAlarmEventType.0 = INTEGER: 1 TAILF-ALARM-MIB::tfAlarmProbableCause.0 = Gauge32: 0 TAILF-ALARM-MIB::tfAlarmTime.0 = STRING: 2017-15-11,16:03:7.6,+0:0 TAILF-ALARM-MIB::tfAlarmText.0 = STRING: "NTD is rebooting"
```

As you can see by the bold sections, the same information is presented, it just has SNMP specific category titles.

SNMP MIBs

There are seven Corero MIB files available with the CMS. You can download the MIBs from the Corero support portal:

- **CORERO-MIB.mib** – Defines the devices and is referenced by the other MIB files
- **CORERO-CMS-MIB.mib** – Contains generic enterprise information referenced by the other MIB files
- **CORERO-CMS-DEVICES-MIB.mib** – Contains the objects for device status information
- **CORERO-CMS-CLUSTERS-MIB.mib** – Contains the objects for Cluster status information
- **CORERO-CMS-SEGMENTS-MIB.mib** – Contains the objects for Segment status information
- **CORERO-CMS-STATISTICS-MIB.mib** – Contains the objects for statistical information
- **CORERO-CMS-SYSTEM-STATUS-MIB.mib** – Contains the objects for system status information

The other important MIB file is **IF-MIB.mib**. This is used by CMS and, when you enable SNMP for specific Defense devices, this is the only MIB they access. IF-MIB is a standard MIB file, but Corero only use two IF-MIB tables: **ifTable** and **ifXTable**.

Tip: Every object in a MIB has a unique Object ID (OID) which you can use to look up specific pieces of information.

Viewing a Corero MIB

Note: Before you can perform an snmpwalk for the CMS you must [enable SNMP for the CMS](#). Before you can perform an snmpwalk for a Defense device, you must [enable SNMP for that device](#).

On the Linux machine you want to use to view information from the MIB, you must do the following:

- Install `snmpwalk` and `snmpget` (from the `net-snmp` and `net-snmp-utils` packages)
- Save a copy of the Corero MIB files in the required folder for `snmpwalk`. By default, this is `.snmp/mibs`

Using SNMP v2c to view values in a MIB

Use the following example to create a command to return all object values in the SNMP MIB:

```
snmpwalk -u test -v 2c -c <communitySecurityName> <IPaddress>:<snmpPort>
<mibName>::<mibList>
```

Alternatively, you can use an object's OID to look up the value of a single object from the MIB:

```
snmpgetnext -v 2c -c <communitySecurityName> <IPaddress>:<snmpPort> <OID>
```

You need to replace the following placeholders:

- `<communitySecurityName>` – The security name of your SNMP community.
- `<IPAddress>:<snmpPort>` – The IP address of your CMS or Defense device, followed by the SNMP port (by default this is port 161). For example, 10.10.1.100:161.
- `<mibName>` – The file name of a Corero MIB, for example, CORERO-CMS-CLUSTERS-MIB
- `<mibList>` – The name of the list of objects you want to return, or example CORERO-CMS-CLUSTERS-MIB::clusters would return all objects in the clusters list, but CORERO-CMS-CLUSTERS-MIB::clusterName would only return the values for the clusterName object. See the below reference table for the list names and object names available in each MIB file.
- `<OID>` – The full OID of the object whose value you want to return. For example, 1.3.6.1.4.1.41036.4.1.5.1.1.3 will look for the value of advancedStatisticsStartTrustedAddresses (the number of trusted IP addresses).

Using SNMP v3 to view values in a MIB

Note: Defense devices cannot use SNMPv3.

Use the following example to create a command to return all object values in the SNMP MIB:

```
snmpwalk -u <userSecurityName> -v 3 -a [md5|sha] -A <authPassword> -x [aes|des] -X
<privPassword> -l [authPriv|authNoPriv|noAuthNoPriv] <IPAddress>:<snmpPort>
<mibName>::<mibList>
```

Alternatively, you can use an object's OID to look up the value of a single object from the MIB.

```
snmpwalk -u <userSecurityName> -v 3 -a [md5|sha] -A <authPassword> -x [aes|des] -X
<privPassword> -l [authPriv|authNoPriv|noAuthNoPriv] <IPAddress>:<snmpPort> <OID>
```

You need to replace the following placeholders:

- `<userSecurityName>` – The security name for the user you created above
- `[md5|sha]` – The authentication protocol for this user
- `<authPassword>` – The password or key value for this authentication protocol
- `[aes|des]` – The privacy protocol for this user
- `<privPassword>` – The password or key value for this privacy protocol
- `[authPriv|authNoPriv|noAuthNoPriv]` – The protocol type you need to use for your system
- `<IPAddress>:<snmpPort>` – The IP address of your CMS or Defense device, followed by the SNMP port (by default this is port 161). For example, 10.10.1.100:161.
- `<mibName>` – The file name of a Corero MIB, for example, CORERO-CMS-STATISTICS-MIB
- `<mibList>` – The name of the list of objects you want to return, or example CORERO-CMS-CLUSTERS-MIB::clusters would return all objects in the clusters list, but CORERO-CMS-CLUSTERS-MIB::clusterName would only return the values for the clusterName object. See the below reference table for the list names and object names available in each MIB file.

- **<OID>** – The full OID of the object whose value you want to return. For example, **.1.3.6.1.4.1.41036.4.1.5.1.1.3** will look for the value of **advancedStatisticsStartTrustedAddresses** (the number of trusted IP addresses).

Note: `-a[md5|sha]-A<authPassword>` is used with `-l authPriv` and `-l authNoPriv` only. `-x[aes|des]-X<privPassword>` is only used with `-l authPriv`.

OID numbers

The tables below lists the objects available in the Corero-specific MIB files. All are current and read-only.

Note: All OID numbers in the Corero MIB tables must be appended to the core OID number:

.1.3.6.1.4.1.41036.4.1

For example, if the OID end digits in the table are **.2.1.1.1**. The full OID is

.1.3.6.1.4.1.41036.4.1.2.1.1.1.

CORERO-MIB and CORERO-CMS-MIB

These MIB files define the devices and contain generic information referenced by the other MIBs. They do not contain any objects which can be accessed in an SNMP walk.

IF-MIB

Available for the CMS and Defense devices (excluding NTD120). The two tables used by Corero are: **ifTable** and **ifXTable**.

The IF MIB uses the standard MIB OID numbers and full documentation for non-Corero MIBs can be found online.

- The OID for the **ifTable** is **.1.3.6.1.2.1.2.2**
- The OID for the **ifXTable** is **.1.3.6.1.2.1.31.1.1**

CORERO-CMS-DEVICES-MIB

Available for the CMS only. The list name for all objects in this table is: **devices**

Name	OID end digits	Syntax	Description
deviceIndex	.2.1.1.1	INTEGER	The SNMP index of the device
deviceName	.2.1.1.2	OCTET STRING	The name of the device
deviceAddress	.2.1.1.3	OCTET STRING	The IP address which the CMS uses to look for the device

Name	OID end digits	Syntax	Description
deviceDescription	.2.1.1.4	OCTET STRING	The device description. If no description is entered, this is blank.
deviceDefenseMode	.2.1.1.5	INTEGER	The configured Defense Mode for the device
deviceAdminState	.2.1.1.6	INTEGER	The current admin-state of the device
deviceModel	.2.1.1.7	INTEGER	The type of device
deviceSerialNumber	.2.1.1.8	OCTET STRING	The serial number of the device
deviceConnectionState	.2.1.1.9	INTEGER	The current state of the connection between the CMS and the device
deviceDeploymentState	.2.1.1.10	INTEGER	The device's current deployment state
deviceDeploymentAction	.2.1.1.11	INTEGER	The deployment action the device is currently performing
deviceSXOSVersion	.2.1.1.12	OCTET STRING	The version number of the device's operating system (SXOS)
deviceSoftwareVersion	.2.1.1.13	OCTET STRING	The device's current software version in '{MAJOR}.{MINOR}.{PATCH}.{BUILD}' format
deviceUptime	.2.1.1.14	OCTET STRING	The amount of time since the device was last rebooted in '{DAYS}d {HOURS}h {MINUTES}m {SECONDS}s' format
deviceStatus	.2.1.1.15	OCTET STRING	The device status indicates whether traffic is running to the device (normal), or if there is an issue which may affect traffic or its connection to the CMS
deviceType	.2.1.1.16	INTEGER	The device type indicates whether this is a Defense (0) or Bypass (1) device
deviceBypassMode	.2.1.1.17	OCTET STRING	The configured Bypass Mode for this device

CORERO-CMS-CLUSTERS-MIB

Available for the CMS only. The list name for all objects in this table is: `clusters`

Name	OID end digits	Syntax	Description
clusterIndex	.3.1.1.1	INTEGER	The SNMP index of the Cluster
clusterName	.3.1.1.2	OCTET STRING	The name of the Cluster
clusterDescription	.3.1.1.3	OCTET STRING	The description of the Cluster. If no description is entered, this is blank.
clusterProtectionProfile	.3.1.1.4	OCTET STRING	The name of the Protection Profile associated with this Cluster
clusterIngressSampleRate	.3.1.1.5	INTEGER	External ingress sampling rate for all devices in the cluster
clusterOptimizeForScrubbing	.3.1.1.6	INTEGER	Indicates whether the devices in the cluster are optimized for scrubbing deployments

CORERO-CMS-SEGMENTS-MIB

Available for the CMS only. The list name for all objects in this table is: `segments`

Name	OID end digits	Syntax	Description
segmentIndex	.4.1.1.1	INTEGER	The SNMP index of the Segment
segmentDevice	.4.1.1.2	OCTET STRING	The device containing the Segment
segmentId	.4.1.1.3	OCTET STRING	The ID of the segment
segmentName	.4.1.1.4	OCTET STRING	The name of the Segment
segmentDescription	.4.1.1.5	OCTET STRING	The description of this Segment. If no description is entered, this is blank.
segmentLinkStatePropagationAdminState	.4.1.1.6	INTEGER	Whether this Segment has Link State Propagation enabled or disabled

Name	OID end digits	Syntax	Description
segmentLinkStatePropagationWaitTime	.4.1.1.7	INTEGER	Number of seconds the CMS currently waits before propagating a link state change to the partner, when Link State Propagation is enabled
segmentLinkStatePropagationRecoveryTimeout	.4.1.1.8	INTEGER	Number of seconds the CMS currently waits after a link is brought back up before using its state to change partner state, when Link State Propagation is enabled
segmentConfiguredDefenseMode	.4.1.1.9	INTEGER	The configured Defense Mode of the Segment
segmentNtdExternalInterface	.4.1.1.10	OCTET STRING	The name of the Segment's external NTD interface
segmentNtdExternalInterfaceStatus	.4.1.1.11	INTEGER	The current status of the Segment's external NTD interface
segmentNtdExternalInterfaceLinkSpeed	.4.1.1.12	Unsigned32	The link speed of the Segment's external NTD interface in Mbit/s
segmentNtdInternalInterface	.4.1.1.13	OCTET STRING	The name of the Segment's internal NTD interface
segmentNtdInternalInterfaceStatus	.4.1.1.14	INTEGER	The current status of the Segment's internal NTD interface
segmentNtdInternalInterfaceLinkSpeed	.4.1.1.15	Unsigned32	The link speed of the Segment's internal NTD interface in Mbit/s
segmentNbaExternalInterface	.4.1.1.16	OCTET STRING	The name of the Segment's external NBA interface
segmentNbaExternalInterfaceStatus	.4.1.1.17	INTEGER	The current status of the Segment's external NBA interface

Name	OID end digits	Syntax	Description
segmentNbaExternalInterfaceLinkSpeed	.4.1.1.18	Unsigned32	The link speed of the Segment's external NBA interface in Mbit/s
segmentNbaInternalInterface	.4.1.1.19	OCTET STRING	The name of the Segment's internal NBA interface
segmentNbaInternalInterfaceStatus	.4.1.1.20	INTEGER	The current status of the Segment's internal NBA interface
segmentNbaInternalInterfaceLinkSpeed	.4.1.1.21	Unsigned32	The link speed of the Segment's internal NBA interface in Mbit/s
segmentCurrentDefenseMode	.4.1.1.22	INTEGER	The Defense Mode the Segment is currently operating in
segmentBypassDevice	.4.1.1.23	OCTET STRING	The name of the external bypass device connected to the Segment. If there is no connected bypass device, this is blank.
segmentConfiguredBypassMode	.4.1.1.24	INTEGER	The configured Bypass Mode for the Segment. If the Segment has no bypass capability, this shows blank.
segmentCurrentBypassMode	.4.1.1.25	INTEGER	The current Bypass Mode the Segment is operating in. If the Segment has no bypass capability, this shows not-applicable.
segmentCurrentBypassState	.4.1.1.26	INTEGER	The current Bypass State the Segment is operating in. If the Segment has no bypass capability, this shows not-applicable.
segmentDefenseModeOverride	.4.1.1.27	INTEGER	The override level applied for the segment defense mode.
segmentBypassModeOverride	.4.1.1.28	INTEGER	The override level applied for the segment bypass mode.

CORERO-CMS-STATISTICS-MIB

Available for the CMS only. The list name for all objects in all of the tables below is: `statistics`

The list name for all objects in this table is: `advancedStatisticsTable`

Name	OID end digits	Syntax	Description
<code>advancedStatisticsGroup</code>	<code>.5.1.1.1</code>	GroupType	The grouping of Advanced statistics
<code>advancedStatisticsGroupIndex</code>	<code>.5.1.1.2</code>	INTEGER	The SNMP index of each element within a grouping
<code>advancedStatisticsStartTrustedAddresses</code>	<code>.5.1.1.3</code>	Counter64	Number of trusted IP addresses
<code>advancedStatisticsStartUnclassifiedAddresses</code>	<code>.5.1.1.4</code>	Counter64	Number of unclassified IP addresses
<code>advancedStatisticsFinishTrustedAddresses</code>	<code>.5.1.1.5</code>	Counter64	Number of no-longer trusted IP addresses
<code>advancedStatisticsFinishUnclassifiedAddresses</code>	<code>.5.1.1.6</code>	Counter64	Number of no-longer unclassified IP addresses
<code>advancedStatisticsTotalAddressAdds</code>	<code>.5.1.1.7</code>	Counter64	Total number of IP addresses added across the device
<code>advancedStatisticsInputOverloadPackets</code>	<code>.5.1.1.8</code>	Counter64	Number of overload packets received from input
<code>advancedStatisticsInputOverloadPacketRate</code>	<code>.5.1.1.9</code>	Counter32	Rate of overload packets received from input (packets/sec)
<code>advancedStatisticsSetupOverloadPackets</code>	<code>.5.1.1.10</code>	Counter64	Number of overload packets received from setup

Name	OID end digits	Syntax	Description
advancedStatisticsSetupOverloadPacketRate	.5.1.1.11	Counter32	Rate of overload packets received from setup (packets/sec)
advancedStatisticsContextOverloadPackets	.5.1.1.12	Counter64	Number of context overload packets received
advancedStatisticsContextOverloadPacketRate	.5.1.1.13	Counter32	Rate of context overload packets received (packets/sec)
advancedStatisticsEgressDropPackets	.5.1.1.14	Counter64	Number of packets dropped on egress
advancedStatisticsEgressDropPacketRate	.5.1.1.15	Counter32	Rate of packets dropped on egress (packets/sec)
advancedStatisticsIngressDropPackets	.5.1.1.16	Counter64	Number of packets dropped on ingress
advancedStatisticsIngressDropPacketRate	.5.1.1.17	Counter32	Rate of packets dropped on ingress (packets/sec)
advancedStatisticsEgressOverloadPackets	.5.1.1.18	Counter64	Number of overload packets from egress
advancedStatisticsEgressOverloadPacketRate	.5.1.1.19	Counter32	Rate of overload packets from egress (packets/sec)
advancedStatisticsFlowOverloadPackets	.5.1.1.20	Counter64	Number of overload packets from flows
advancedStatisticsFlowOverloadPacketRate	.5.1.1.21	Counter32	Rate of overload packets from flows (packets/sec)
advancedStatisticsSmartRuleOverloadPackets	.5.1.1.22	Counter64	Number of overload packets from Smart-Rules

Name	OID end digits	Syntax	Description
advancedStatisticsSmartRuleOverloadPacketRate	.5.1.1.23	Counter32	Rate of overload packets from Smart-Rules (packets/sec)
advancedStatisticsSourceSmartRuleOverloadPackets	.5.1.1.24	Counter64	Number of overload packets from source Smart-Rules
advancedStatisticsSourceSmartRuleOverloadPacketRate	.5.1.1.25	Counter32	Rate of overload packets from source Smart-Rules (packets/sec)
advancedStatisticsFragmentOverloadPackets	.5.1.1.26	Counter64	Number of overload packets from fragments
advancedStatisticsFragmentOverloadPacketRate	.5.1.1.27	Counter32	Rate of overload packets from fragments (packets/sec)
advancedStatisticsIpOverloadPackets	.5.1.1.28	Counter64	Number of IP overload packets
advancedStatisticsIpOverloadPacketRate	.5.1.1.29	Counter32	Rate of IP overload packets (packets/sec)
advancedStatisticsFlexRuleOverloadPackets	.5.1.1.30	Counter64	Number of overload packets from Flex-Rules
advancedStatisticsFlexRuleOverloadPacketRate	.5.1.1.31	Counter32	Rate of overload packets from Flex-Rules (packets/sec)
advancedStatisticsIngressOverloadPackets	.5.1.1.32	Counter64	Number of ingress packets protected with overload

Name	OID end digits	Syntax	Description
advancedStatisticsIngressOverloadPacketRate	.5.1.1.33	Counter32	Rate of ingress packets protected with overload (packets/sec)
advancedStatisticsIngressOverloadBytes	.5.1.1.34	Counter64	Number of ingress bytes protected with overload
advancedStatisticsIngressOverloadBitRate	.5.1.1.35	Counter32	Rate of ingress bits protected with overload (Mbits per sec)
advancedStatisticsStartTrackingFlow	.5.1.1.36	Counter64	Number of tracked TCP flows during DDOS attack started
advancedStatisticsStopTrackingFlow	.5.1.1.37	Counter64	Number of tracked TCP flows during DDOS attack stopped

The list name for all objects in this table is: `blockRateStatisticsTable`

Name	OID end digits	Syntax	Description
blockRateStatisticsGroup	.5.2.1.1	GroupType	The grouping of Defense Block Rate statistics
blockRateStatisticsGroupIndex	.5.2.1.2	INTEGER	The SNMP index of each element within a grouping
blockRateStatisticsAllRulesBlockPackets	.5.2.1.3	Counter32	Aggregate number of blocked packet across all rules
blockRateStatisticsAllRulesBlockPacketRate	.5.2.1.4	Counter32	Aggregate blocked packet rate of all rules (packets per second)
blockRateStatisticsAllRulesBlockBytes	.5.2.1.5	Counter64	Aggregate number of blocked bytes across all rules

Name	OID end digits	Syntax	Description
blockRateStatisticsAllRulesBlockBitRate	.5.2.1.6	Counter32	Aggregate blocked bit rate of all rules (Mbits per second)

The list name for all objects in this table is: `interfaceStatisticsTable`

Name	OID end digits	Syntax	Description
interfaceStatisticsGroup	.5.3.1.1	GroupType	The grouping of Interface statistics
interfaceStatisticsGroupIndex	.5.3.1.2	INTEGER	The SNMP index of each element within a grouping
interfaceStatisticsExternalPortBitReceiveRate	.5.3.1.3	Counter32	Receive rate on the external ports (Mbits per second)
interfaceStatisticsExternalPortBitTransmitRate	.5.3.1.4	Counter32	Transmit rate on the external ports (Mbits per second)
interfaceStatisticsExternalPortEgressDroppedPackets	.5.3.1.5	Counter64	Number of dropped egress packets from the external port
interfaceStatisticsExternalPortIngressDroppedPackets	.5.3.1.6	Counter64	Number of dropped ingress packets from the external port
interfaceStatisticsExternalPortPacketReceiveRate	.5.3.1.7	Counter32	Receive rate on the external ports (packets per second)
interfaceStatisticsExternalPortPacketTransmitRate	.5.3.1.8	Counter32	Transmit rate on the external ports (packets per second)
interfaceStatisticsExternalPortReceivedBadCrcPackets	.5.3.1.9	Counter64	Number of packets received to the external port with an invalid CRC
interfaceStatisticsExternalPortReceivedBytes	.5.3.1.10	Counter64	Number of bytes received to the external port

Name	OID end digits	Syntax	Description
interfaceStatisticsExternalPortReceivedJabberPackets	.5.3.1.11	Counter64	Number of jabber packets received to the external port
interfaceStatisticsExternalPortReceivedOversizedPackets	.5.3.1.12	Counter64	Number of oversized packets received to the external port
interfaceStatisticsExternalPortReceivedPackets	.5.3.1.13	Counter64	Number of packets received to the external port
interfaceStatisticsExternalPortTransmitErrorPackets	.5.3.1.14	Counter64	Number of errors transmitting packets from the external port
interfaceStatisticsExternalPortTransmittedBytes	.5.3.1.15	Counter64	Number of bytes transmitted from external port
interfaceStatisticsExternalPortTransmittedPackets	.5.3.1.16	Counter64	Number of packets transmitted from the external port
interfaceStatisticsInternalPortBitReceiveRate	.5.3.1.17	Counter32	Receive rate on the internal ports (Mbits per second)
interfaceStatisticsInternalPortBitTransmitRate	.5.3.1.18	Counter32	Transmit rate on the internal ports (Mbits per second)
interfaceStatisticsInternalPortEgressDroppedPackets	.5.3.1.19	Counter64	Number of dropped egress packets from the internal port
interfaceStatisticsInternalPortIngressDroppedPackets	.5.3.1.20	Counter64	Number of dropped ingress packets from the internal port
interfaceStatisticsInternalPortPacketReceiveRate	.5.3.1.21	Counter32	Receive rate on the internal ports (packets per second)
interfaceStatisticsInternalPortPacketTransmitRate	.5.3.1.22	Counter32	Transmit rate on the internal ports (packets per second)
interfaceStatisticsInternalPortReceivedBadCrcPackets	.5.3.1.23	Counter64	Number of packets received to the internal port with an invalid CRC

Name	OID end digits	Syntax	Description
interfaceStatisticsInternalPortReceivedBytes	.5.3.1.24	Counter64	Number of bytes received to the internal port
interfaceStatisticsInternalPortReceivedJabberPackets	.5.3.1.25	Counter64	Number of jabber packets received to the internal port
interfaceStatisticsInternalPortReceivedOversizedPackets	.5.3.1.26	Counter64	Number of oversized packets received to the internal port
interfaceStatisticsInternalPortReceivedPackets	.5.3.1.27	Counter64	Number of packets received to the internal port
interfaceStatisticsInternalPortTransmitErrorPackets	.5.3.1.28	Counter64	Number of errors transmitting packets from the internal port
interfaceStatisticsInternalPortTransmittedBytes	.5.3.1.29	Counter64	Number of bytes transmitted from the internal port
interfaceStatisticsInternalPortTransmittedPackets	.5.3.1.30	Counter64	Number of packets transmitted from the internal port
interfaceStatisticsExternalPortIngressOverloadPackets	.5.3.1.31	Counter64	Number of packets transmitted to the external port protected with overload
interfaceStatisticsExternalPortIngressOverloadBytes	.5.3.1.32	Counter64	Number of bytes transmitted to the external port protected with overload
interfaceStatisticsExternalPortReceivedFecErrorPackets	.5.3.1.33	Counter64	Number of packets to the external port with FEC errors
interfaceStatisticsInternalPortReceivedFecErrorPackets	.5.3.1.34	Counter64	Number of packets to the internal port with FEC errors

The list name for all objects in this table is: `ipAddressStatisticsTable`

Name	OID end digits	Syntax	Description
ipAddressStatisticsGroup	.5.4.1.1	GroupType	The grouping of IP Address statistics
ipAddressStatisticsGroupIndex	.5.4.1.2	INTEGER	The SNMP index of an element within each grouping
ipAddressStatisticsInUseAddresses	.5.4.1.3	Counter32	Total number of IP Address Statistics table entries in use
ipAddressStatisticsInUseTrustedAddresses	.5.4.1.4	Counter32	Total number of trusted IP addresses across the devices
ipAddressStatisticsInUseUnclassifiedAddresses	.5.4.1.5	Counter32	Total number of unclassified IP addresses across the devices
ipAddressStatisticsPanicGood	.5.4.1.6	Counter64	Total number of source IP addresses which were deemed good while in panic mode
ipAddressStatisticsPanicGoodRate	.5.4.1.7	Counter32	Rate of source IP addresses which were deemed good while in panic mode
ipAddressStatisticsPanicBad	.5.4.1.8	Counter64	Total number of source IP addresses which were deemed bad while in panic mode
ipAddressStatisticsPanicBadRate	.5.4.1.9	Counter32	Rate of source IP addresses which were deemed bad while in panic mode
ipAddressStatisticsPanicTimedOut	.5.4.1.10	Counter64	Total number of source IP addresses which timed out while in panic mode
ipAddressStatisticsPanicTimedOutRate	.5.4.1.11	Counter32	Rate of source IP addresses which were timed out while in panic mode
ipAddressStatisticsPromotedToTrusted	.5.4.1.12	Counter64	Total number of source IP addresses which were promoted to trusted

Name	OID end digits	Syntax	Description
ipAddressStatisticsPromotedToTrustedRate	.5.4.1.13	Counter32	Rate of source IP addresses which were promoted to trusted
ipAddressStatisticsTrackedTcpFlows	.5.4.1.14	Counter64	Total number of tracked TCP flows in flow based threat awareness
ipAddressStatisticsTrackedTcpFlowsSuccess	.5.4.1.15	Counter64	Total number of TCP flows successfully tracked by flow based threat awareness
ipAddressStatisticsTrackedTcpFlowsSuccessRate	.5.4.1.16	Counter32	Rate of TCP flows successfully tracked by flow based threat awareness
ipAddressStatisticsTrackedTcpFlowsTimedOut	.5.4.1.17	Counter64	Total number of TCP flows that timed out when tracked by flow based threat awareness
ipAddressStatisticsTrackedTcpFlowsTimedOutRate	.5.4.1.18	Counter32	Rate of TCP flows that timed out when tracked by flow based threat awareness

The list name for all objects in this table is: `ruleStatisticsTable`

Name	OID end digits	Syntax	Description
ruleStatisticsGroup	.5.5.1.1	GroupType	The grouping of Rule statistics
ruleStatisticsGroupIndex	.5.5.1.2	INTEGER	The SNMP index of an element within each grouping
ruleStatisticsRuleIndex	.5.5.1.3	INTEGER	The SNMP integer representation of the rule - usually the rule name with 'cns-' omitted
ruleStatisticsRuleName	.5.5.1.4	OCTET STRING	The name of the rule for which these statistics belong
ruleStatisticsRuleDescription	.5.5.1.5	OCTET STRING	The description of the rule

Name	OID end digits	Syntax	Description
ruleStatisticsBlockEventCount	.5.5.1.6	Counter64	Number of events blocked by this rule
ruleStatisticsBlockPacketCount	.5.5.1.7	Counter64	Number of packets blocked by this rule
ruleStatisticsBlockByteCount	.5.5.1.8	Counter64	Number of bytes blocked by this rule
ruleStatisticsDetectEventCount	.5.5.1.9	Counter64	Number of events detected by this rule
ruleStatisticsDetectPacketCount	.5.5.1.10	Counter64	Number of packets detected by this rule
ruleStatisticsDetectByteCount	.5.5.1.11	Counter64	Number of bytes detected by this rule
ruleStatisticsBlockPacketRate	.5.5.1.12	Counter32	Rate of packets blocked by this rule (packets per second)
ruleStatisticsDetectPacketRate	.5.5.1.13	Counter32	Rate of packets detected by this rule (packets per second)
ruleStatisticsBlockBitRate	.5.5.1.14	Counter32	Rate of data blocked by this rule (Mbits per second)
ruleStatisticsDetectBitRate	.5.5.1.15	Counter32	Rate of data detected by this rule (Mbits per second)

The list name for all objects in this table is: `setupRateStatisticsTable`

Name	OID end digits	Syntax	Description
setupRateStatisticsGroup	.5.6.1.1	GroupType	The grouping of Setup Rate statistics
setupRateStatisticsGroupIndex	.5.6.1.2	INTEGER	The SNMP index of an element within each grouping
setupRateStatisticsIcmpSetupRate	.5.6.1.3	Counter32	ICMP flow setup rate (flows/sec)
setupRateStatisticsNonTcpSetupRate	.5.6.1.4	Counter32	Protocols other than TCP flow setup rate (flows/sec)
setupRateStatisticsOtherIPSetupRate	.5.6.1.5	Counter32	Protocols other than TCP and UDP setup rate (flows/sec)
setupRateStatisticsTcpSetupRate	.5.6.1.6	Counter32	TCP flows setup rate (flows/sec)

Name	OID end digits	Syntax	Description
setupRateStatisticsUdpSetupRate	.5.6.1.7	Counter32	UDP flows setup rate (flows/sec)

The list name for all objects in this table is: `usageStatisticsTable`

Name	OID end digits	Syntax	Description
usageStatisticsGroup	.5.7.1.1	GroupType	The grouping of Usage statistics
usageStatisticsGroupIndex	.5.7.1.2	INTEGER	The SNMP index of an element within each grouping
usageStatisticsFinishIcmpFlows	.5.7.1.3	Counter64	ICMP flows finished across the devices
usageStatisticsFinishOtherFlows	.5.7.1.4	Counter64	Other IP flows finished across the devices
usageStatisticsFinishTcpFlows	.5.7.1.5	Counter64	TCP flows finished across the devices
usageStatisticsFinishUdpFlows	.5.7.1.6	Counter64	UDP flows finished across the devices
usageStatisticsInUseFlows	.5.7.1.7	Counter32	Total number of flows in use across the devices
usageStatisticsInUseIcmpFlows	.5.7.1.8	Counter32	Total number of ICMP flows in use across the devices
usageStatisticsInUseOtherFlows	.5.7.1.9	Counter32	Total number of non-TCP, non-UDP, non-ICMP flows in use across the devices
usageStatisticsInUseTcpFlows	.5.7.1.10	Counter32	Total number of TCP flows in use across the devices
usageStatisticsInUseUdpFlows	.5.7.1.11	Counter32	Total number of UDP flows in use across the devices
usageStatisticsStartIcmpFlows	.5.7.1.12	Counter64	ICMP flows started across the devices
usageStatisticsStartOtherFlows	.5.7.1.13	Counter64	Other IP flows started across the devices
usageStatisticsStartTcpFlows	.5.7.1.14	Counter64	TCP flows started across the devices
usageStatisticsStartUdpFlows	.5.7.1.15	Counter64	UDP flows started across the devices

CORERO-CMS-SYSTEM-STATUS-MIB


Available for the CMS only. The list name for all objects in this table is: `issues`

Name	OID end digits	Syntax	Description
issueIndex	.6.1.4.1	INTEGER	The issue index
issueType	.6.1.4.2	INTEGER	The issue type: protection (0), devices (1), network (2)
issueDevice	.6.1.4.3	OCTET STRING	The device for which issue was created
issueSegment	.6.1.4.4	OCTET STRING	The segment for which issue was created
issueDescription	.6.1.4.5	OCTET STRING	The issue description
issueSeverity	.6.1.4.6	INTEGER	The issue severity: normal (0), warning (1), error (2)

CMS Web User Interface

For reference information on the CMS Web UI, including descriptions of every onscreen field and button, see your built in CMS help.

To open the CMS built in help

1. Open the CMS Web UI in a browser and log in.
2. On the top menu, click  the help button.

CMS CLI Overview

The SmartWall Central Management Server (CMS) Command Line Interface (CLI) is an alternative method of working with the CMS (rather than using the Web UI in a browser). The CLI has all the functionality of the Web UI plus a few advanced features you may be asked to use by a Corero Support Engineer.

Accessing the CLI

To access the CLI you need to connect to your CMS application using an SSH client:

```
ssh -p 2024 <username>@<ipaddress>
```

CLI Modes

There are two main CLI modes:

- **Operational Mode** – The CMS CLI starts in operational mode, which is used for displaying information about the CMS and the devices that it manages.
- **Configuration Mode** – Type `configure` to enter the mode for changing the configuration of the CMS. You can return to operational mode by typing `exit`.

```
admin@vcms172> configure
Entering configuration mode private
[ok] [2018-02-13 10:40:46]

[edit]
admin@vcms172 (config) #
```

View possible completions

When you're writing a CLI command, you can press the tab key at any time to view a list of possible completions. If there is only one possible completion, it is added automatically. In the image below, you can see tab being used twice, first to see the possible Protection Profiles available and then to see the possible configuration options for Inspection Control.


```
admin@vcms172(config)# set policy protection-profile
Possible completions:
  Name used to identify Protection Profile  default
admin@vcms172(config)# set policy protection-profile default inspection-control

Possible completions:
  admin-state          - Enable/disable Inspection Control
  default-inspection-mode - Inspection mode used for destination addresses
                        not described in the overrides entries table
  override-entry       - A list of override entries for inspection control
  white-list-event-logging - (cns-001043) Enable or disable analytics logging
                        for white listed traffic
admin@vcms172(config)# set policy protection-profile default inspection-control
```

Commit a change

Just like using the Web UI, you need to commit a change before it takes effect. To do that, enter the command:

```
commit
```

```
admin@vcms172(config)# set policy protection-profile default inspection-control
override-entry entry1 destination-ip 1.1.1.1
[ok] [2018-02-13 11:03:40]

[edit]
admin@vcms172(config)# commit
Commit complete.
[ok] [2018-02-13 11:03:49]

[edit]
admin@vcms172(config)#
```

Example: Using Set and Commit commands to Add a new NTD120 and NBA pair

The following example shows how to add and configure a new NTD120 and NBA device pair. The commands in the image below do the following:

1. Enter configuration mode.
2. (Optional) Create a new Protection Profile you want to use for the Defense device.
3. (Optional) Create a new Cluster for the Defense device.
4. Add a Bypass device (nba) to the CMS.
5. Add a Defense device (ntd-120) to the CMS.
6. Add the Defense device to a Cluster.
7. Commit the changes. Note: if you don't commit after adding the devices, the CMS is unable contact the new Defense device to see the available Segments for the next command.
8. Connect the Bypass device to the correct Segment on the Defense device.
9. Commit this change.

```

admin connected from 192.168.11.28 using ssh on vcms172
admin@vcms172> configure
Entering configuration mode private
[ok][2018-02-14 05:11:53]

[edit]
admin@vcms172(config)# set policy protection-profile EUprofile
[ok][2018-02-14 05:13:05]

[edit]
admin@vcms172(config)# set clusters cluster EUdevices protection-profile EUprofile
[ok][2018-02-14 05:13:34]

[edit]
admin@vcms172(config)# set devices device nba address 10.10.148.160 type bypass
[ok][2018-02-14 05:14:22]

[edit]
admin@vcms172(config)# set devices device ntd-120 address 10.10.148.161 type defense
[ok][2018-02-14 05:14:50]

[edit]
admin@vcms172(config)# set clusters cluster EUdevices device ntd-120
[ok][2018-02-14 05:15:14]

[edit]
admin@vcms172(config)# commit
Commit complete.
[ok][2018-02-14 05:15:26]

[edit]
admin@vcms172(config)# set segments segment ntd-120 1 bypass-device nba
[ok][2018-02-14 05:15:59]

[edit]
admin@vcms172(config)# commit
commit-queue-id 104600383426
Commit complete.
[ok][2018-02-14 05:16:03]

[edit]
admin@vcms172(config)# █

```

Using pipes

When you're inputting a CLI command, you can modify how the output is displayed by adding a pipe character followed by a display command. For example, if you wanted a command to repeat every 10 seconds you would add `| repeat 10`. To view the statistics for a segment and have the information update every 10 seconds, you could use the command `show statistics segment ntd-1 1 | repeat 10`.

By pressing the tab key after the pipe character, you can see all available pipe modifications available for this command. Below you can see all possible modifications for the segment statistics example command.

```
admin@vcms172> show statistics segment ntd-1 1 |
Possible completions:
count          - Count the number of lines in the output
csv            - Emit table output in CSV format
de-select      - Select columns to not include
display        - Display options
display-level  - Display level
except         - Show only text that does not matches a pattern
find           - Search for the first occurrence of a pattern
linnum         - Enumerate lines in the output
match          - Show only text that matches a pattern
match-all     - All selected filters must match
match-any      - At least one filter must match
more           - Paginate output
nomore         - Suppress pagination
notab          - Suppress table output
repeat         - Repeat show command with a given interval
select         - Select additional columns
sort-by        - Select sorting indices
tab            - Enforce table output
until          - Display until the first occurrence of a pattern
admin@vcms172> show statistics segment ntd-1 1 |
```

Viewing tables

Some information can display differently depending on the size of the CLI window. When you're viewing statistics, a thin CLI window causes the information to display in a list, and a wide CLI window causes the information to display as a table. You can change the window size, or you can use the pipe command to force this behavior:

- | `tab` – to force the table view regardless of window size
- | `no tab` – to force the list view regardless of window size

Example: Using the show command and pipes to view device information

You can view device statistics and information in the Web UI (Network > Devices). You can also use the CLI to view detailed device statistics. The following commands are an example of the most popular commands in this area:

`show configuration devices` – view the configuration of all devices in the CMS. You can also specify a single device e.g. `show configuration devices device ntd-120`.

```

authgroups {
  group default {
    default-map {
      remote-name      admin;
      remote-password  $4$HIU0acQxHJgk2BZrIhVWlg==;
    }
  }
}
device Bypass {
  address      12.12.12.101;
  description  "";
  authgroup    default;
  connect-timeout 5;
  read-timeout 60;
  write-timeout 60;
  type         bypass;
  interfaces {
    interface xe-1/1;
    interface xe-1/2;
    interface xe-1/3;
    interface xe-1/4;
  }
}
device NTD {
  address      12.12.12.102;
  description  "";
  authgroup    default;
  connect-timeout 5;
  read-timeout 60;
  write-timeout 60;
  bypass-mode {
    automatic;
  }
  operating-mode mitigate;
  type         defense;
  interfaces {
    interface xe-1/1;
    interface xe-1/2;
    interface xe-1/3;
    interface xe-1/4;
  }
}
advanced-settings;
[ok][2018-01-25 18:27:07]

```

`show devices device status` – view the current status of all devices in the CMS. You can also specify a single device e.g. `show devices device ntd-120 status`.

NAME	MODEL	SERIAL NUMBER	CONNECTION STATE	DEPLOYMENT STATE	DEPLOYMENT ACTION	SXOS VERSION	SOFTWARE VERSION	UPTIME	HEALTH
BYPASS1	nba	133155517300005	connected	in-sync	not-in-progress	N/A	8.18.0.0243	7d 1h 29m 54s	normal
NTD1	ntd120	611055518070008	connected	in-sync	not-in-progress	mde418.10.sda2	8.18.0.0999	6d 21h 28m 17s	normal

`show devices device interfaces interface | tab` – view the current status of all interfaces on all devices in a table. You can also specify a single device or single interface e.g. `show devices device ntd-120 interfaces interface xe-1/1`.

NAME	NAME	ROLE	MAC ADDRESS	TYPE	OPER STATE	LINK SPEED	LINK DUPLEX	NTU	RECEIVED PACKETS	TRANSMITTED PACKETS	RECEIVED BYTES	TRANSMITTED BYTES	RECEIVED DROPPED PACKETS	RECEIVED ERROR PACKETS	TRANSMITTED ERROR PACKETS	TRANSMITTED DROPPED PACKETS	RESTARTS
BYPASS1	xe-1/1	network	00-00-00-00-00-00	marvell	up	nb10000	full	0	14368977230	3616	919615008236	250412	0	0	0	0	0
	xe-1/2	network	00-00-00-00-00-00	marvell	up	nb10000	full	0	3616	2513313177	250412	160852508044	0	0	0	0	0
	xe-1/3	inspection	00-00-00-00-00-00	marvell	up	nb10000	full	0	21990355	14343921270	1407401788	918011426796	0	0	0	0	0
	xe-1/4	inspection	00-00-00-00-00-00	marvell	up	nb10000	full	0	2488286416	21990419	159250796140	1407405004	0	0	0	0	0
NTD1	xe-1/1	external	00-10-d1-70-0b-f0	mpipe	up	nb10000	full	1500	12782135153	21785693	818856662520	1394280552	0	0	0	0	0
	xe-1/2	internal	00-10-d1-70-0b-f1	mpipe	up	nb10000	full	1500	21785693	2476209823	1394280552	158476805480	0	0	0	0	0
	xe-1/3	external	00-10-d1-70-0b-f2	mpipe	down	unknown	half	0	0	0	0	0	0	0	0	0	0
	xe-1/4	internal	00-10-d1-70-0b-f3	mpipe	down	unknown	half	0	0	0	0	0	0	0	0	0	0

show segments segment | repeat 10 – view the current status of all segments in the CMS and update the information every 10 seconds. You can also specify a single segment e.g. show segments segment ntd-120 1.

DEVICE	ID	SEGMENT	NTD EXTERNAL INTERFACE	NTD EXTERNAL INTERFACE LINK SPEED	NTD INTERNAL INTERFACE	NTD INTERNAL INTERFACE LINK SPEED	NBA EXTERNAL INTERFACE	NBA EXTERNAL INTERFACE LINK SPEED	NBA INTERNAL INTERFACE	NBA INTERNAL INTERFACE LINK SPEED	OPERATING MODE	INBOUND RX RATE	INBOUND TX RATE	OUTBOUND RX RATE	OUTBOUND TX RATE	CURRENT INUSE	BYPASS STATE	CURRENT INUSE	BYPASS STATE
NTD	1	normal	xe-1/1	up	10000	xe-1/2	up	10000	xe-1/3	up	10000	mitigate	27	0	0	0	automatic	disabled	not-applicable
NTD	2	normal	xe-1/3	down	0	xe-1/4	down	0	-	-	-	mitigate	0	0	0	0	not-applicable	not-applicable	not-applicable

show statistics segment – view statistics for all segments in the CMS. You can also specify a single segment e.g. show statistics segment ntd-120 1.


```

statistics segment NTD 1
interface-statistics external-port-packet-receive-rate 48998
interface-statistics external-port-bit-receive-rate 25
interface-statistics external-port-packet-transmit-rate 32
interface-statistics external-port-bit-transmit-rate 0
interface-statistics internal-port-packet-receive-rate 32
interface-statistics internal-port-bit-receive-rate 0
interface-statistics internal-port-packet-transmit-rate 160
interface-statistics internal-port-bit-transmit-rate 0
interface-statistics external-port-received-packets 4068849001
interface-statistics external-port-transmitted-packets 7681815
interface-statistics external-port-received-bytes 260406340320
interface-statistics external-port-transmitted-bytes 491638300
interface-statistics internal-port-received-packets 7681815
interface-statistics internal-port-transmitted-packets 265917314
interface-statistics internal-port-received-bytes 491638300
interface-statistics internal-port-transmitted-bytes 17018712288
interface-statistics external-port-ingress-dropped-packets 0
interface-statistics external-port-egress-dropped-packets 0
interface-statistics internal-port-ingress-dropped-packets 0
interface-statistics internal-port-egress-dropped-packets 0
interface-statistics external-port-received-bad-crc-packets 0
interface-statistics internal-port-received-bad-crc-packets 0
interface-statistics external-port-received-oversized-packets 0
interface-statistics internal-port-received-oversized-packets 0
interface-statistics external-port-received-jabber-packets 0
interface-statistics internal-port-received-jabber-packets 0
interface-statistics external-port-transmit-error-packets 0
interface-statistics internal-port-transmit-error-packets 0
statistics segment NTD 2
interface-statistics external-port-packet-receive-rate 0
interface-statistics external-port-bit-receive-rate 0
interface-statistics external-port-packet-transmit-rate 0
interface-statistics external-port-bit-transmit-rate 0
interface-statistics internal-port-packet-receive-rate 0
interface-statistics internal-port-bit-receive-rate 0
interface-statistics internal-port-packet-transmit-rate 0
interface-statistics internal-port-bit-transmit-rate 0
interface-statistics external-port-received-packets 0
interface-statistics external-port-transmitted-packets 0
interface-statistics external-port-received-bytes 0
interface-statistics external-port-transmitted-bytes 0
interface-statistics internal-port-received-packets 0
interface-statistics internal-port-transmitted-packets 0
interface-statistics internal-port-received-bytes 0
interface-statistics internal-port-transmitted-bytes 0
interface-statistics external-port-ingress-dropped-packets 0
interface-statistics external-port-egress-dropped-packets 0
interface-statistics internal-port-ingress-dropped-packets 0
interface-statistics internal-port-egress-dropped-packets 0
interface-statistics external-port-received-bad-crc-packets 0
interface-statistics internal-port-received-bad-crc-packets 0
interface-statistics external-port-received-oversized-packets 0
interface-statistics internal-port-received-oversized-packets 0
interface-statistics external-port-received-jabber-packets 0
interface-statistics internal-port-received-jabber-packets 0
interface-statistics external-port-transmit-error-packets 0
interface-statistics internal-port-transmit-error-packets 0

```

show statistics all rule-statistics – view statistics for all rules in the CMS.

RULE NAME	RULE DESCRIPTION	BLOCK EVENT COUNT	BLOCK PACKET COUNT	BLOCK BYTE COUNT	DETECT EVENT COUNT	DETECT PACKET COUNT	DETECT BYTE COUNT	BLOCK PACKET RATE	DETECT PACKET RATE	BLOCK BIT RATE	DETECT BIT RATE
cms-001032	UDP source port 1080 packet (possible UDP amplification attack)	150777	150777	9046028	0	0	0	0	0	0	0
cms-001034	UDP source port 111 packet (possible RPC Portmapper amplification attack)	0	0	0	150772	150772	9046320	0	0	0	1
cms-001039	UDP source port 19 packet (possible CHARGEN amplification attack)	150772	150772	9046320	0	0	0	0	0	0	1
cms-001042	UDP source port 520 packet (possible RDP amplification attack)	150772	150772	9046320	0	0	0	0	0	0	1
cms-002023	UDP service flood packet rate to server limited	804910032	804910032	53084601928	0	0	0	43427	0	20	0
cms-002061	Any non-TCP protocol connection from unknown client sent to destination already under DDoS attack	8737323649	8737323649	524239416940	0	0	0	346037	0	100	0

pCLI Overview

The Provisioning Command Line Interface (pCLI) provides the initial interface for configuring SmartWall components. Once you use the setup wizard to configure the application, you can usually perform all other tasks in the corresponding web interfaces. You can return to the pCLI if you need to edit these basic configuration settings later.

Accessing the pCLI

You can access the pCLI using a terminal emulator (e.g. Putty) and an SSH connection.

- For NTD120 or NBA devices, use the following command:
`ssh -p 22 <adminUser>@<deviceIP>`
- For all other devices and application, use the following command:
`ssh -p 2222 <adminUser>@<deviceIP>`

When the pCLI opens, you must log in with the corresponding password for your admin user credentials. The default username/password is admin/smartwall.

Tip: For virtual editions, you can also access the pCLI by opening the console window for that application.

Using the pCLI

You can use commands to access various wizards which enable you to setup or edit your device/application. For example, `setup network` opens a wizard for setting up your device's network settings like IP address or DNS connection.

Note: The pCLI has an auto-complete function which can help you select a command. Tab to the correct option and press Enter to use that command. To view a full list of possible commands, type `help`.

Once you've completed a wizard, you have three options: to `[A]ccept` changes, `[C]hange`, or `[E]xit` without saving. Type the highlighted letter for the option you want to select.

pCLI Commands

There is a pCLI available for the majority of SmartWall products: CMS, SWA, all Defense devices and the NBA (external Bypass device). There are commands which are available in all pCLIs. There are also commands which are unique to specific devices or applications.

Commands available for all applications

pCLI Command	Tasks Available
debug ntpq	Query the NTP daemon.
exit	Log out and close SSH session
help	Show a list of possible pCLI commands
quit	Log out and close SSH session
nslookup <dnsName>	Perform a DNS lookup for a specified name. Use Ctrl-C to return to the top level.
packet-dump mgmt	Perform a packet dump (network trace) on the management interface. You may need to analyze packet traffic on the management network when troubleshooting network issues. Use Ctrl-C to return to the top level.
ping <ipAddress>	Perform a network ping to a specified target. This can be used to test connection to a SWA application or connected devices.
reboot	<p>Reboot the application. Following confirmation, you will be logged out of the pCLI and the application will restart.</p> <p>Caution: Route traffic away from devices before rebooting as this can cause link flaps. Defense devices with external Bypass devices will not create a link flap.</p>
setup	Begin the full setup wizard for the application. For example, in a vCMS pCLI, this includes aaa, network, DNS, and time settings.
setup aaa	<p>Setup the authentication configuration. This enables you to change the admin username and password.</p> <p>Caution: Changing the Admin user's username or password will delete all local users created in the application. You can change the Admin user's password using the GUI without affecting the other accounts.</p>
setup dns	Setup the DNS configuration. This enables you to configure the connection to DNS servers and edit the hostname.

pCLI Command	Tasks Available
setup ip-filter	Enable IP filtering for this application and manage a list of permitted IP addresses who can access the application over the management interface. You can [I]nsert a new IP or [D]elete an existing IP.
setup network	Setup the network configuration for the management interface. This enables you to choose to use DHCP or enter static IP, mask and gateway addresses. You can also configure MTU size. For devices with a secondary interface, you also have the option to enable and configure this in the same way.
setup routes	Setup static routing. You can [I]nsert a new route or [D]elete an existing route
setup time	Setup the time configuration. This includes configuring NTP and the local timezone.
show	Show the current network interface configuration and, for vCMS and vSWA, SecureWatch status.
show app-log	View the application log. Use Ctrl-C to return to the top level.
show arp	Show the ARP cache. Use Ctrl-C to return to the top level.
show audit-log	View the CLI audit log. Use Ctrl-C to return to the top level.
show dns	Show the DNS configuration.
show hwclock	Show the current hardware clock time. Note: For virtual applications, this shows the emulated hardware clock time.
show interface	Show the current network interface status.
show netstat	Show the current network connections.
show routes	Show the routing table.
show system-log	View the system log. Use Ctrl-C to return to the top level.
show time	Show the current system time.

pCLI Command	Tasks Available
show uptime	show uptime – Show the current system uptime.
show version	Show version information. This includes the system UUID, application type, application version, and SXOS version.
shutdown	<p>Shutdown the application. Following confirmation, you will be logged out of the pCLI and the application will shutdown.</p> <p>Caution: Route traffic away from devices before shutting down as this can cause link flaps. Defense devices with external Bypass devices will not create a link flap.</p>
support-account disable	Disable the Corero support account. No confirmation is shown unless it is already disabled; then you will see an error.
support-account enable <token>	Enable the Corero support account. Optionally, you can supply the token used to access the account. To generate a random token, leave blank. No confirmation is shown unless it is already disabled; then you will see an error.
support-account status	View the current Corero support account status.
tail app-log	Tail the application log. Use Ctrl-C to return to the top level.
tail audit-log	Tail the CLI audit log. Use Ctrl-C to return to the top level.
tail system-log	Tail the system log. Use Ctrl-C to return to the top level.
time hwclock-sync	<p>Change the hardware clock to match the system time.</p> <p>Note: For virtual applications, this syncs the emulated hardware clock.</p>
time ntp-sync	Synchronize system clock with NTP server. Only successful if you have configured an NTP server for this application (see <code>setup time</code>).

pCLI Command	Tasks Available
tracert <ipAddress>	Perform a network traceroute on a specified target. Use Ctrl-C to return to the top level.

CMS: Additional commands

pCLI Command	Tasks Available
app-cli	Launch the application CLI. Type <code>exit</code> to return to the pCLI.
package-install <url>	Install a package from the specified URL (SFTP, FTP, HTTP or HTTPS supported). If the package is verified, it is installed immediately after upload.
package-install base64	Install a package from base64-encoded value. Paste the base64 encoded value then press Ctrl-D to complete. If the package is verified, it is immediately installed.
packet-dump secondary	Packet dump on secondary interface. Only available when you have the secondary interface configured (see: <code>setup network</code>). You may need to analyze packet traffic on the secondary network when troubleshooting network issues. Use Ctrl-C to stop and return to the top level.
securewatch disable	Disable the SecureWatch service connection. This command only completes if you have a SecureWatch package installed.
securewatch enable	Enable the SecureWatch service connection. This command only completes if you have a SecureWatch package installed.
setup securewatch	Setup the SecureWatch Proxy configuration. This enables you to use a proxy to connect to SecureWatch over the VPN connection.
show pcli- log	View the pCLI log. Use Ctrl-C to return to the top level.
show securewatch	Show the current SecureWatch status. Use Ctrl-C to return to the top level.
show vpn- log	View the SecureWatch VPN log. Use Ctrl-C to return to the top level. Note: The VPN log is only available once a SecureWatch package is installed.

pCLI Command	Tasks Available
<code>tail pcli-log</code>	Tail the pCLI log. Use Ctrl-C to return to the top level.
<code>tail vpn-log</code>	Tail the SecureWatch VPN log. Use Ctrl-C to return to the top level. Note: The VPN log is only available once a SecureWatch package is installed.

SWA: Additional commands

pCLI Command	Tasks Available
<code>file-copy diagnostics-package <url></code>	Download a diagnostic package from the SWA to a specified URL.
<code>package-install <url></code>	Install a package from the specified URL (SFTP, FTP, HTTP or HTTPS supported). If the package is verified, it is installed immediately after upload.
<code>package-install base64</code>	Install a package from base64-encoded value. Paste the base64 encoded value then press Ctrl-D to complete. If the package is verified, it is immediately installed.
<code>packet-dump secondary</code>	Packet dump on secondary interface. Only available when you have the secondary interface configured (see: <code>setup network</code>). You may need to analyze packet traffic on the secondary network when troubleshooting network issues. Use Ctrl-C to stop and return to the top level.
<code>securewatch disable</code>	Disable the SecureWatch service connection. This command only completes if you have a SecureWatch package installed.
<code>securewatch enable</code>	Enable the SecureWatch service connection. This command only completes if you have a SecureWatch package installed.
<code>setup data-disk</code>	Setup the data disk configuration. You must have at least 1GB unpartitioned free space on the disk to complete this operation.
<code>setup http-proxy</code>	Setup the SWA HTTP Proxy configuration. This enables you to access the analytics server using a HTTP proxy.
<code>setup index</code>	Reconfigure the index sizes with respect to overall disk size.

pCLI Command	Tasks Available
setup securewatch	Setup the SecureWatch Proxy configuration. This enables you to use a proxy to connect to SecureWatch over the VPN connection.
setup service- portal	Setup the service portal connection and enable sending data from SWA.
show data- disk	Show the data disk configuration.
show index	Show the index configuration.
show pcli- log	View the pCLI log. Use Ctrl-C to return to the top level.
show securewatch	Show the current SecureWatch status. Use Ctrl-C to return to the top level.
show vpn-log	View the SecureWatch VPN log. Use Ctrl-C to return to the top level. Note: The VPN log is only available once a SecureWatch package is installed.
ssl- certificates forwarder <URI>	Upload and install SWA Forwarder SSL certificates in PKCS#12 format from specified URI. If the certificate is verified, it is installed immediately after upload.
ssl- certificates https <URI>	Upload and install SWA HTTPS SSL certificate in PKCS#12 format from specified URI. If the certificate is verified, it is installed immediately after upload.
tail pcli- log	Tail the pCLI log. Use Ctrl-C to return to the top level. Note: The VPN log is only available once a SecureWatch package is installed.
tail vpn-log	Tail the SecureWatch VPN log. Use Ctrl-C to return to the top level.

vNTD: Additional commands

pCLI Command	Tasks Available
day0 reload	Reload day0 configuration. Only available when there is configuration in day0cfg file.

pCLI Command	Tasks Available
day0 show	Show day0 configuration. Only available when there is configuration in day0cfg file.
reset-config	Reset application configuration.
show nic	Show NIC information.
watchdog enable	Enable the watchdog.
watchdog disable	Disable the watchdog.
watchdog status	Show the current status of the watchdog.

NTD1100 and NTD280: Additional commands

pCLI Command	Tasks Available
day0 reload	Reload day0 configuration. Only available when there is configuration in day0cfg file.
day0 show	Show day0 configuration. Only available when there is configuration in day0cfg file.
reset-config	Reset application configuration.
show modules	Show module information.
show nic	Show NIC information.
watchdog enable	Enable the watchdog.
watchdog disable	Disable the watchdog.
watchdog status	Show the current status of the watchdog.

NTD120: Additional commands

pCLI Command	Tasks Available
psoc	Invoke the PSOC utility to complete high level device tasks. Caution: Always consult your Corero representative before changing these settings.
reset-config	Reset application configuration.
show console-log	View the console log. Use Ctrl-C to return to the top level.

pCLI Command	Tasks Available
<code>tail console-log</code>	Tail the console log. Use Ctrl-C to return to the top level.

NBA: Additional commands

pCLI Command	Tasks Available
<code>bypass-tools</code>	Invoke bypass tools utility. Caution: Always consult your Corero representative before changing these settings.
<code>psoc</code>	Invoke the PSOC utility to complete high level device tasks. Caution: Always consult your Corero representative before changing these settings.
<code>reg-tools</code>	Invoke reg tools utility. Caution: Always consult your Corero representative before changing these settings.
<code>reset-config</code>	Reset application configuration.
<code>restart-port port <number></code>	Restart a specified port.
<code>reset-port-stats [port <number>]</code>	Reset port statistics for all ports or a specified port.
<code>show console-log</code>	View the console log. Use Ctrl-C to return to the top level.
<code>show port-all [port <number>]</code>	Show all port information for all ports or a specified port.
<code>show port-diags [port <number>]</code>	Show port diagnostics for all ports or a specified port.
<code>show port-sfp [port <number>]</code>	Show port sfp info for all ports or a specified port.
<code>show port-stats [port <number>] [detail]</code>	Show port statistics for all ports or a specified port. You can also append the command with detail to include additional information.

pCLI Command	Tasks Available
<code>show port-status [port <number>]</code>	Show port status for all ports or a specified port.
<code>show power</code>	Show the current bypass power status.
<code>show state</code>	Show the current bypass state.
<code>show status</code>	Show the current bypass status.
<code>tail console-log</code>	Tail the console log. Use Ctrl-C to return to the top level.

CMS REST API Overview

As well as being able to edit a Policy through the Web UI and CLI, you can edit some features using the SmartWall Central Management Server REST API. You can access online documentation for the REST API in your browser.

Caution: If another user needs to log into the REST API on the same computer, you must first close your browser session to log out otherwise the REST API session will retain your credentials.

Using the REST API

You can use any tool, that enables you to send http requests to a URL, to interact with the CMS REST API. For example, cURL, the UNIX/Linux command line tool, or Postman, the REST client for Google Chrome. You can also send individual requests using the Swagger REST API documentation web interface.

Versions

When a new version of the API is released the old version will be supported at least for the next release. This current version of the REST API is **v4**. v2, v3, and v4 are still supported.

Available operations

The CMS REST API supports the following HTML operations:

- **GET** – Retrieves and displays information about a known resource or list of resources.
- **PUT** – Creates new resources or edits existing ones. This can be a single resource or multiple resources.
- **DELETE** – Removes a known resource.

Tip: You can use the REST API to bulk add or bulk delete objects. For example, you could delete multiple Address Groups in one operation.

You can use these methods to perform operations in the following areas:

- Viewing the status of your managed devices

- Managing Protection Profiles and Policy:
 - Protection Profiles:
 - Managing your Protection Profiles (bulk add and delete available)
 - Inspection Control:
 - Configuring the default inspection mode and managing override entries (bulk add and delete available)
 - Source Control:
 - Managing Source Control entries (bulk add and delete available)
 - Packet Rules:
 - Configuring Packet-Rules
 - Flex-Rules:
 - Configuring the Block Only rule and managing filters on that rule (bulk add and delete available for filters)
 - Configuring the Detect Only rule and managing filters on that rule (bulk add and delete available for filters)
 - Configuring the General rules and managing filters on those rules (bulk add and delete available for filters)
 - Configuring the Programmable rules and managing filters on those rules (bulk add and delete available for filters)
 - Managing Flex-Rule IP Tables (bulk add and delete available)
 - Smart-Rules:
 - Configuring ICMP Smart-Rules (bulk add and delete available for ICMP v4 types, v6 Types, and Dest ports)
 - Managing Programmable ICMP Smart-Rules (bulk add and delete available)
 - Configuring Reflection Smart-Rules
 - Managing Custom Reflection Smart-Rules (bulk add and delete available)
 - Managing Programmable Reflection Smart-Rules (bulk add and delete available)
 - Configuring Server Smart-Rules
 - Managing Custom Server Smart-Rules (bulk add and delete available)
 - Managing Programmable Server Smart-Rules (bulk add and delete available)
 - Configuring Service Smart-Rules
 - Managing Custom Service Smart-Rules (bulk add and delete available)
 - Managing Programmable Service Smart-Rules (bulk add and delete available)
 - Configuring Source Smart-Rules
 - Managing Programmable Source Smart-Rules (bulk add and delete available)
 - Address Groups:
 - Managing Address Groups

- Managing BGP Mitigation:
 - RTBH:
 - Configuring Auto-withdraw delay and initial states for new black holes
 - Managing black hole entries in the addresses table
 - Sending activation or withdraw requests for black hole routes
 - Flow Spec:
 - Configuring Auto-withdraw delay and initial states for new Flow Spec routes
 - Managing Flow Spec routes
 - Sending activation or withdraw requests for Flow Spec routes

HTML return codes

The CMS REST API supports the following HTML return codes:

Code	Message	Description
200	OK	Your request was completed successfully, and a response is returned.
201	Created	Your requested resource was created. The news resource URI is returned in the “Location” header.
202	Accepted	Your request was accepted but has not been executed (and may not be executed).
204	No Content	Your request was completed successfully but there is no response to return.
400	Bad Request	Your request could not be processed because it contains missing or invalid information (for example a validation error on an input field or a missing required value).
403	Forbidden	You cannot access this resource with the credentials given.
404	Not Found	The resource you requested does not exist.
408	Request Timeout	The request took too long to complete and was rejected by the server.
409	Conflict	The resource you are trying to create already exists.
412	Precondition Failed	The server has failed one of the preconditions of the request.
423	Locked	The resource you are trying to access has been locked.

Code	Message	Description
422	Unprocessable Entity	Unable to process the request because of semantic errors.
500	Generic Server Error	There is an internal server error which has prevented your request being processed.
501	Not Implemented	The server does not recognize the request, most likely because this is a new API operation which has not yet been implemented.

Tip: After you send a request, if you see the HTTP return code "204 No Content", that doesn't mean your request has failed just that the CMS does not have anything to return after success. Also, when you're performing operations from Swagger, the 404 message "Ancestor instance does not exist" usually means the Protection Profile name you provided does not exist.

Accessing the REST API documentation

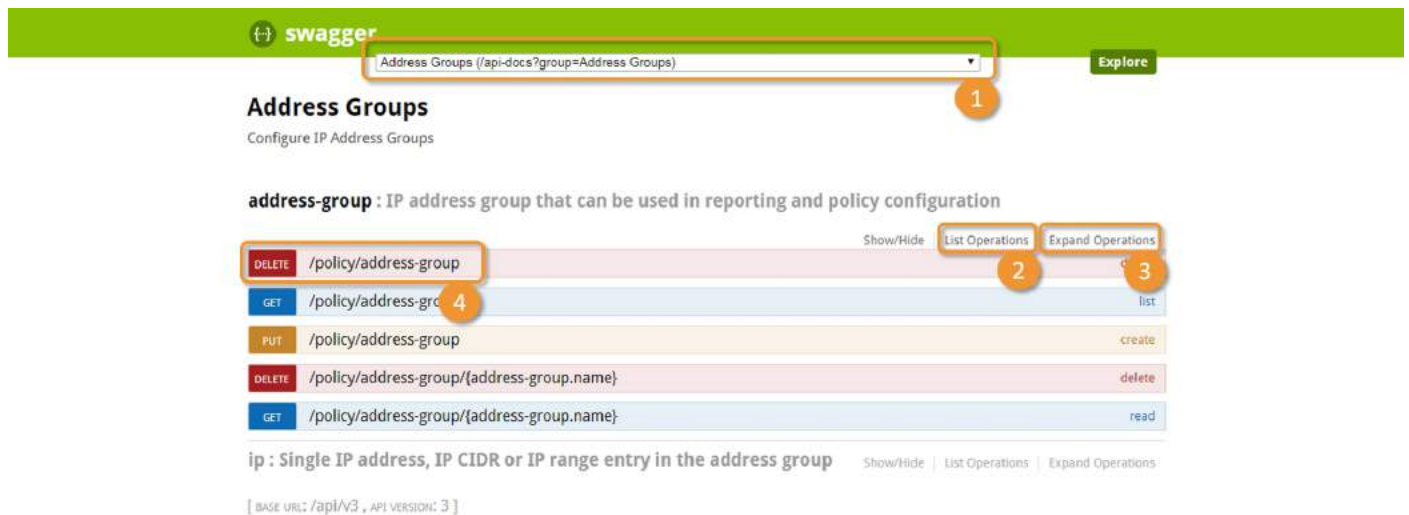
To access the current version of the REST API

1. Open a browser.
2. Type the following URL: **`https://<cmsIPaddress>/api`**
3. Log in with your CMS user credentials.
4. The Swagger web interface for the current version of the CMS REST API opens. You can see the version number in the URL.

To access other versions of the REST API

1. Open a browser.
2. Type the following URL: **`https://<cmsIPaddress>/api/<versionNumber>/swagger-ui.html`**. Replacing `<versionNumber>` with the version number you need to access, e.g. **v4**.
3. Log in with your CMS user credentials.
4. The Swagger web interface for that version of the CMS REST API opens. You can see the version number in the URL.

Using the Swagger web interface



When you first open the Swagger web interface, you are in the first category of REST API operations: **Address Groups** (1). Use the drop-down at the top of the screen to navigate between categories.

To view a set of operations within a category, click **List Operations** (2). To view that list expanded, click **Expand Operations** (3). To expand a single operation in a set, click on the operation title (4).

Within each operation you can view the API model, an example value, the necessary parameters, and a list of possible response messages.

Within the Swagger interface, you can perform the operation by filling in any applicable parameter values and clicking **Try it out!**.

Tips for using Swagger to perform operations:

- For PUT operations where you require a body, click the Example Value to the right of the body field to populate the body field with the example text. You can then replace the placeholder strings with your own values. This ensures the body is formatted correctly.
- Swagger does not stop you entering invalid values in parameters (for example, a string value in a field expecting a number value, like a Smart-Rule Threshold). You will see an error when you perform the operation.
- Once you perform an operation, you will also see a cURL example of the same command.

- If the response body contains a long message, it can be truncated. To see the full message, run the same operation in cURL.
- When making a large number of changes quickly via REST, you can customize the timeout for the device commit by specifying an additional header in the request: `Device-Commit-Timeout`. The value should be a uint32, i.e. (0..4294967295) and represents the timeout in milliseconds. If not provided this defaults to 60000 (1 minute).

REST API Examples

The following sections show notable examples for using certain operations and an example of using the REST API in two different REST clients.

Operation examples

Using the Programmable Flex-Rules

Programmable Flex-Rule are reserved for use with integrated systems able to send REST API calls to add or update Flex-Rule Filters as needed by analyzing your incoming attack traffic. To do this, you need to first configure a Programmable Flex-Rule (cns-002501, cns-002600, cns-002601, cns-002602, cns-002603, cns-002604, cns-002605, cns-002606, cns-002607, cns-002608, cns-002609, or cns-002610) and then you can send operations that add filters to that rule.

Configure a Programmable Flex-Rule to have the Rule Action and Match Rate Limit you need:

```
curl -k -u admin:smartwall -X PUT --header 'Content-Type: application/json' --header
'Accept: */*' -d '{ \
"items": [ \
{ \
"id": "cns-002501", \
"matchRateLimit": 0, \
"name": "standard_http_ports", \
"ruleAction": "block" \
} \
] \
}' 'https://10.10.143.87/api/v2/policy/protection-profile/default/flex-rule-
blocking/programmable'
```

Add a new filter to that Flex-Rule:

```
curl -k -u admin:smartwall -X PUT --header 'Content-Type: application/json' --header
'Accept: */*' -d '{ \
"items": [ \
```

```
{ \
  "adminState": "enabled", \
  "definition": "tcp and dst port 80", \
  "name": "http_filter" \
} \
] \
}' 'https://10.10.143.87/api/v2/policy/protection-profile/default/flex-rule-
blocking/programmable/cns-002501/filter'
```

Deleting objects from a list

When there is a possible list of objects, you will have two different Delete operations available. One for deleting a single object, and one for deleting multiple objects. For example, in the Swagger documentation:

- **DELETE /policy/protection-profile** – Enables you to write a json list containing all the objects you need to delete
- **DELETE /policy/protection-profile/ {protection-profile.name}** – Enables you to specify a single object to delete from the list

If you wanted to delete two Protection Profiles, your operation body may look like this, with objects separated by a comma between the curly brackets:

```
{
  "items": [
    {
      "name": "Profile1"
    },
    {
      "name": "Profile2"
    }
  ]
}
```

Adding multiple objects to a list

When you want to add more than one object in a single REST API operation (for example, adding multiple Address Groups or Flex-Rules), you need to separate the objects in the body using a comma between the curly brackets. For example, to add two Address Groups at the same time the body may look like the following:

```
{
  "items": [
```



```
{
  "description": "group1 description",
  "name": "Group 1"
},
{
  "description": "group2 description",
  "name": "Group 2"
}
]
```

Interface examples

The following two examples show how to create a new Flex-Rule filter on the Block-Only Flex-Rule in the default Protection Profile.

cURL

If you're working in UNIX/Linux you can use cURL in the terminal to send requests to the CMS. In the table below, the following example operation for creating a new Flex-Rule filter is broken down into its fields:

```
curl -k -u [username:password] -X PUT --header 'Content-Type: application/json' --
header 'Accept: */*' -d '{ \
  "items": [ \
    { \
      "adminState": "enabled", \
      "definition": "udp and dst host 10.10.111.222 and src port 520", \
      "name": "RIPblock" \
    } \
  ] \
}' 'https://[cmsipaddress]/api/v2/policy/protection-profile/default/flex-rule-
blocking/block-only/filter'
```

Example	Description
curl	Access cURL

Example	Description
<code>-k</code>	By default the CMS is installed with a self-signed certificate which will not be trusted by your client machine. You can use the <code>-k</code> option to run the command in 'insecure' mode or you can install a new, valid, certificate which is part of a trust chain known to your client machine.
<code>-u [username:password]</code>	Authentication. After <code>-u</code> include your username and password separated by a colon, e.g. <code>admin:smartwall</code> .
<code>-X PUT</code>	HTTP method
<code>PUT --header 'Content-Type: application/json' --header 'Accept: */*'</code>	Header

Example	Description
<pre>-d '{ \ "items": [\ { \ "adminState": "enabled", \ "definition": "udp and dst host 10.10.111.222 and src port 520", \ "name": "RIPblock" \ } \] \ }'</pre>	Body
<pre>'https://[cmsipaddress]/api/v2/policy/protection-profile/default/flex-rule-blocking/block-only/filter'</pre>	URL. Replace [cmsipaddress] with the IP address of your CMS.

Postman

A REST client, like Postman, provides a structured form for sending HTTP requests. You can also use it to save your common requests and view a history of the requests you have sent.

The basic method for sending a request to the CMS is:

1. Authenticate to your CMS, using the browser associated with your REST client.
2. In **Authorization**, from the **Type** drop-down select **Basic Auth** and type your admin **Username** and **Password**.
3. Select the **HTTP** method from the drop-down menu (for example, **PUT**).
4. Type in the **URL** (for example, `https://[cmsipaddress]:443/api/v2/policy/protection-profile/default/flex-rule-blocking/block-only/filter`).
5. In **Body**, select the **Raw** radial button.
6. Type the body information into the text field (for example, `{"adminState":"enabled", "name":"RIPblock", "definition":"udp and dst host 10.10.111.222 and src port 520"}`).
7. In **Header**, add the **Key** "Content-Type" and the Value "application/json".
8. Click **Send**.

Tip: When you want to create or update multiple objects, the REST API performs best when you send a bulk change rather than making multiple REST API calls in a row.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://corero.force.com/support>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

Requesting Licenses

The system requires a TDD license key, plus keys for each vNTD, to become fully operational. Juniper devices do not require license keys to support the solution. To obtain the keys, please contact the Corero Customer Services team by one of the following methods:

- Email: Support.Portal@corero.com
- Web: <https://corero.force.com/support>
- Telephone: Dial +1.978.212.1500 -> Select Option 2

GLOSSARY

A

Activation Threshold

In Global Threat Awareness, the Activation Threshold is the rate of the new connections (new IP address or TCP setup) which indicates an attack on your system. When the rate crosses that Threshold, the Global Threat Awareness action is triggered.

See Also: [Global Threat Awareness](#), [Exit Threshold](#), [trigger](#)

Address Group

An Address Group is a set of related IP addresses which you can use (and reuse) in multiple Protection Profiles. In addition to its use in Protection Profiles, the Address Group associated with an IP address can be made visible as part of any Security Event or sFlow syslog messages sent to SmartWall SecureWatch Analytics (SWA). This enables you to perform searches aimed at a specific Address Group. If you associate a name with an individual IP address it can also appear in the messages.

See Also: [Policy](#), [attack mitigation feature](#), [syslog message](#)

admin state

The admin state of a feature or object (e.g. Flex-Rule filter, override entry, etc) can be set to:

- **Enabled** – When triggered the feature or object performs as specified
- **Disabled** – The feature or object cannot be triggered

See Also: [trigger](#), [Flex-Rule filter](#), [override entry](#)

Alarm

An Alarm is created when something happens in the SmartWall Threat Defense System which may require your attention. It tells you what has occurred and where in the system. You can view them in the Alarm Center.

See Also: [SmartWall Threat Defense System](#)

analytics

Analytics is the processing and display of information (sFlow, event logs, and syslog messages) from the SmartWall Central Management Server and SmartWall devices. It can be viewed and analyzed in SmartWall SecureWatch Analytics.

See Also: [SmartWall SecureWatch Analytics](#), [SmartWall Central Management Server](#), [SmartWall device sFlow](#), [events](#), [syslog messages](#)

Analytics Server

A server running the SmartWall SecureWatch Analytics application.

See Also: [SmartWall SecureWatch Analytics](#), [Syslog Server](#)

assets

See: protected assets

attack mitigation feature

Attack mitigation feature is a general name for any of the features that make up a Policy.

See Also: [Policy](#)

attack rules

See: [Packet Rules](#)

attack traffic

Attack traffic is external traffic (coming from the internet) which the Policy has determined is untrustworthy.

See Also: [non-attack traffic](#), [Policy](#)

Authentication Group

An Authentication Group manages the authentication credentials which the SmartWall Central Management Server (CMS) uses to connect with the SmartWall devices.

See Also: [SmartWall device](#), [SmartWall Central Management Server](#)

B

Berkeley Packet Filter syntax

The syntax used to create Flex-Rule filter definitions.

See Also: [Flex-Rule filters](#), [Flex-Rules](#)

Black List

See: [Inspection Mode \(Inspection Control\)](#), [Source Control](#)

Block

See: [Rule Action](#)

Bypass device

See: [SmartWall Network Bypass Appliance](#)

Bypass Mode

Some SmartWall devices include Bypass capability which directs all traffic to the internal network before it reaches the Defense device's Policy.

See Also: [SmartWall device](#), [Policy](#), [SmartWall Network Threat Defense](#)

C

CLI

The Command Line Interface of the SmartWall Central Management Server

See Also: [Web UI](#), [SmartWall Central Management Server](#)

Cluster

A Cluster is a set of identically configured Defense devices. When you create a new Cluster, you must associate it with a Protection Profile; this Protection Profile contains a Policy which controls how the devices in that Cluster respond to traffic. A single SmartWall Central Management Server (CMS) can control up to 16 Clusters. After installation, the CMS initially has a single default Cluster which is associated with the default Protection Profile and default Authentication Group.

See Also: [Protection Profile](#), [SmartWall device](#), [SmartWall Central Management Server](#)

CMS

See: [SmartWall Central Management Server](#)

cns-admin

See: [local user](#)

cns-defense

See: [local user](#)

cns-monitor

See: [local user](#)

commit

When you commit a change in the CLI or Web UI, you save that change and push that change to any affected SmartWall devices.

See Also: [CLI](#), [Web UI](#), [SmartWall device](#)

Connection State

The Connection State of a device provides information on whether the SmartWall Central Management Server and the device are currently connected. This is aggregated with Deployment State in the Devices table, but visible in the CLI and the Software Upgrade screen.

See Also: [SmartWall device](#), [Deployment State](#), [Deployment Action](#), [CLI](#), [SmartWall Central Management Server](#)

D

DDoS Attack

A distributed denial of service (DDoS) attack is an event in which multiple sources assault a destination server with a volume of traffic that overwhelms that server's ability to respond to any traffic at all, making it unavailable to the legitimate traffic for which it is intended. DDoS attacks can take many different forms and exploit a wide variety of protocol behaviors and design features to achieve their goal of making a server unavailable.

Defense device

See: [SmartWall Network Threat Defense device](#)

Defense Mode

The Defense Mode, tells devices how to handle incoming traffic. It can be one of the following modes:

- **Mitigate** – Inspect the traffic and, if it triggers a rule in an attack mitigation feature, honor that rule action (to block, allow, or detect the packet)
- **Monitor** – Inspect the traffic without dropping any packets. If a packet triggers a Rule Action, send a syslog message indicating the Rule Action but do not block any traffic.
- **Pass-through** – Send all traffic to the internal network without inspecting any packets.

Note: There is a Global Defense Mode for the CMS which you can choose to override for specific Clusters, devices, or Segments.

See Also: [SmartWall device](#), [Segment](#)

definition (Flex-Rule filter)

See: [Flex-Rule filter](#)

Deployment Action

The Deployment Action of a device provides information on whether that device is currently performing a system action.

See Also: [SmartWall device](#), [Connection State](#), [Deployment State](#)

Deployment State

The Deployment state of a device provides information on the status of the Policy on the device. This is aggregated with Connection State in the Device Summary table, but visible on its own in the CLI.

See Also: [SmartWall device](#), [Connection State](#), [Deployment Action](#), [CLI](#), [Policy](#)

Destination-Based Threat Awareness

Destination-Based Threat Awareness identifies when the rate of new connections, to a single destination, and uses a Threshold to identify if it has risen to attack

levels. It can then drop untrustworthy connections. If the rate of new connections rises to a dangerously high level, it can use a Rate Limit to drop all connections above the specified rate.

See Also: [Threat Awareness](#), [Global Threat Awareness](#), [Threshold](#), [Rate Limit](#)

Detect

See: [Rule Action](#)

device

See: [SmartWall device](#)

E

event

An event is logged when a rule is triggered in a Defense device. A summary of the events are sent to SmartWall SecureWatch Analytics for analysis.

See also: [rule](#), [trigger](#), [syslog message](#), [SmartWall SecureWatch Analytics](#), [SmartWall device](#)

Exit Threshold

In Global Threat Awareness, the Exit Threshold is the rate of the new connections (new IP address or TCP setup) which indicates there is no longer an attack on your system. When that Threshold is passed, if Threat Awareness mode was active, it is disabled.

See Also: [Global Threat Awareness](#), [Activation Threshold](#), [trigger](#)

external user

A SmartWall Central Management Server (CMS) user who is authenticated using external credentials through LDAP. Their LDAP group is mapped to a local CMS user role.

See also: [local user](#), [SmartWall Central Management Server](#)

F

filter

See: [Flex-Rule filter](#)

filter syntax

See: [Berkeley Packet Filter syntax](#)

Flex-Rules

An attack mitigation feature which enables you to define custom filters which can block or detect specific packets. There are three Flex-Rules you can customize using filters; Block-only, Detect-only, and Programmable.

See Also: [Flex-Rule filter](#), [attack mitigation feature](#)

Flex-Rule filter

You can add a Flex-Rule filter to a Flex-Rule to define a packet type which that Flex-Rule will act on. For example, if a packet matches the definition of a filter on the Block-only Flex-Rule, then that packet is blocked.

See Also: [Flex-Rules](#), [Berkeley Packet Filter syntax](#)

force-sync

The action for returning a device to the in-sync state after an error has pushed it out of sync.

See Also: [in-sync](#), [sync](#), [SmartWall device](#), [Deployment State](#)

G

Global Threat Awareness

Global Threat Awareness enables you to set network level Activation and Exit Thresholds for Threat Awareness mode.

See Also: [Threat Awareness](#), [Destination-Based Threat Awareness](#), [Activation Threshold](#), [Exit Threshold](#)

ICMP Smart-Rule

An ICMP Smart-Rule looks for a flood of packets with ICMP error messages.

See Also: [Smart-Rules](#)

in-sync

The Deployment State of a device when the device Policy is up to date with all changes committed in the CMS.

See Also: [sync](#), [force-sync](#), [SmartWall device](#), [Deployment State](#)

Inspect

See: [Inspection Mode](#)

Inspection Control

An attack mitigation feature which enables you to set a default Inspection Mode for traffic going to your destination IP addresses and set exceptions (called override entries) to that mode for specific destination IP addresses, ranges, and subnets.

See Also: [Inspection Mode](#), [attack mitigation feature](#)

Inspection Mode

The Inspection Mode of each override entry tells the Defense device how to handle traffic going to the specified destination IP addresses in that override entry, and the Default Inspection Mode tells the Defense device how to handle everything else not specified in an override entry. It can be one of four modes:

- **White List** – Allow the traffic into the internal network without any further inspection by the attack mitigation features

- **Black List** – Drop the traffic without any further inspection by the attack mitigation features
- **Monitor** – Inspect the traffic without dropping any packets. If a packet triggers a Rule Action, send a syslog message indicating the Rule Action but do not block any traffic.
- **Inspect** – (Default) Treat the traffic as specified by the Defense Mode. If the Defense Mode is Pass-through, traffic is never inspected or subjected to Inspection Control.

See Also: [Inspection Control](#)

L

Link State Propagation

When Link State Propagation is enabled, if one interface in a Segment goes down then the other interface is also brought down. This prevents an external interface from continuing to receive traffic after its linked internal interface has gone down.

See Also: [Segment](#)

local user

A SmartWall Central Management Server (CMS) user who is authenticated using local credentials managed by the CMS. They can be assigned one of three CMS user roles:

- **cns-admin** – The administrative role. An admin user can edit all **Policy**, **Network**, and **System** configurations, including managing users.
- **cns-defense** – A non-administrative role which enables its users to edit all **Policy** options but no Network or System administrative settings
- **cns-monitor** – A primarily read-only role which enables its users to view settings without being able to enact any changes (aside from their own password)

See Also: [external user](#), [SmartWall Central Management Server](#)

M

Management Controller

See: [SmartWall Management Controller](#)

Match Rate Limit

Match Rate Limit is the number of packets that need to match a Flex-Rule filter before it triggers the Rule Action.

See Also: [Flex-Rule](#), [Flex-Rule filter](#), [Rule Action](#)

Mitigate

See: [Defense Mode](#)

Monitor

See: [Defense Mode](#) , [Inspection Mode](#)

N

NBA

See: [SmartWall Network Bypass Appliance](#)

non-attack traffic

Non-attack traffic is external traffic (coming from the internet) which the Policy has determined is trustworthy.

See Also: [attack traffic](#), [Policy](#)

Notification

In the SmartWall Central Management Server Web UI, notifications inform you of your successful and unsuccessful operations.

See Also: [SmartWall Central Management Server](#)

NTD

See: [SmartWall Network Threat Defense device](#)

NTD1100

The 100G Defense device.

See: [SmartWall Network Threat Defense device](#)

NTD280

A Defense device which can contain multiple 10G modules.

See: [SmartWall Network Threat Defense device](#)

NTD120

A 10G Defense device.

See: [SmartWall Network Threat Defense device](#)

O

Operating Mode

There are two types of Operating Mode: Defense Mode and Bypass Mode. These are set at a global level but can be overridden for specific Clusters, devices, or Segments.

See Also: [SmartWall device](#), [Segment](#), [Cluster](#), [Defense Mode](#), [Bypass Mode](#)

override entry

In Inspection Control, override entries are specified groups of destination IP addresses which you want the Defense device to handle differently to the default Inspection Mode in Inspection Control.

See Also: [Inspection Control](#), [Inspection Mode](#)

P

Packet Rules

A Packet Rule is an attack mitigation feature which checks the incoming packet to see if it has any anomalies that could indicate it is an attack packet, or if it is one of the common reflection attack packet types. There are two types of Packet Rule:

- **attack rules** – Identifies common traffic types used in reflection attacks
- **validation rules** – Looks for a simple anomaly in a packet which indicates that the packet is either corrupted or not trustworthy.

See Also: [attack mitigation feature](#)

Packet Validation Rules

See: [Packet Rules](#)

Pass-through

See: [Defense Mode](#)

pCLI

The Provisioning Command Line Interface is used for initial configuration of the SmartWall components.

See Also: [setup wizard](#)

Policy

A Policy is a configuration of the attack mitigation features which tells the Defense devices how to handle incoming traffic. Each Policy is contained in a Protection Profile.

See Also: [attack mitigation features](#), [Protection Profile](#)

probation interval

The time between an IP address being identified as untrusted by the Defense device and when it can attempt a new connection.

See Also: [untrusted IP address](#)

protected assets

Destination IP addresses whose traffic travels through the SmartWall Threat Defense System before it reaches them.

See Also: [SmartWall Threat Defense System](#)

Protection Profile

A Protection Profile is a container for a configuration of the attack mitigation features known as a Policy.

See Also: [Policy](#), [attack mitigation features](#)

R

Rate Limit

A Rate Limit, in Smart-Rules, is the rate of traffic which is still allowed through after Threshold has been crossed.

A Rate Limit, in Destination-Based Threat Awareness, is the rate of traffic which triggers the Rate Limit Rule Action which can block traffic above the Rate Limit.

See Also: [Smart-Rules](#), [Threshold](#), [Destination-Based Threat Awareness](#), [Rule Action](#)

reachable

When a device is reachable, it can communicate with the CMS.

See Also: [SmartWall device](#), [SmartWall Central Management Server](#)

Reflection Smart-Rule

A Reflection Smart-Rule looks for a flood of packets with the same source port.

See Also: [Smart-Rules](#)

rule

Every attack mitigation feature is generated from a set of rules. It is these rules which a packet can trigger to be blocked or detected by the Defense device.

See Also: [trigger](#), [Rule Action](#), [event](#), [attack mitigation feature](#)

Rule Action

When a rule is triggered it performs a Rule Action. This is usually one of three actions, but some rules have fewer options:

- **Block** – The Defense device blocks all traffic matching the rule definition
- **Detect** – The Defense device inspects all traffic matching the rule definition and sends event syslog messages, but it does not drop the packets
- **Disabled** – The Threshold is disabled, and the matching traffic is not blocked or detected.

See Also: [trigger](#), [rule](#), [event](#)

S

sample packet

See: [sFlow](#)

SecureWatch Service

The Corero service which constantly monitors your Analytics feed, keeps your Policies optimized for your network and responds immediately to an unmitigated attack.

See Also: [Security Operations Center](#)

Security Operations Center

The hub of the Corero SecureWatch Service.

See Also: [SecureWatch Service](#)

Segment

A Segment is a linked external and internal interface defined from a front-panel port pair on a Defense device.

See Also: [SmartWall Network Threat Defense device](#)

Server Smart-Rule

A Server Smart-Rule looks for a flood of packets with the same destination IP address.

See Also: [Smart-Rules](#)

Service Smart-Rule

A Service Smart-Rule looks for a flood of packets with the same destination port.

See Also: [Smart-Rules](#)

setup wizard

The pCLI commands that assist you when you're setting up a new SmartWall device or application.

See Also: [pCLI](#)

sFlow

Sample traffic taken from the traffic coming into a Defense device and sent to the SmartWall Central Management Server.

See Also: [SmartWall Network Threat Defense device](#), [SmartWall Central Management Server](#)

Smart-Rules

An attack mitigation feature which looks for a large number of packets with similar characteristics. Once the number of these packets passes a set threshold, which denotes a flood attack is happening, the Smart-Rule can surgically block just the packets which match those attack characteristics.

See Also: [attack mitigation feature](#), [threshold](#)

SmartWall Central Management Server

The SmartWall Central Management Server (CMS) application is the central hub of the SmartWall Threat Defense System. It is used to define the rules which make up DDoS protection policies, and then push those configurations to all your managed Defense devices, and to send the analytics data to SmartWall SecureWatch Analytics. It can be hosted on a SmartWall Management Controller or as a VM using the SmartWall Central Management Server Virtual Edition.

See Also: [SmartWall Central Management Server Virtual Edition](#), [rule](#), [SmartWall Threat Defense System](#), [SmartWall Network Threat Defense device](#), [SmartWall SecureWatch Analytics](#), [SmartWall Management Controller](#)

SmartWall Central Management Server Virtual Edition

The virtual edition of the SmartWall Central Management Server, hosted as a VM on your own server, rather than on a SmartWall Management Controller.

See Also: [SmartWall Central Management Server](#), [SmartWall Management Controller](#)

SmartWall device

There are two types of SmartWall device: Defense devices and SmartWall Management Controllers. When discussing the SmartWall Central Management Server, SmartWall device most commonly refers to Defense device.

See Also: [SmartWall Central Management Server](#), [SmartWall Management Controller](#), [SmartWall Network Threat Defense device](#)

SmartWall Management Controller

The SmartWall Management Controller is a physical device which you can deploy to centrally manage your Defense devices. It hosts the SmartWall Central Management Server and SmartWall SecureWatch Analytics applications.

See Also: [SmartWall Central Management Server](#), [SmartWall Network Threat Defense device](#), [SmartWall SecureWatch Analytics](#)

SmartWall Network Bypass Appliance

A SmartWall Network Bypass Appliance is a physical device which you can use with a Defense device to ensure no traffic loss in the event of a power failure. The Bypass device sits between the internet and your internal network and, when configured to, sends your traffic to the Defense device and through the Policy. It then receives the traffic back and sends it on to your internal network. In the event of a power failure, the Bypass device sends all traffic directly to your internal network, bypassing the Defense device.

See Also: [SmartWall Network Threat Defense device](#), [Defense Mode](#), [Bypass Mode](#), [Policy](#)

SmartWall Network Threat Defense device

A SmartWall Network Threat Defense device sits between the internet and your internal network, either physically, or logically, inline with the traffic. It uses a Policy to block attack traffic and allow non-attack traffic through to the internal network. It is managed by the SmartWall Central Management Server.

See Also: [SmartWall Central Management Server](#), [attack traffic](#), [non-attack traffic](#)

SmartWall Network Threat Defense Device Virtual Edition

The virtual edition of the physical SmartWall Network Threat Defense device. This can be deployed on your own ESXi or KVM server.

See Also: [SmartWall Network Threat Defense device](#)

SmartWall SecureWatch Analytics

SmartWall SecureWatch Analytics (SWA) is a web portal which stores and indexes events and operational syslog messages from the SmartWall Central Management Server, and displays that information as real-time and historical charts and tables for attack analysis.

See Also: [SmartWall Central Management Server](#), [event](#), [syslog message](#), [SmartWall SecureWatch Analytics Virtual Edition](#)

SmartWall SecureWatch Analytics Virtual Edition

The virtual edition of the SmartWall SecureWatch Analytics, hosted as a VM on your own server, rather than on a SmartWall Management Controller.

See Also: [SmartWall SecureWatch Analytics](#), [SmartWall Management Controller](#)

SmartWall TDS

See: [SmartWall Threat Defense System](#)

SmartWall Threat Defense System

The SmartWall Threat Defense System (SmartWall TDS) is a family of DDoS protection appliances that eliminate DDoS attacks in real-time. It comprises of three distinct components: SmartWall Network Threat Defense devices, the SmartWall Central Management Server, and SmartWall SecureWatch Analytics.

See Also: [SmartWall Central Management Server](#), [SmartWall SecureWatch Analytics](#), [SmartWall Network Threat Defense device](#)

SMC

See: [SmartWall Management Controller](#)

Snapshot

A snapshot is a package which contains the SmartWall Central Management Server configuration from the moment you created it, which you can use to restore the SmartWall Central Management Server to a previous state.

See Also: [SmartWall Central Management Server](#)

Source Control

An attack mitigation feature which enables you to create black list and white list entries for specific source IP addresses, ranges, and subnets.

See Also: [attack mitigation feature](#)

Source Smart-Rule

A Source Smart-Rule looks for a flood of packets with the same source IP address.

See Also: [Smart-Rules](#)

Support token

A randomly generated code which enables a Support user to access your system for troubleshooting purposes.

See Also: [Support user](#)

Support user

A Corero Support Engineer who you have given access to your system by generating a support token.

See Also: [Support token](#)

SWA

See: [SmartWall SecureWatch Analytics](#)

sync

The action for returning a device to the in-sync state after it has fallen out of sync.

See Also: [in-sync](#), [force-sync](#), [SmartWall device](#), [Deployment State](#)

syslog message

A syslog message contains information on security events, system status, traffic information etc in a compressed form. You can learn to read syslog messages in the **Corero SmartWall Syslog Reference Guide**.

See Also: [analytics](#), [SmartWall SecureWatch Analytics](#), [event](#)

Syslog Server

A server running an application which consumes syslog messages

See Also: [Analytics Server](#), [Syslog messages](#)

T

Threat Awareness

An attack mitigation feature which detects high amounts of traffic and, when one or more traffic thresholds are crossed, enters Threat Awareness Mode where it starts to drop new connections from IP addresses that it cannot confirm are trustworthy.

See Also: [Global Threat Awareness](#), [Destination-Based Threat Awareness](#), [attack mitigation feature](#)

Threat Awareness Mode

See: [Threat Awareness](#)

Threshold

You can set a Threshold to trigger a rule when the matching traffic rate reaches that Threshold value.

See Also: [Smart-Rules](#), [Threat Awareness](#), [trigger](#)

trigger

When an incoming packet matches a rule definition it "triggers" that rule to perform the associated Rule Action.

See Also: [rule](#), [Rule Action](#), [trigger](#)

tuning

Tuning a Policy is the name for configuring the attack mitigation features to optimize their ability to block attack traffic in your network.

See Also: [Policy](#), [attack mitigation feature](#), [attack traffic](#)

U

untrusted IP address

An unknown IP address which does not meet the SmartWall Central Management Server's criteria for trustworthy behavior.

See Also: [probation interval](#), [SmartWall Central Management Server](#)

upgrade package

A file containing an updated software version for the SmartWall Central Management Server or for a SmartWall device.

See Also: [SmartWall device](#), [SmartWall Central Management Server](#)

V

validation rules

See: [Packet Rules](#)

vCMS

See: [SmartWall Central Management Server Virtual Edition](#)

Virtual Editions

The collective name for SmartWall applications which are run as VMs on your own servers.

See Also: [SmartWall SecureWatch Analytics Virtual Edition](#), [SmartWall Central Management Server Virtual Edition](#)

vNTD

See: [SmartWall Network Threat Defense Virtual Edition](#)

vSWA

See: [SmartWall SecureWatch Analytics Virtual Edition](#)

W

Web UI

The browser based version of the SmartWall Central Management Server interface.

See also: [CLI](#), [SmartWall Central Management Server](#)

White List

See: Inspection Mode (Inspection Control), Source Control

GLOSSARY

