Exinda How To Guide:

Exinda Mangement Center User Guide

Exinda Management Center Version 1.5.0

© 2016 Exinda Networks Inc.

Copyright

© 2016 Exinda Networks Inc. All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Document Built on Monday, February 29, 2016 at 6:02 PM

Using this guide

Before using this guide, become familiar with the Exinda documentation system. See the following for more information:

© 2016 Exinda Networks Inc.

Documentation conventions

These documentation conventions apply across all of the Exinda documentation sets. All instances of the following may not appear in this documentation

Typographical conventions

- **bold** - Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
- *italics* - Reference to other documents. For example: Refer to the *Exinda Application List*. Also used to identify in the various procedures the response the systems provide after applying an action.
- **>** - Separates navigation elements. For example: Select **File > Save**.
- `monospace text` - Command line text.
- `<variable>` - Command line arguments.
- `[x]` - An optional CLI keyword or argument.
- `{x}` - A required CLI element.
- `|` - Separates choices within an optional or required element.

Links

All links throughout the documentation are **blue**. Most links refer to topics within the documentation, but there may be links that take you to web pages on the Internet. In this documentation we differentiate between these types of links by **underlining** only the external links.

Tips, Notes, Examples, Cautions, etc.

Throughout this manual, the following text styles are used to highlight important information:

- **Tips** include hints and shortcuts. Tips are identified by a pale green background.

> **TIP**
>
> *text*

- **Notes** provide information that is useful at the points where they are encountered. Notes are identified by a light blue background.

> **NOTE:**
>
> *Text*

- **Important** notes provide information that is important at the point where they are encountered. Important notes are identified by a light yellow background.

> **IMPORTANT**
>
> *Text*

- **Cautions** provide warnings of areas of operation that could cause damage to appliances. Cautions are identified by a light red background.

> **CAUTION:**
>
> ***Text***

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a pale green background.

> **EXAMPLE**
>
> Text

- **Best Practices** identify Exinda recommended methods for achieving the best from your Exinda appliances and the Exinda Management Center. Best Practices are identified by their light blue background and the "thumbs-up" icon.

© 2016 Exinda Networks Inc.

Best Practice:

It is a best practice to

© 2016 Exinda Networks Inc.

Table of Contents

© 2016 Exinda Networks Inc.

© 2016 Exinda Networks Inc.

Chapter 1: EMC Overview

The Exinda Management Center (EMC) provides complete management insight and configuration control of your Exinda Network Orchestrator appliances from one central console. All applications, devices, users, and activities across all network locations are managed from a central location giving IT Administrators the ability to manage network policies and manage appliance configuration across the entire organization.

The Exinda Network Orchestrator appliances process the traffic. You can configure the appliances and monitor network usage directly from the appliance. However, once you have more than a few appliances to manage, it can become difficult to manage them individually and maintain standard configurations when needed. The EMC solves the management gap by enabling policy configuration on multiple appliances. When used in conjunction with SDP (Service Delivery Point), you can have aggregated reporting of your network traffic across your appliances and/or reporting of the individual appliances all within a single report.

If deploying an on-premises instance of EMC, you can deploy it as a multi-tenant solution, where each estate is enrolled under a separate tenancy account. Objects and data cannot be shared across tenancies. For a single estate use of EMC, a single tenant is added to the system. Within a tenant, multiple appliance groups can be added to help organize the appliances and to ensure that the correct configuration is sent to the sets of appliances. These appliance groups can be nested in other appliance groups.

If using the Exinda-hosted service, only a single tenant appears in the system.

See the following for more information:

© 2016 Exinda Networks Inc.

How the Exinda Management Center fits into the appliance feedback loop

Whenever policy configuration is required on the appliances, use EMC to configure the appliances using the following steps:

1. Start monitoring your traffic on the appliances.
2. Configure "Policy Library" on page 81 using EMC such that it is applied to multiple appliances.
3. Create Alerts and Application Performance Scores on the appliances.

> **NOTE:**
> *You can also define your Alerts and Application Performance Scores in the Exinda Management Center.*

4. Wait for the appliances to send monitoring data to EMC.
5. Investigate the notifications by monitoring your traffic on the appliances.
6. Configure and tune the "Optimizer Policy Tree" on page 61 using Exinda Management Center by applying policy changes broadly across appliances as needed.
7. Repeat from (4).

New Concepts

If you are familiar with managing the Exinda Network Orchestrator appliances, be aware that there are new concepts introduced in the Exinda Management Center.

- **Policy Sets:** A set of policies that can be re-used in multiple virtual circuits and various appliance groups.
- **Circuit Type:** A named object that acts as the tie between circuits and appliance bridges. This allows different bridges on different appliances to be bound to the same circuit definition.
- **Library:** Any item that is used and re-used in various policy trees is a Library item.
- **Network Object Location:** The location of a network object (internal or external) is determined by the system comparing the IP addresses in the network object to those in the local network object.
- **Service Level Agreements:** A set of Library objects that allow you monitor the availability of specified IP addresses.
- **VLANs:** A set of Library objects that allow you to separate hosts on their functional attributes rather than their physical location.

© 2016 Exinda Networks Inc.

- **Dynamic Virtual Circuits:** A set of policies that allow you to enforce fair sharing among hosts or to limit the number of hosts on the circuit.

© 2016 Exinda Networks Inc.

Chapter 2: Introduction the Operation of the Exinda Management Center

This chapter provides an overview of the operation of the Exinda Management Center. See the following topics for more information:

Estate Management Best Practices

The information below is provided to ensure that you follow best practices when configuring the Exinda Management Center:

Deployment

Regardless of the Exinda fleet size you are working with, it is very important to test EMC configuration on a single appliance before pushing the configuration to many appliances. Pull one appliance into the subgroup and push the configuration to the group. To ensure all the configuration and customizations are working as you expect, log on to the appliance and check the Optimizer Policy Tree. If there is a problem with the policy, it is far easier to back out a single appliance rather than an entire appliance group. After you confirm the configuration, add the rest of the appliances to the appliance group and then push the configuration to the group again.

Appliance Group Inheritance

- When working with device subgroups, remember to plan for group inheritance. Implement common configuration at the parent group level because all subgroups can inherit settings from the parent group.
- Plan to support a common Optimizer Policy Tree that can also provide distinct network objects or applications per group, as appliance groups cannot inherit applications and network objects from their parent groups.

Circuit Size

When configuring circuits and bridges, remember that you might need multiple circuits with different sizes to monitor various circuit types. For example, if each link has a different Internet speed, you will have to create a different circuit for each link. Use the Library to create the different circuits for the different links, which are then re-usable when duplicating policy trees with only minor changes in link speeds.

What to Configure in the EMC vs. the Appliance

The following chart outlines which configuration items to manage ONLY in the EMC, and which options you can update on individual appliances. Note that if you make changes to VLANs or protocols at the group level, you should send CLI commands from within EMC only.

Configuration Item	Configure on EMC	Configure on Appliance
Optimizer	✓	✗
Network Objects	✓	✗
Users and Groups	✗	✓
VLANs	✓	✗
Protocols	✗	✓
Applications	✓	✗
Application Groups	✓	✗
Schedules	✓	✗
Adaptive Response	✗	✓
Service Levels	✓	✗
HTML Response	✗	✓

Recommended Approach to Integrate Appliances into EMC

1. Import Configuration

Although not compulsory, it is highly recommended that you import the available appliance configuration into the tenant library to reduce redundancy and avoid re-programming the same configuration in the EMC. The configuration import is not required if the appliance is new and does not contain any configuration.

Follow these steps to import configuration into a tenant:

1. Setup an appliance to call into EMC.
2. To migrate an appliance into a tenant, do one of the following:
   - For on-premises installations:
     a. If only one tenant exists, there is no need to manually bring an appliance into the tenant because the connected appliance automatically appears on the tenant **Not Deployed** page.
     b. If multiple tenants exist, the appliance appears on the **Appliance Pool** page from where you can move it to the desired tenant.
   - For cloud-based instances, the appliance automatically appears on the tenant **Not Deployed** page.
3. Import the configuration from appliance:

> **NOTE**
>
> *Importing configuration is optional, but if an appliance has already been in use, its configuration can be applied globally across all other appliances without having to apply the configuration to the appliances individually.*

   a. Select an appliance and click **Import Configuration**.
   This starts the "Import Configuration" wizard.

> **NOTE**
>
> *When importing the configuration from an appliance, you work your way through a wizard that allows you to select the configuration items you need to import. There are eight classes of configuration that you can import, with each offering the configuration items that already exist on the appliance.*
>
> - *Network Objects*
> - *Applications*
> - *Schedules*
> - *VLANs*
> - *Circuits*
> - *Virtual Circuits*
> - *Policies*
> - *Service Level Agreements*
>
> *For each of these classes, you can select from the configuration items that exist, or you can skip to the next class. The process of importing each of the configuration classes is the same.*

b. In the wizard. click the **Import <configuration class>** button.
For the configuration class, if there are existing configuration items, they appear in a grid.

c. If configuration items do not exist in the tenant library, select their check-boxes and click **Add Selected <configuration items> to the Library**.

> **NOTE**
>
> *If configuration items already exist in the tenant library, a green check mark appears before the configuration item name. You cannot use the same configuration item again.*

4. Click **Next** to move on to the next configuration class.
5. Repeat steps 3 and 4 for each configuration class.
6. At the end of the wizard, click **Close**.

2. Configure Optimizer Policy Tree

The Optimizer Policy Tree is applied based on a hierarchical structure of device groups, where child groups can inherit policy from parent groups. It is therefore important to start by defining the group names you will need. See Creating Policies for Appliance Groups on page 59 for more information

As a best practice, use the Library to add circuits, virtual circuits, policy sets and policies <Add link to Define Library Objects>. These settings are all re-useable and will be available as a selection when defining the optimizer policy for each appliance group. For each group, you can then create an optimizer policy tree to combine circuits, virtual circuits, policy sets and policy rules. See Optimizer Policy Tree on page 61 for more information.

Follow these steps to setup the Optimizer Policy Tree:

1. Navigate to **Configured Appliances > Optimizer Policy Tree**.

> **NOTE**
>
> *You will not see the option to Add Circuit from Library if no circuits exist in the Library. The circuit is automatically added to the common Library if it does not exist. See "Circuits" on page 75 for more information.*

2. To define the Circuit:
   a. You can either create a new circuit (click Create new circuit) or add a custom defined circuit from the Library.
   b. When creating a new circuit, you are required to define a circuit type. You can either use the circuit types from library or define a new one. See "Circuit Types" on page 74 for more information.
3. To define Virtual Circuit, you can either create a new virtual circuit (click Create new virtual circuit) or add a custom defined virtual circuit from the library.

> **NOTE**
>
> *You will not see the option to Add virtual circuit from Library if no virtual circuits exist in the library. The virtual circuit is automatically added into common Library if it does not exist. See "Virtual Circuits" on page 76 for more information.*

4. To define Policies, you can either create a Policy Set (click Create new policy set) or add a custom defined policy sets (click Add Policy Set from Library). See "Policy Sets" on page 80 for more information.

3. Migrating Appliance into Group

At this stage, you can move the individual appliances from the **Not Deployed** list to the appropriate Appliance Group within the Tenant. See "Application Groups" on page 88 for more information.

4. Tying Bridge to Circuit Type

When the appliance is moved into the desired appliance group, a warning icon appears after **Bridge/Circuit Type Mapping** (see "Circuit Types" on page 74 for more information). This means that the recently moved appliance bridge is not mapped to any circuit type.

To tie a bridge to a circuit type, navigate to **Bridge/Circuit Type Mapping** page. Select the appliance and either select an existing circuit type from drop-down menu or create a new circuit type.

5. Send Configuration

Click the download icon on right of appliance group name to push configuration for the group.

The first user-initiated push of the configuration to the appliance(s) deletes the following configuration on the appliance:

- The definitions for local and private net network objects.
- The Circuits in the Optimizer (and hence the entire optimizer tree).
- The **After Work** and **Work Hours** schedules.

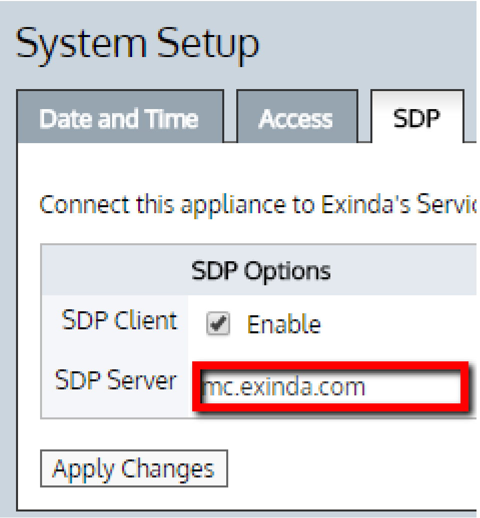
> **NOTE**
>
> *The configuration is sent only to the appliances belonging to that appliance group, not to all the groups within a tenant.*

How to Get Your Appliance Configured Quickly

1. Appliance Settings

Make sure all your appliances are configured to call EMC.

1. On each appliance, navigate to the **Configuration > System Setup > SDP** page.
2. Enable the SDP Client option and program `mc.exinda.com` as the SDP Server.



Connect this appliance to Exinda's Servi

SDP Options

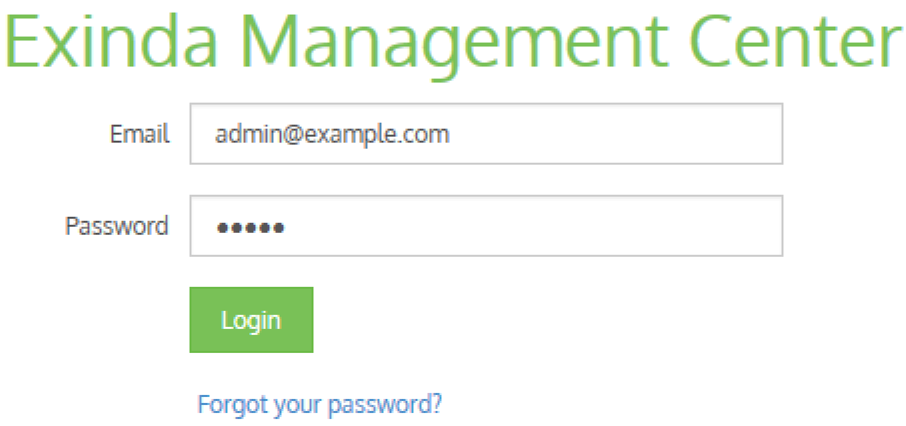
SDP Client ☑ Enable

SDP Server mc.exinda.com

2. Logging into the Cloud-based EMC

> **NOTE**
>
> *If you are using an on-premises instance of the EMC, you can skip this step.*

1. Navigate to mc.exinda.com and insert your credentials.

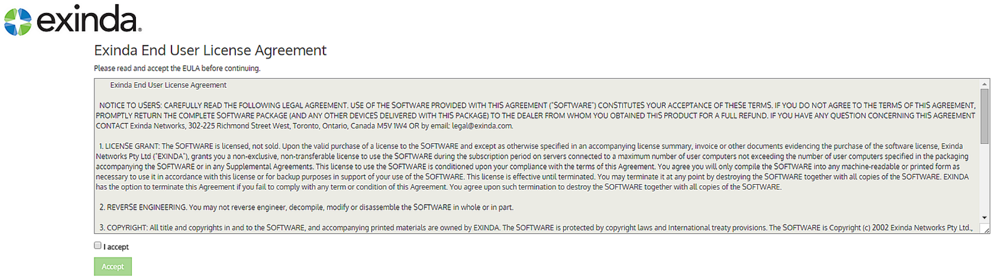


Exinda Management Center

Email: admin@example.com

Password: ●●●●●

2. Read and accept the license agreement.



exinda

Exinda End User License Agreement

Please read and accept the EULA before continuing.

Exinda End User License Agreement

NOTICE TO USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT. USE OF THE SOFTWARE PROVIDED WITH THIS AGREEMENT ("SOFTWARE") CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE COMPLETE SOFTWARE PACKAGE (AND ANY OTHER DEVICES DELIVERED WITH THIS PACKAGE) TO THE DEALER FROM WHOM YOU OBTAINED THIS PRODUCT FOR A FULL REFUND. IF YOU HAVE ANY QUESTION CONCERNING THIS AGREEMENT CONTACT Exinda Networks, 302-225 Richmond Street West, Toronto, Ontario, Canada M5V 1W4 OR by email: legal@exinda.com.

1. LICENSE GRANT: The SOFTWARE is licensed, not sold. Upon the valid purchase of a license to the SOFTWARE and except as otherwise specified in an accompanying license summary, invoice or other documents evidencing the purchase of the software license, Exinda Networks Pty Ltd ("EXINDA"), grants you a non-exclusive, non-transferable license to use the SOFTWARE during the subscription period on servers connected to a maximum number of user computers not exceeding the number of user computers specified in the packaging accompanying the SOFTWARE or in any Supplemental Agreements. This license to use the SOFTWARE is conditioned upon your compliance with the terms of this Agreement. You agree you will only compile the SOFTWARE into any machine-readable or printed form as necessary to use it in accordance with this license or for backup purposes in support of your use of the SOFTWARE. This license is effective until terminated. You may terminate it at any point by destroying the SOFTWARE together with all copies of the SOFTWARE. EXINDA has the option to terminate this Agreement if you fail to comply with any term or condition of this Agreement. You agree upon such termination to destroy the SOFTWARE together with all copies of the SOFTWARE.

2. REVERSE ENGINEERING. You may not reverse engineer, decompile, modify or disassemble the SOFTWARE in whole or in part.

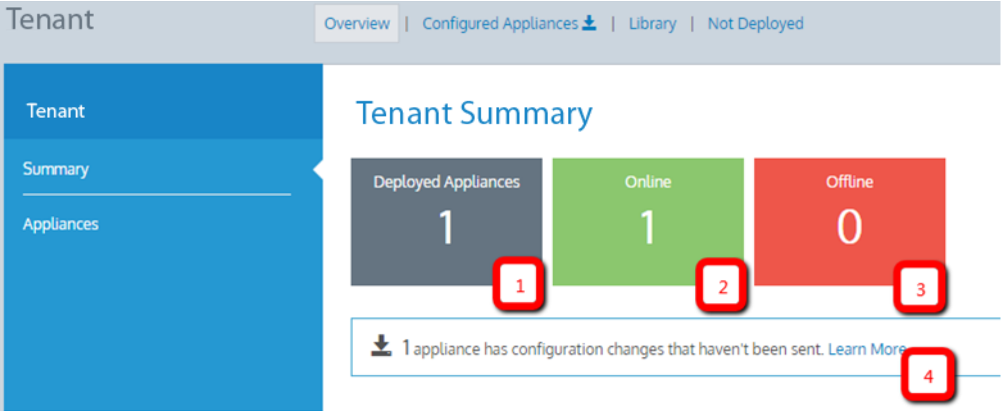
3. COPYRIGHT: All title and copyrights in and to the SOFTWARE, and accompanying printed materials are owned by EXINDA. The SOFTWARE is protected by copyright laws and International treaty provisions. The SOFTWARE is Copyright (c) 2002 Exinda Networks Pty Ltd.,

☐ I accept

3. Tenant Summary Page Overview

This page provides a high-level snapshot of your tenant status. It shows how many appliances have been deployed, are online, and are offline. This page also displays a warning if configuration has not been pushed to the appliance(s) under Configured Appliances.

Summary Page



Tenant Summary

Deployed Appliances 1

Online 1

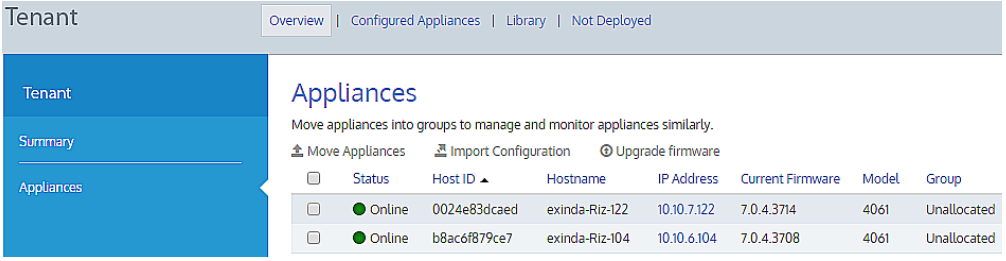
Offline 0

1 appliance has configuration changes that haven't been sent. Learn More

1. **Deployed Appliances:** This box displays the total number of appliances in the Configured Appliances group.
2. **Online:** This box displays the total number of appliances successfully enrolled into the EMC. The number of online appliances does not indicate the number of appliances appearing in the Configured Appliances group, these must be manually shifted into an appliance group. Please read further for more information.
3. **Offline:** This box displays the total number of appliances that are successfully enrolled into EMC, but are offline.
4. If appliances need configuration updates, at warning appears below the summary.

Appliances Page

This page lists all the appliances within your tenant; their status, group affiliation, and other details:



Appliances

Move appliances into groups to manage and monitor appliances similarly.

□	Status	Host ID ▲	Hostname	IP Address	Current Firmware	Model	Group
□	● Online	0024e83dcaed	exinda-Riz-122	10.10.7.122	7.0.4.3714	4061	Unallocated
□	● Online	b8ac6f879ce7	exinda-Riz-104	10.10.6.104	7.0.4.3708	4061	Unallocated

4. Create an Appliance Group (Optional)

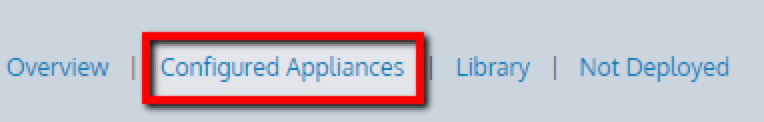
An appliance group is the concept of bundling appliances with same configuration into one single group. The benefits of creating appliance groups are:

© 2016 Exinda Networks Inc.

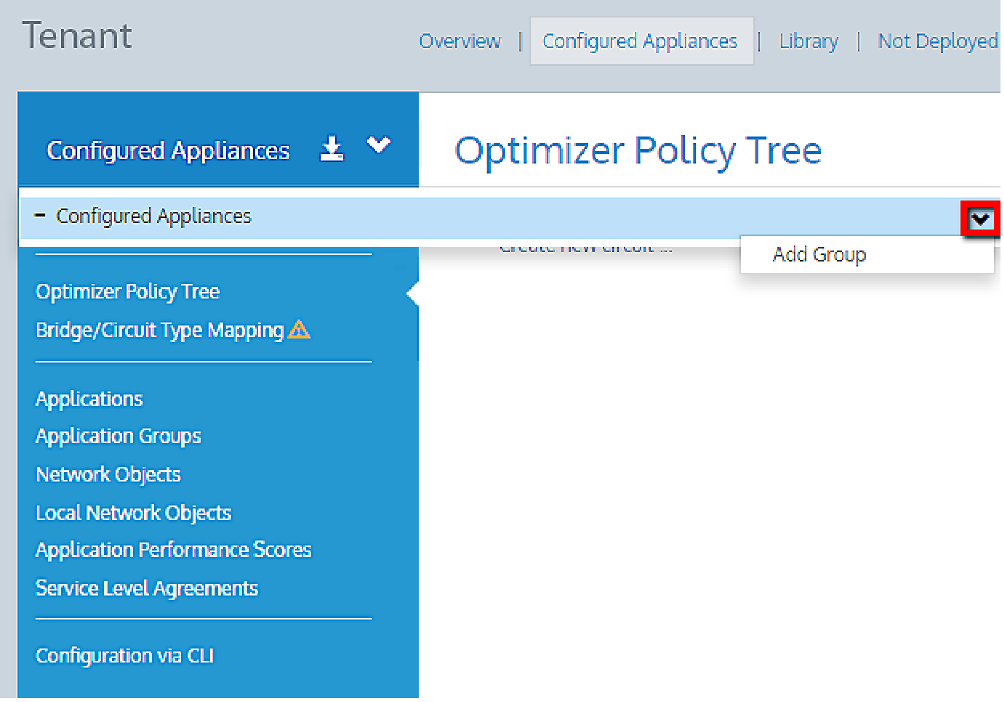
- Organizing your appliances by region
- If your network topology requires a set of Exinda appliances to have a particular set of policies, and other sets of appliances require a different set of policies, then it is best to group the appliances by their similarity.

> **NOTE**
>
> ***You do not need to create an appliance group if all your appliances within your network require same configuration.***

1. Navigate to Configured Appliances page.

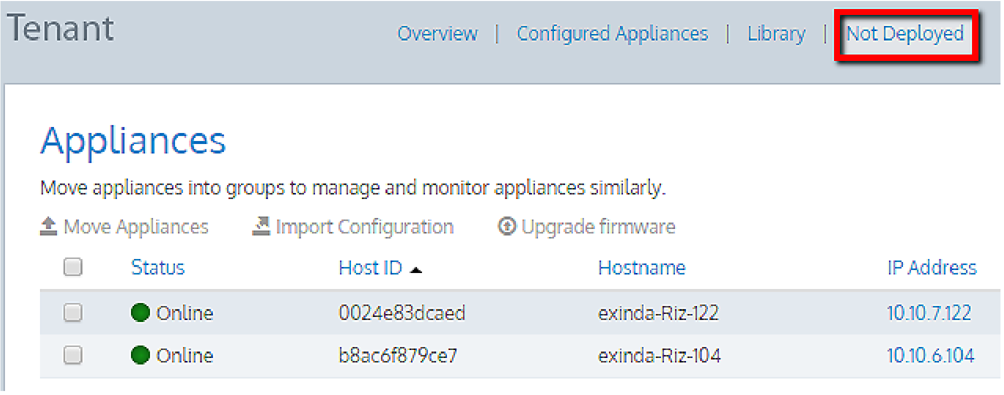


2. Click the drop down icon to view and navigate to appliance groups.
3. To add an appliance group, click the second drop down icon and click Add Group.



5. Migrate an Appliance into a Group

After configuring your appliance with the EMC information, it takes roughly 20 minutes for an appliance to successfully appear in the EMC. The appliance is then listed on the '**Not Deployed**' page.



Tenant

Overview | Configured Appliances | Library | Not Deployed

Appliances

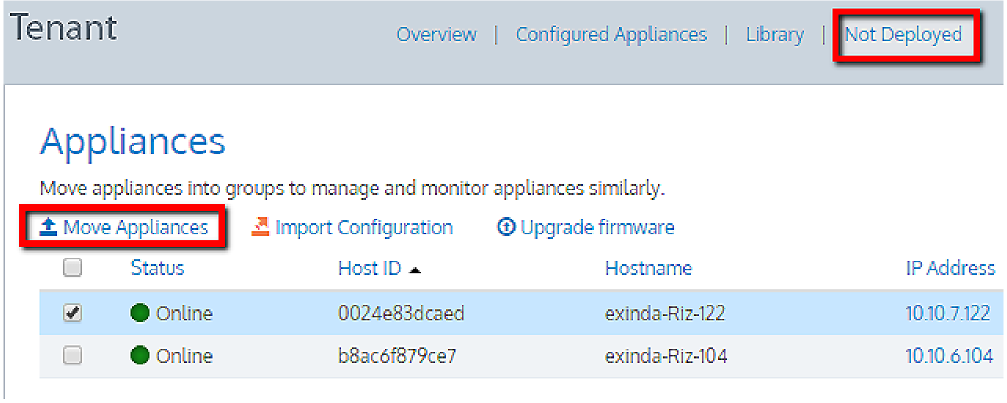
Move appliances into groups to manage and monitor appliances similarly.

Move Appliances Import Configuration Upgrade firmware

□	Status	Host ID ▲	Hostname	IP Address
□	● Online	0024e83dcaed	exinda-Riz-122	10.10.7.122
□	● Online	b8ac6f879ce7	exinda-Riz-104	10.10.6.104

Appliances on the **Not Deployed** page do not belong to any appliance group and so any configuration push has no affect on these appliances.

1. On the **Not Deployed** page, select an appliance and click **Move Appliances**



Tenant

Overview | Configured Appliances | Library | Not Deployed

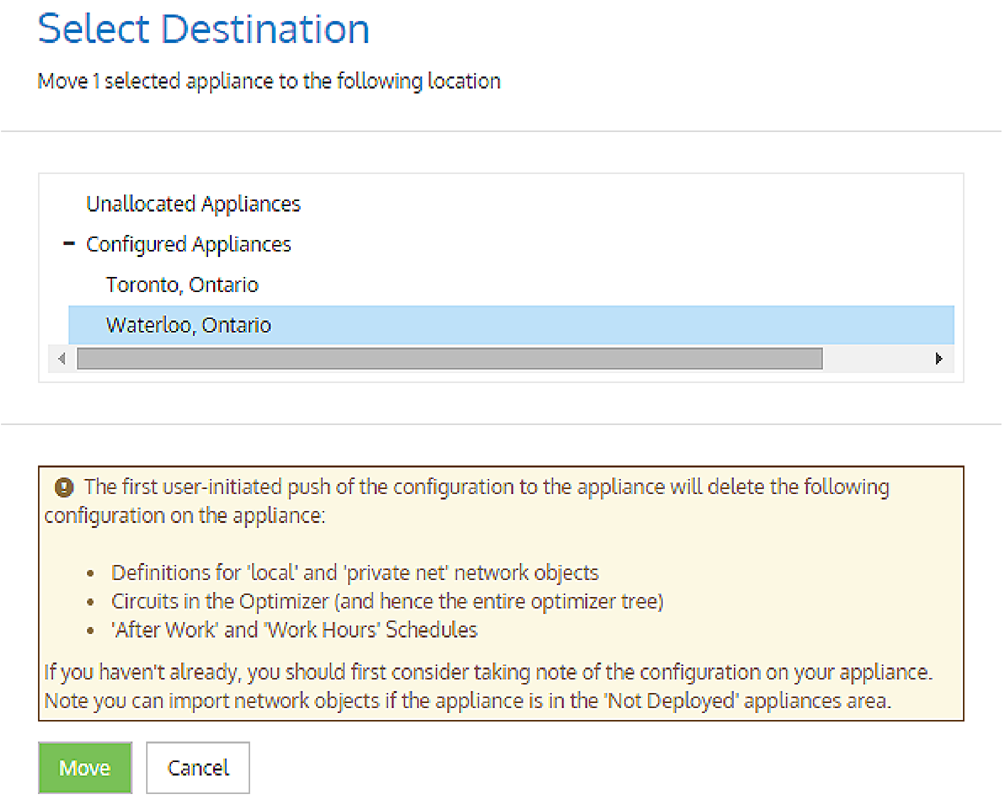
Appliances

Move appliances into groups to manage and monitor appliances similarly.

Move Appliances Import Configuration Upgrade firmware

□	Status	Host ID ▲	Hostname	IP Address
☑	● Online	0024e83dcaed	exinda-Riz-122	10.10.7.122
□	● Online	b8ac6f879ce7	exinda-Riz-104	10.10.6.104

2. Select a desired appliance group for the appliance and click ‘**Move**’.



Select Destination

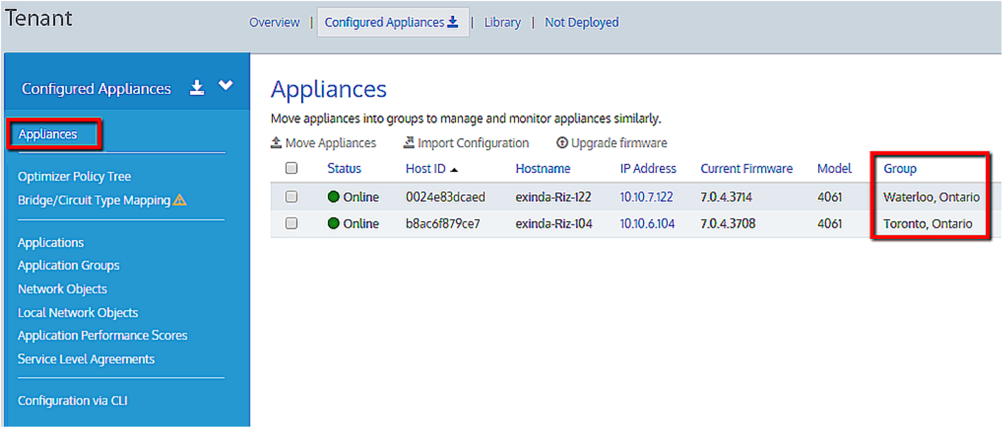
Move 1 selected appliance to the following location

The first user-initiated push of the configuration to the appliance will delete the following configuration on the appliance:

- Definitions for 'local' and 'private net' network objects
- Circuits in the Optimizer (and hence the entire optimizer tree)
- 'After Work' and 'Work Hours' Schedules

If you haven't already, you should first consider taking note of the configuration on your appliance. Note you can import network objects if the appliance is in the 'Not Deployed' appliances area.

3. The moved appliance will now show up under **Configured Appliances** and listed under the appliance group to which it belongs.



Appliances

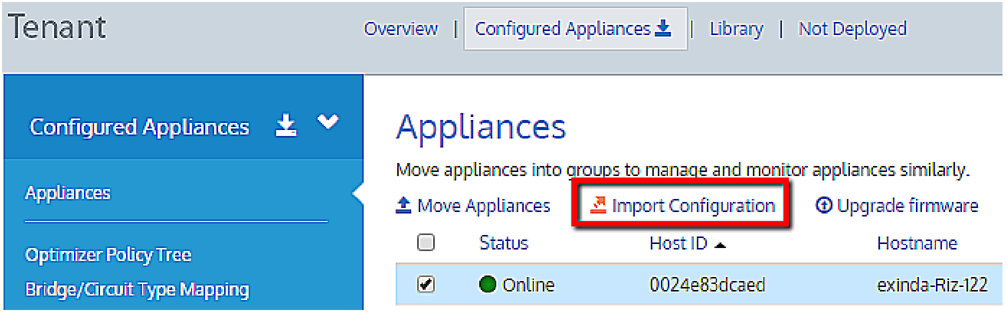
Move appliances into groups to manage and monitor appliances similarly.

□	Status	Host ID ▲	Hostname	IP Address	Current Firmware	Model	Group
□	● Online	0024e83dcaed	exinda-Riz-122	10.10.7.122	7.0.4.3714	4061	Waterloo, Ontario
□	● Online	b8ac6f879ce7	exinda-Riz-104	10.10.6.104	7.0.4.3708	4061	Toronto, Ontario

6. Import Configuration (Optional)

If you would like to retain your appliance network objects and policies, you have the option to transfer them into a common library for future use and/or integrate them into the global configuration for your group.

1. On the **Configured Appliances** page, navigate to **Appliances**.
2. Select an appliance and click Import Configuration.



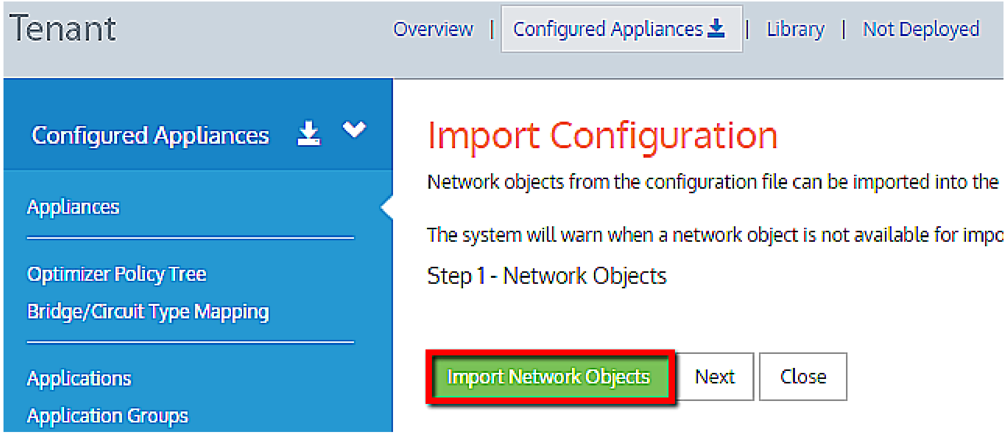
Appliances

Move appliances into groups to manage and monitor appliances similarly.

□	Status	Host ID ▲	Hostname
☑	● Online	0024e83dcaed	exinda-Riz-122

Step 1 – Import Network Objects

1. If you would like to import your network objects, click **Import Network Objects**, otherwise click **Next** to skip this step.



Import Configuration

Network objects from the configuration file can be imported into the

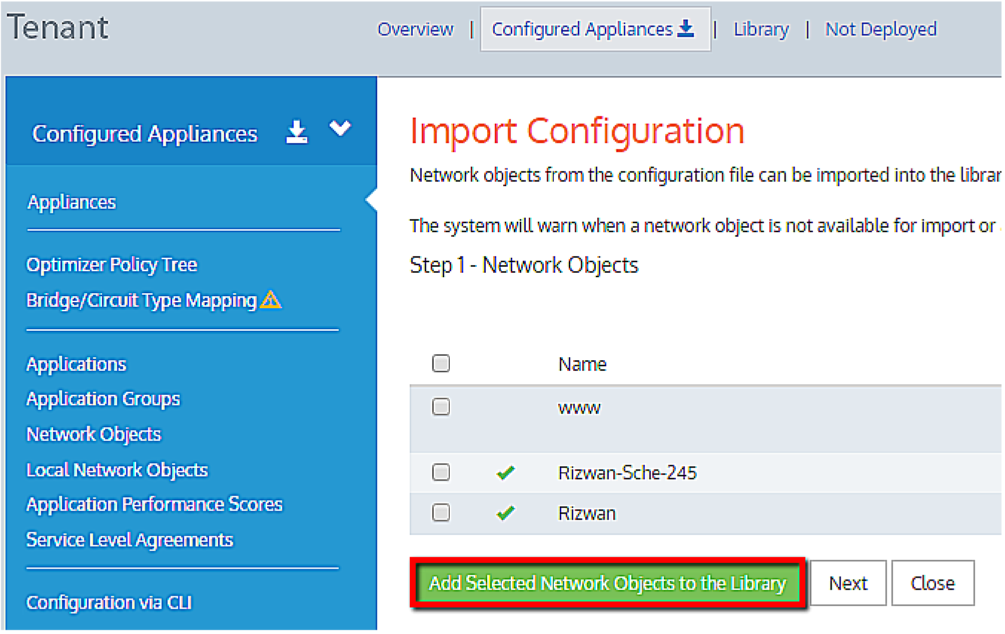
The system will warn when a network object is not available for impo

Step 1 - Network Objects

The network objects that exist on the appliance appear in the grid

> **NOTE**
>
> ***If any network objects already exist in the library, a green checkmark appears in front of it. Once used, you will not be able reuse it.***

2. Click **Add Selected Network Objects to the Library**.



Import Configuration

Network objects from the configuration file can be imported into the librar

The system will warn when a network object is not available for import or

Step 1 - Network Objects

□		Name
□		www
□	✓	Rizwan-Sche-245
□	✓	Rizwan

Step 2 – Import Applications

1. If you need to import any applications that exist in the configuration of the appliance, click **Import Applications**, or skip this step by clicking **Next**.
   The application appear in the grid.
2. Select the checkboxes next to each of the applications you need to import.
3. Click **Add Selected Application to Library**.
4. Click **Next**.

Step 3 – Import Schedules

1. If you need to import any schedules that exist in the configuration of the appliance, click **Import Schedules**, or skip this step by clicking **Next**.
   The schedules appear in the grid.
2. Select the checkboxes next to each of the schedules you need to import.
3. Click **Add Selected Schedules to Library**.
4. Click **Next**.

Step 4 – Import VLANs

1. If you need to import any VLANs that exist in the configuration of the appliance, click **Import VLANs**, or skip this step by clicking **Next**.
   The VLANs appear in the grid.
2. Select the checkboxes next to each of the VLANs you need to import.

© 2016 Exinda Networks Inc.

3. Click **Add Selected VLANs to Library**.
4. Click **Next**.

Step 5 – Import Circuits

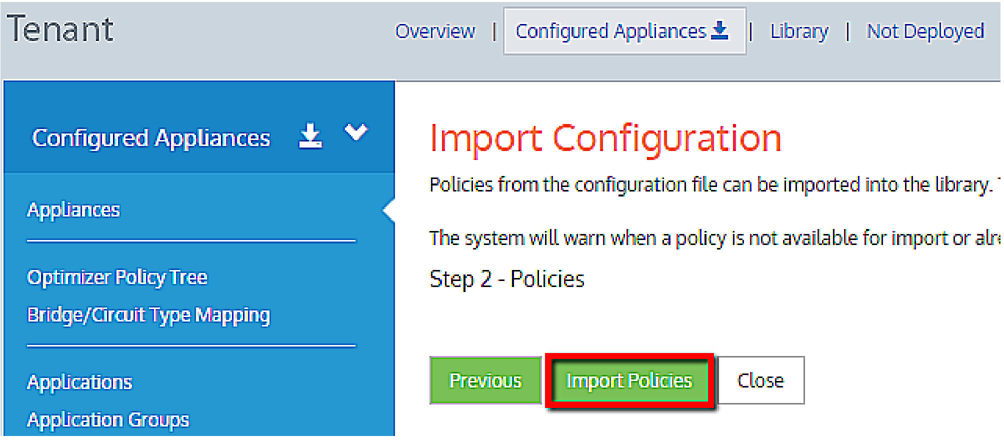
1. If you need to import any circuits that exist in the configuration of the appliance, click **Import Circuits**, or skip this step by clicking **Next**.
   The circuits appear in the grid.
2. Select the checkboxes next to each of the circuits you need to import.
3. Click **Add Selected Circuits to Library**.
4. Click **Next**.

Step 6 – Import Virtual Circuits

1. If you need to import any virtual circuits that exist in the configuration of the appliance, click **Import Virtual Circuits**, or skip this step by clicking **Next**.
   The virtual circuits appear in the grid.
2. Select the checkboxes next to each of the virtual circuits you need to import.
3. Click **Add Selected Virtual Circuits to Library**.
4. Click **Next**.

Step 7 – Import Policies

1. If you need to import any policies that exist in the configuration of the appliance, click **Import Policies**, or skip this step by clicking **Next**.
   The policies appear in the grid.



Import Configuration

Policies from the configuration file can be imported into the library.

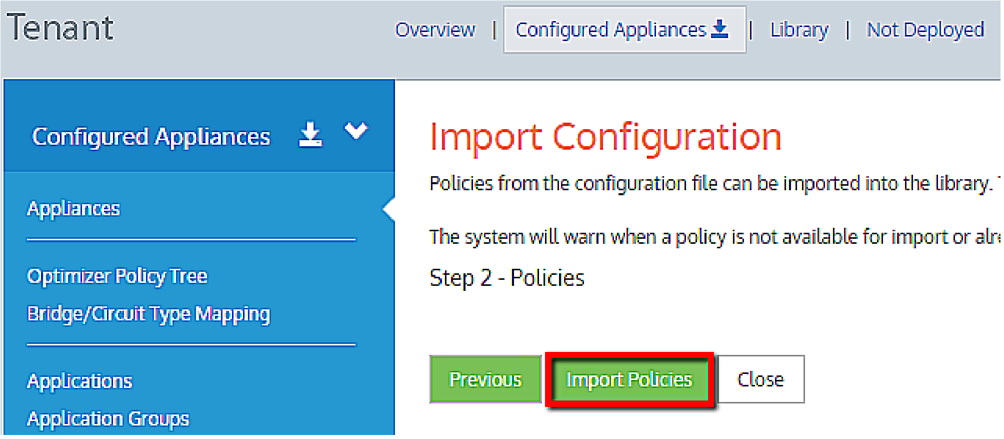
The system will warn when a policy is not available for import or alr

Step 2 - Policies

NOTE

You will not be able to import policies that already exist in library and policies tied to a network object that is not available in the library. Hover over the error icon to see the specific error message.

2. Select the checkboxes next to each of the virtual circuits you need to import.
3. Click **Add Selected Polices to Library**.
4. Click **Next**.
5. Click **Import Policies** to import the current policies from the appliance.



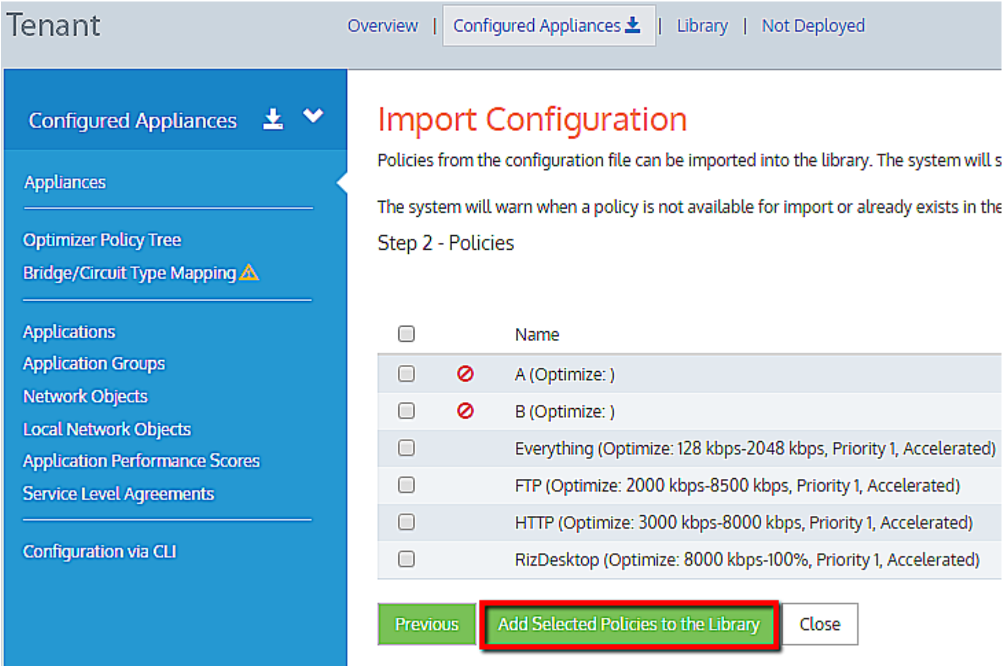
Import Configuration

Policies from the configuration file can be imported into the library. '

The system will warn when a policy is not available for import or alr

Step 2 - Policies

6. You will not be able to import policies that already exist in library and policies tied to a network object that is not available in the library. Hover over the error icon to see the specific error message. Make sure to click **Add Selected Policies to the Library** to successfully add selected policies into the library:



Import Configuration

Policies from the configuration file can be imported into the library. The system will s

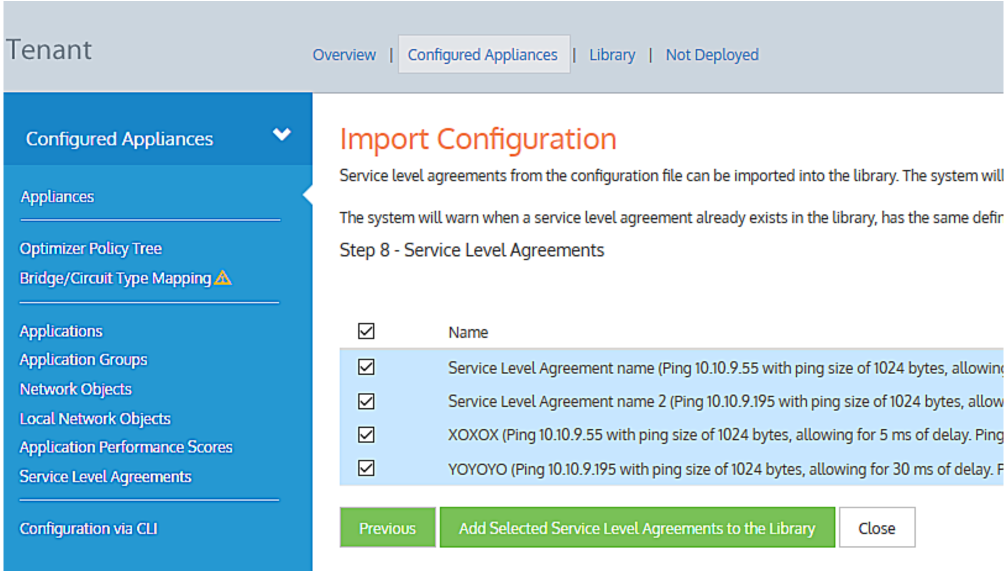
The system will warn when a policy is not available for import or already exists in the

Step 2 - Policies

☐		Name
☐	⊘	A (Optimize:)
☐	⊘	B (Optimize:)
☐		Everything (Optimize: 128 kbps-2048 kbps, Priority 1, Accelerated)
☐		FTP (Optimize: 2000 kbps-8500 kbps, Priority 1, Accelerated)
☐		HTTP (Optimize: 3000 kbps-8000 kbps, Priority 1, Accelerated)
☐		RizDesktop (Optimize: 8000 kbps-100%, Priority 1, Accelerated)

Step 8 – Import Service Level Agreements

1. If you need to import any service level agreements that exist in the configuration of the appliance, click **Import Serice Level Agreements**, or skip this step by clicking **Close**.
   The virtual circuits appear in the grid.
2. Select the checkboxes next to each of the virtual circuits you need to import.



Import Configuration

Service level agreements from the configuration file can be imported into the library. The system will

The system will warn when a service level agreement already exists in the library, has the same defir

Step 8 - Service Level Agreements

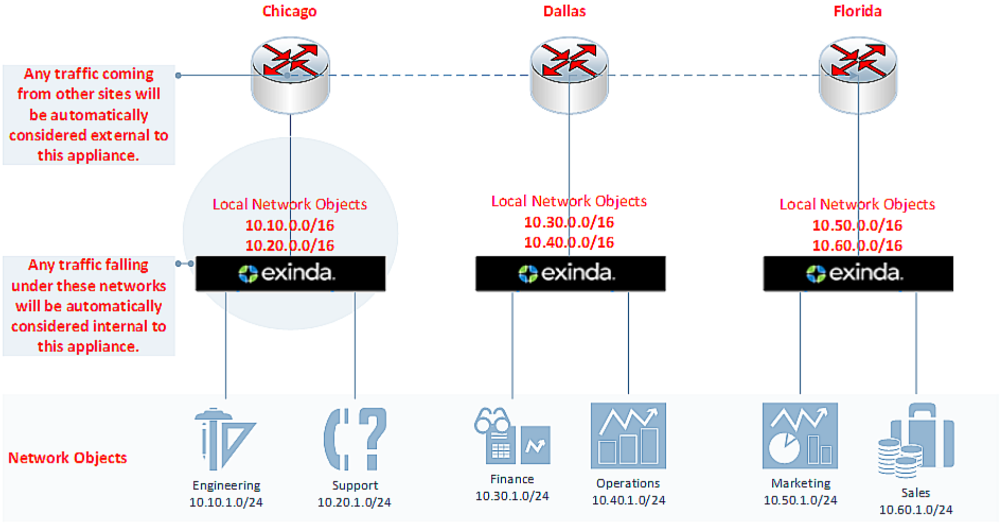
☑	Name
☑	Service Level Agreement name (Ping 10.10.9.55 with ping size of 1024 bytes, allowin
☑	Service Level Agreement name 2 (Ping 10.10.9.195 with ping size of 1024 bytes, allow
☑	XOXOX (Ping 10.10.9.55 with ping size of 1024 bytes, allowing for 5 ms of delay. Ping
☑	YOYOYO (Ping 10.10.9.195 with ping size of 1024 bytes, allowing for 30 ms of delay. F

3. Click **Add Selected Service Level Agreements to Library**.

4. Click **Close**.

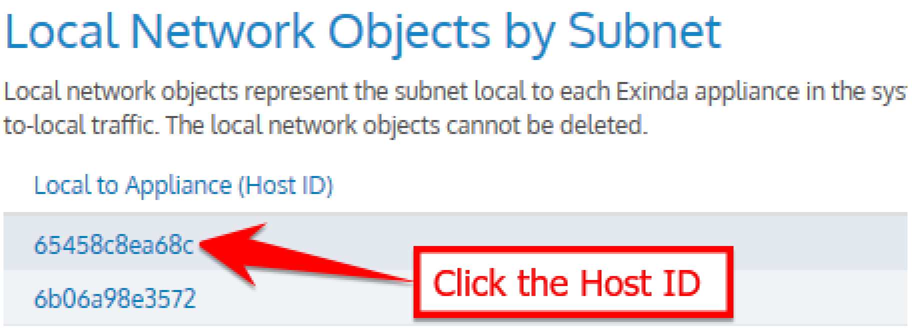
7. Configure Local Network Objects

The local network object is the subnet that resides behind (or is local to) the appliance on the network. Local network objects take their definition from an IP network address and mask length to identify the range of IP addresses that exist in the LAN behind the appliance. You define a local network object for each appliance, so that each appliance can differentiate between traffic that is external and internal to the LAN on which it operates. In the EMC configuration, local network objects are appliance specific, so appliances cannot share these objects.



To configure the local network object, do the following:

1. Click **Configured Appliances > Local Network Objects**.
   The page on the right refreshes to display the configured appliances.
2. For each appliance where you need to configure the local network object, click the entry under the **Local to Appliance (Host ID)** column heading.
   The page refreshes to display the Local Network Objects by Subnet configuration.



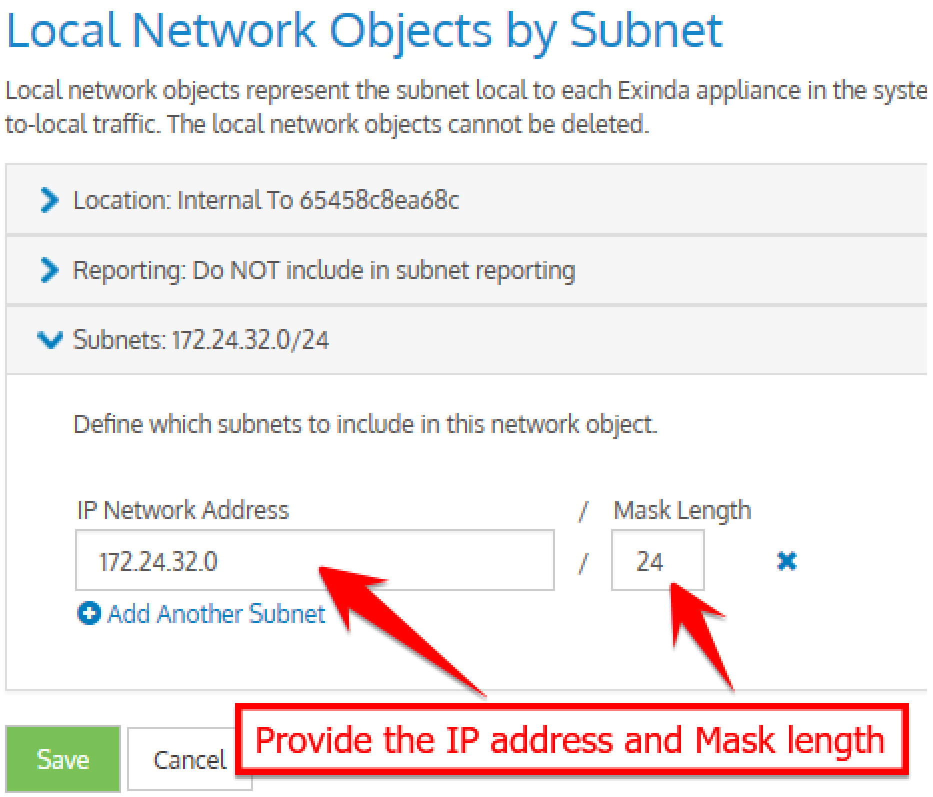
Local Network Objects by Subnet

Local network objects represent the subnet local to each Exinda appliance in the sys to-local traffic. The local network objects cannot be deleted.

Local to Appliance (Host ID)
65458c8ea68c
6b06a98e3572

Click the Host ID

3. In the **IP Network Address** and **Mask Length** fields type the needed information.



Local Network Objects by Subnet

Local network objects represent the subnet local to each Exinda appliance in the syste to-local traffic. The local network objects cannot be deleted.

Location: Internal To 65458c8ea68c

Reporting: Do NOT include in subnet reporting

Subnets: 172.24.32.0/24

Define which subnets to include in this network object.

IP Network Address / Mask Length

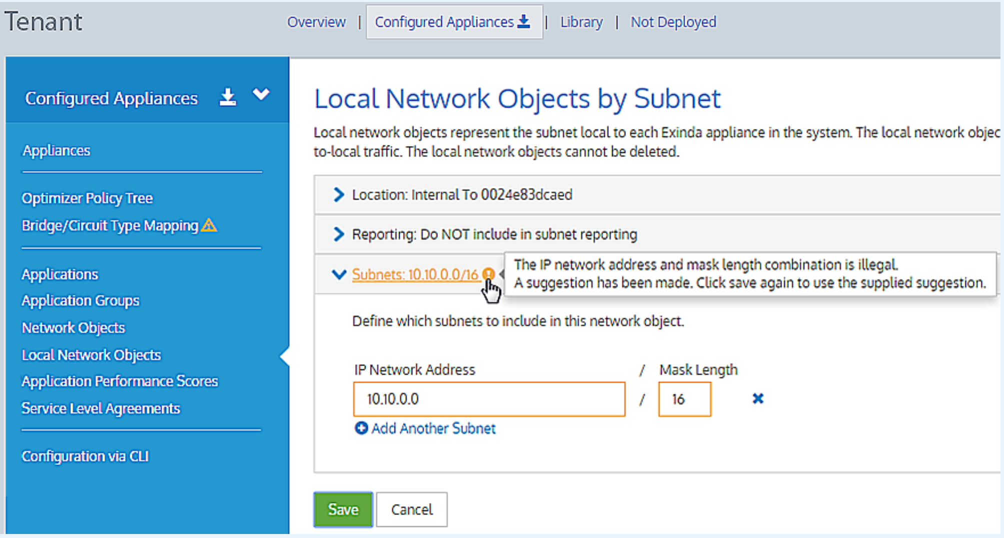
172.24.32.0 / 24

Provide the IP address and Mask length

4. Click **Save**.

NOTE

If the IP address and mask length you define are illegal, the EMC returns a warning and provides a suggestion for correcting the issue. Click Save.



Local Network Objects by Subnet

Local network objects represent the subnet local to each Exinda appliance in the system. The local network objec to-local traffic. The local network objects cannot be deleted.

Location: Internal To 0024e83dcaed

Reporting: Do NOT include in subnet reporting

Subnets: 10.10.0.0/16

The IP network address and mask length combination is illegal. A suggestion has been made. Click save again to use the supplied suggestion.

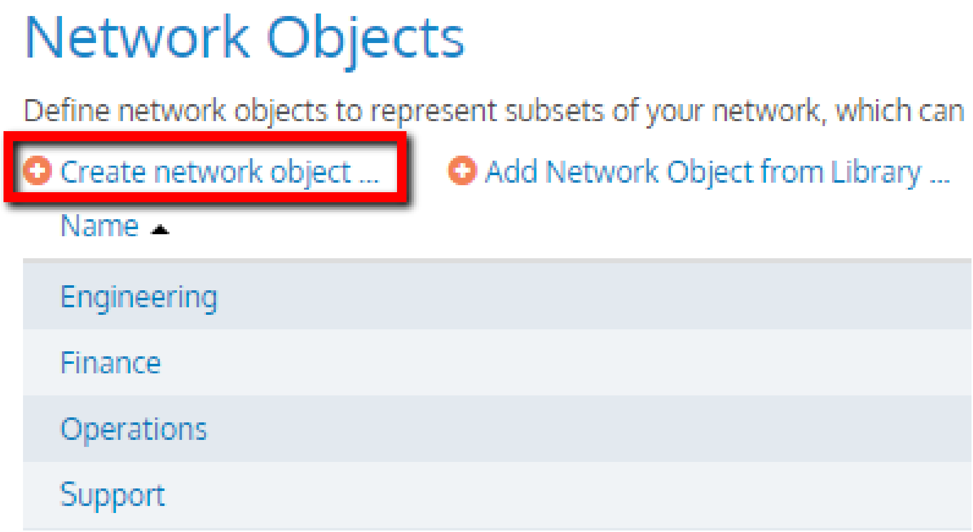
Define which subnets to include in this network object.

IP Network Address: 10.10.0.0 / Mask Length: 16

8. Configure Network Objects

A network object represents the hosts on a network. They can be subnets, single hosts, groups of one or other, or groups of both. A network object can either be created in the Library or on the Network Objects page under Configured Appliances. When adding a network object to an appliance group, you can create what you need first, or use an existing network object from the library. To create and apply a network object, do the following:

1. Do *one* of the following:
   a. Under the **Library**, click **Network Objects**.
   b. Under **Configured Appliances**, click **Network Objects**.
2. Click **Create network object...**.
   Network objects created under Configured Appliances are also saved in the Library.

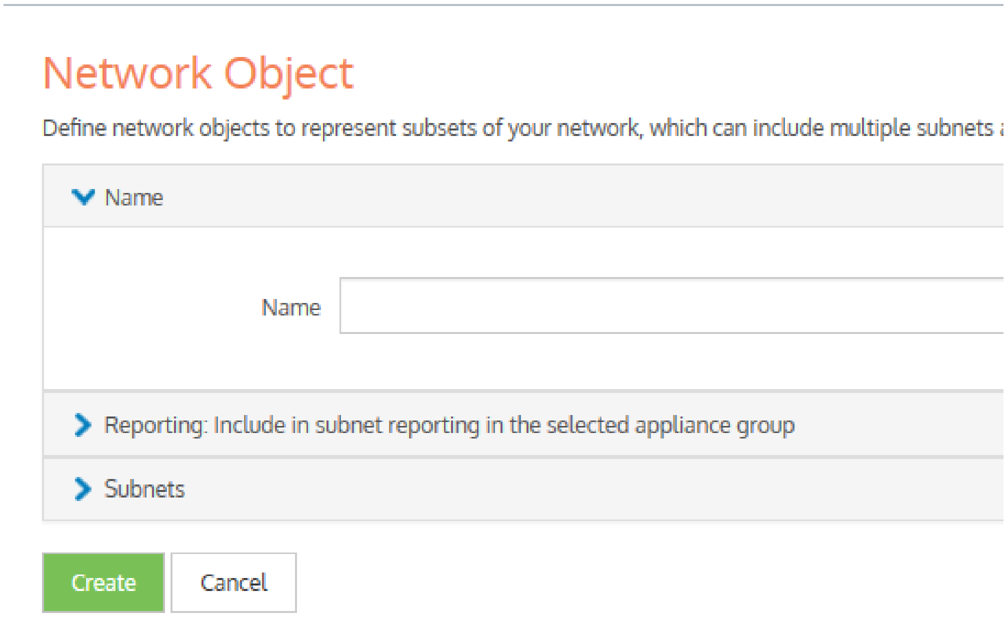


Network Objects

Define network objects to represent subsets of your network, which can

Create network object ...
Add Network Object from Library ...
Name
Engineering
Finance
Operations
Support

3. Open the **Name** section and type a meaningful name for the object.

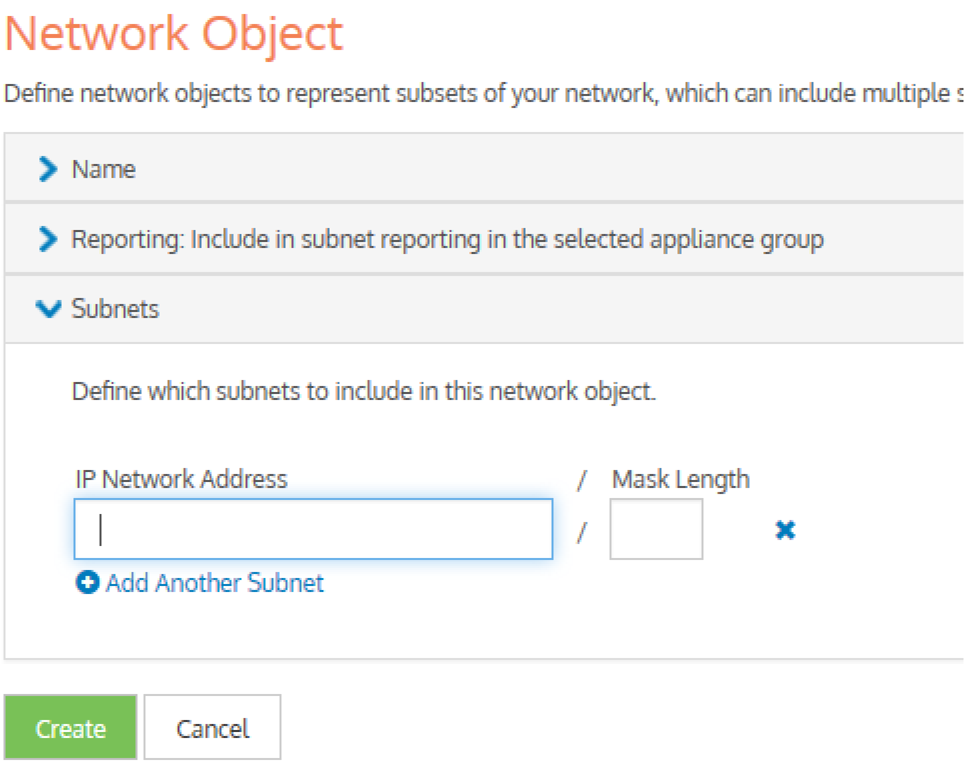


Network Object

Define network objects to represent subsets of your network, which can include multiple subnets a

Name
Name
Reporting: Include in subnet reporting in the selected appliance group
Subnets
Create
Cancel

4. Open the **Subnets** section and provide the **IP Network Address** and **Mask Length** in the appropriate fields.



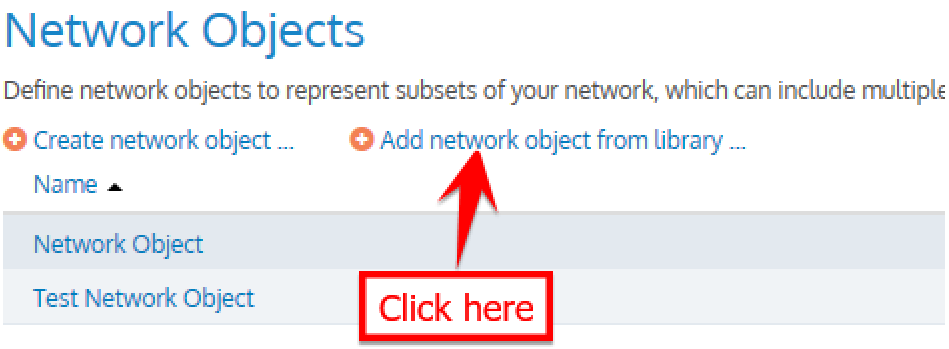
Network Object

Define network objects to represent subsets of your network, which can include multiple s

Name
Reporting: Include in subnet reporting in the selected appliance group
Subnets

Define which subnets to include in this network object.

5. Click **Create**.
   Once created, you add the network object to the appliance group from the Library.
6. Open the Network Objects page under Configured Appliances.
7. Click **Add network object from Library…**



Network Objects

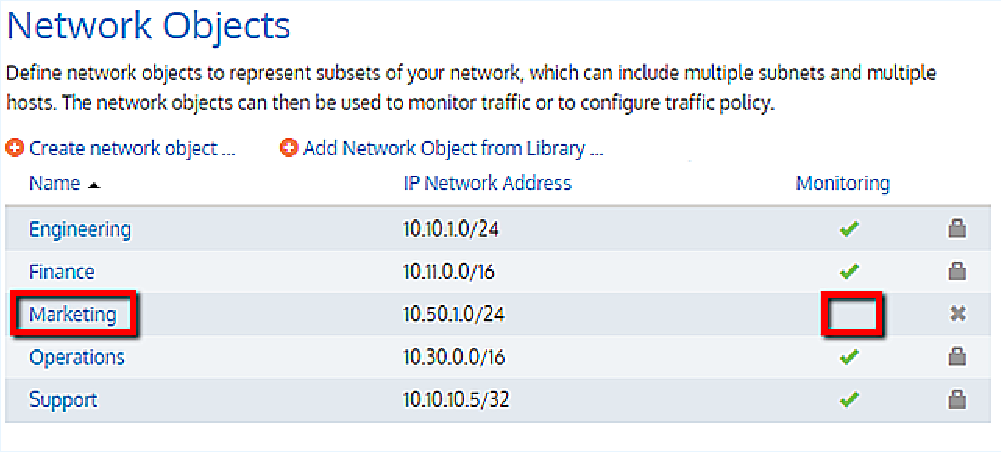
Define network objects to represent subsets of your network, which can include multiple

Create network object ...
Add network object from library ...
Name ▲
Network Object
Test Network Object
Click here

The Add network object from Library dialog box opens.

NOTE

You have to manually enable monitoring of the network object if it is required for subnet reporting. If the entry for the network object does not have a check mark under the Monitoring column, subnet reporting is not available.



Network Objects

Define network objects to represent subsets of your network, which can include multiple subnets and multiple hosts. The network objects can then be used to monitor traffic or to configure traffic policy.

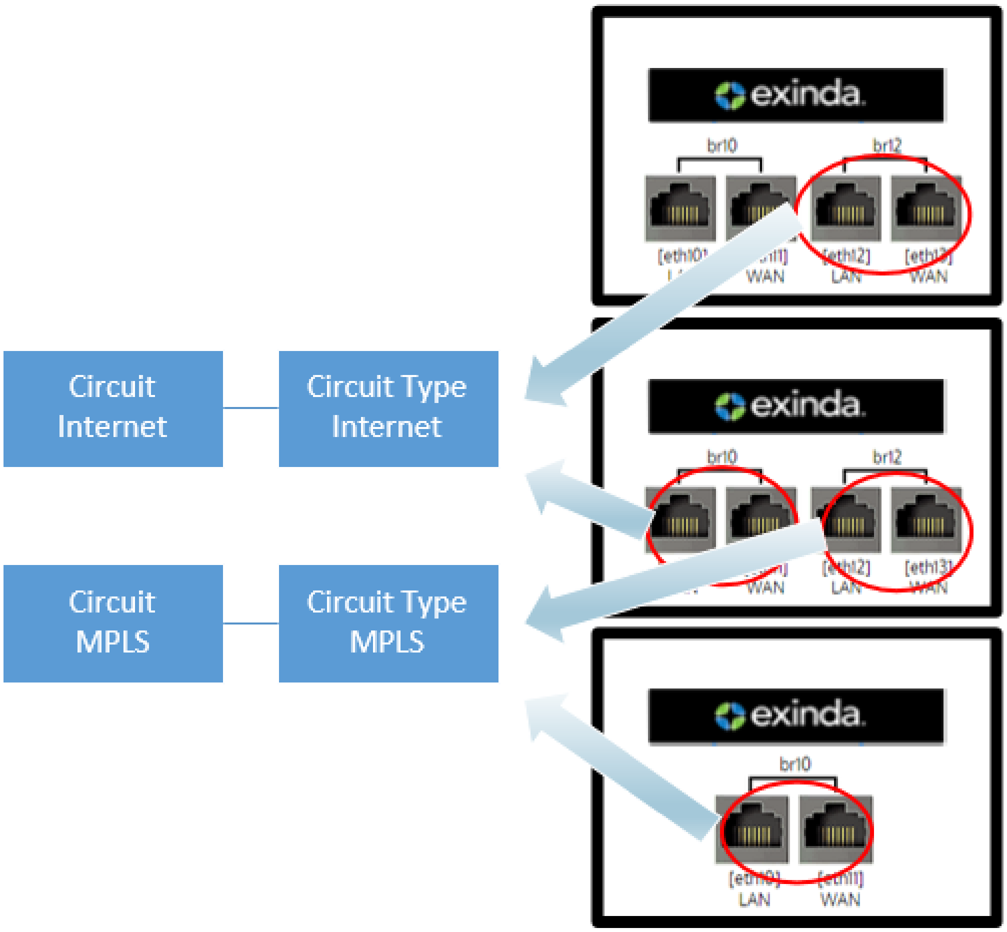
Create network object ...
Add Network Object from Library ...

Name ▲	IP Network Address	Monitoring	
Engineering	10.10.1.0/24	✓	🔒
Finance	10.11.0.0/16	✓	🔒
Marketing	10.50.1.0/24		✖
Operations	10.30.0.0/16	✓	🔒
Support	10.10.10.5/32	✓	🔒

9. Define Circuit Types

A Circuit Type is a container that binds appliance bridges to a circuit so policies within the circuit apply only to the bridges in that circuit type. The following example will further clarify the concept of circuit types:

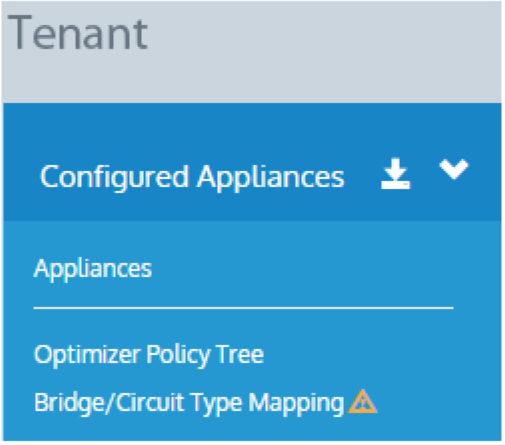
© 2016 Exinda Networks Inc.



Consider the following:

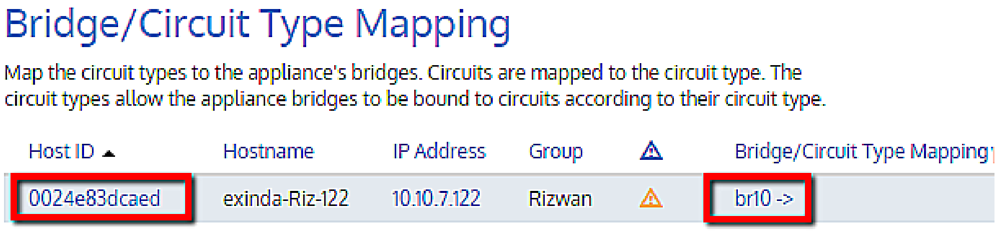
- Bridge **br12** from first appliance and bridge **br10** from second appliance are both bound to circuit type "Internet". If this circuit type is tied to the "Internet" circuit,' then all the policies within this circuit will apply to bridge br12 on the first appliance and br10 on the second appliance.
- Bridge **br12** on the second appliance and bridge **br10** from third appliance are bound to circuit type "MPLS". If this circuit type is tied to the "MPLS" circuit, then all the policies within this circuit will apply to bridge br12 on the second appliance and br10 on the third appliance.
- If an appliance is moved in the Configured Appliances group, by default the appliance bridge will not bind to the circuit type and a warning icon appears next to the Bridge/Circuit Type Mapping

item.:



9a. Create Circuit Type

1. Navigate to the Bridge/Circuit Type Mapping page within Configured Appliances page.
2. Click either the **Host ID** or **Bridge ID** of the appliance to bind the circuit type to the bridge.



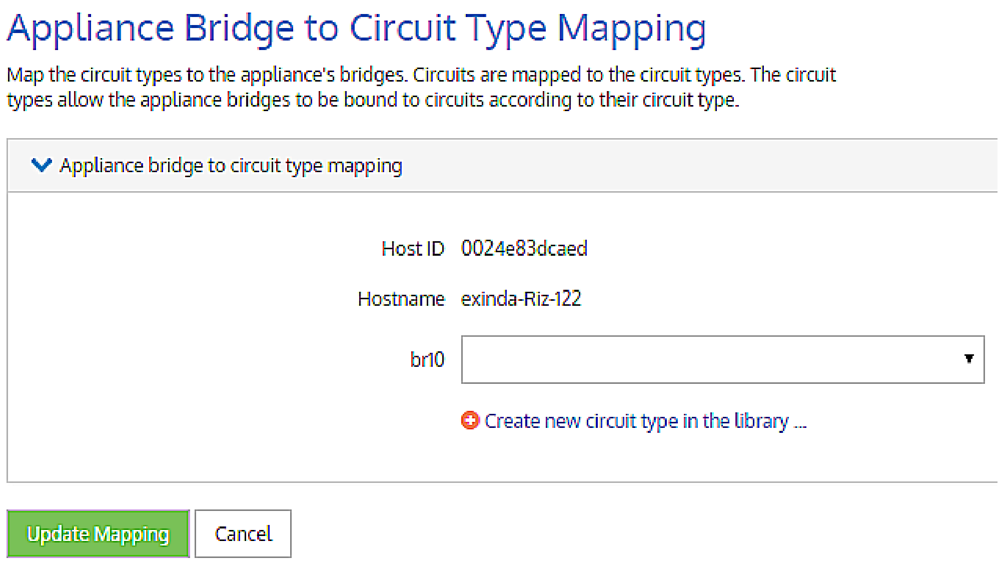
Bridge/Circuit Type Mapping

Map the circuit types to the appliance's bridges. Circuits are mapped to the circuit type. The circuit types allow the appliance bridges to be bound to circuits according to their circuit type.

Host ID ▲	Hostname	IP Address	Group	⚠	Bridge/Circuit Type Mapping
0024e83dcaed	exinda-Riz-122	10.10.7.122	Rizwan	⚠	br10 ->

3. You could select the already created circuit types from the drop down menu or create a new

circuit type.



Appliance Bridge to Circuit Type Mapping

Map the circuit types to the appliance's bridges. Circuits are mapped to the circuit types. The circuit types allow the appliance bridges to be bound to circuits according to their circuit type.

Appliance bridge to circuit type mapping

Host ID 0024e83dcaed

Hostname exinda-Riz-122

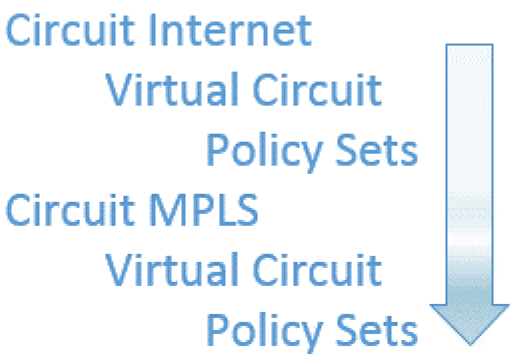
br10

Create new circuit type in the library ...
Update Mapping
Cancel

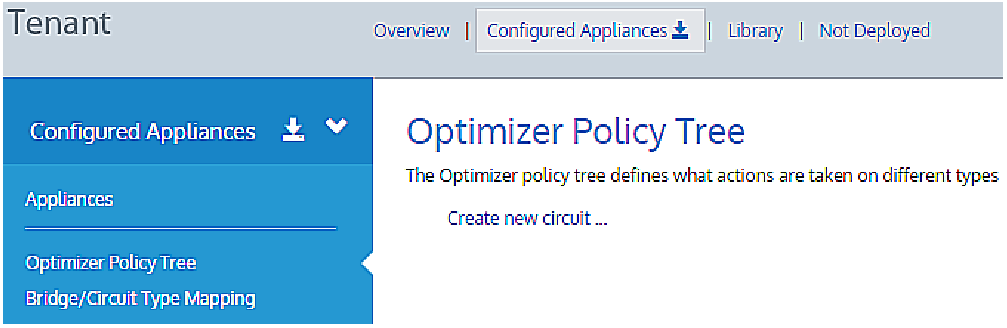
The recommendation is that you give the circuit type the same name as circuit as it makes it easier to map them together.

10. Optimizer Policy Tree (OPT)

The Optimizer Policy Tree outlines what actions can be taken on different types of traffic going through the appliance. The tree is processed in a top-down order and policies on traffic are applied in that order.



Navigate to Optimizer Policy Tree within Configured Appliances Page.

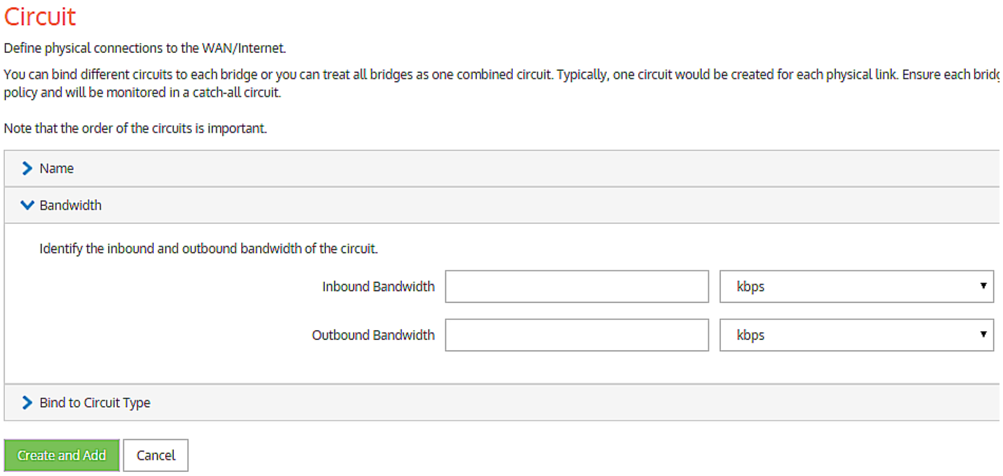

Tenant
Overview | Configured Appliances | Library | Not Deployed
Configured Appliances
Appliances
Optimizer Policy Tree
Bridge/Circuit Type Mapping
Create new circuit ...

Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different types

10a. Circuits

1. Define physical connections to the WAN/Internet. Click **Create new circuit...**
2. Name the circuit, program the desired bandwidth and bind the circuit to the circuit type.



Circuit

Define physical connections to the WAN/Internet.

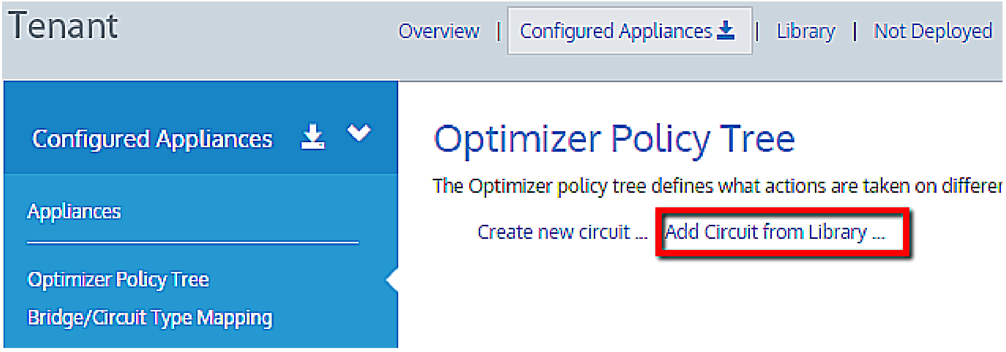
You can bind different circuits to each bridge or you can treat all bridges as one combined circuit. Typically, one circuit would be created for each physical link. Ensure each brid policy and will be monitored in a catch-all circuit.

Note that the order of the circuits is important.

Identify the inbound and outbound bandwidth of the circuit.

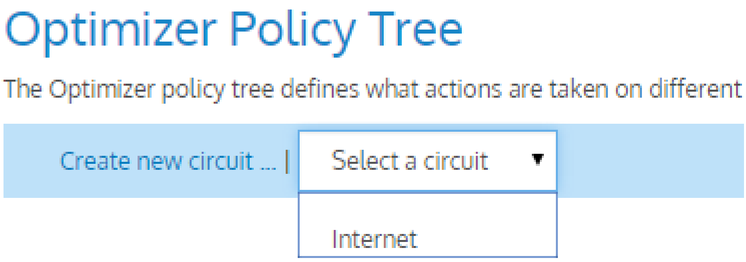
Inbound Bandwidth		kbps
Outbound Bandwidth		kbps

3. If a circuit exists in a library then you can add it from there. Click **Add Circuit from Library...** and select a desired circuit.


Tenant
Overview | Configured Appliances | Library | Not Deployed
Configured Appliances
Appliances
Optimizer Policy Tree
Bridge/Circuit Type Mapping
Create new circuit ...
Add Circuit from Library ...

Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on differer



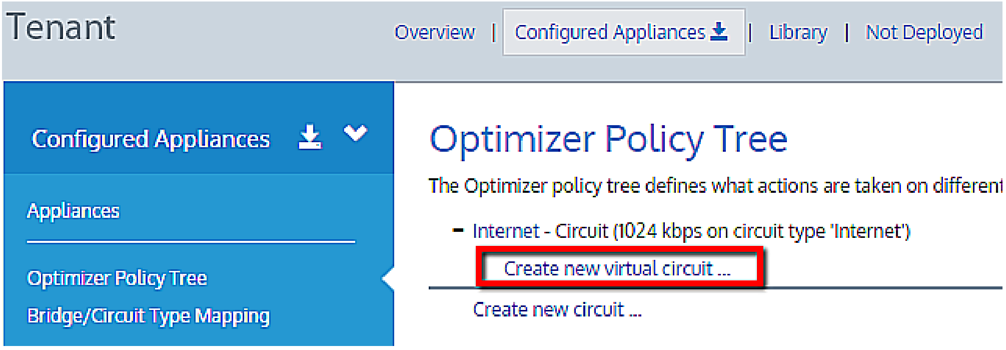
Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different

10b. Virtual Circuits

Virtual circuits logically partition the circuit. The virtual circuit defines the traffic that is processed in the partition and how much bandwidth it will use. Each virtual circuit has its own set of policies.

1. Click **Create new virtual circuit…**

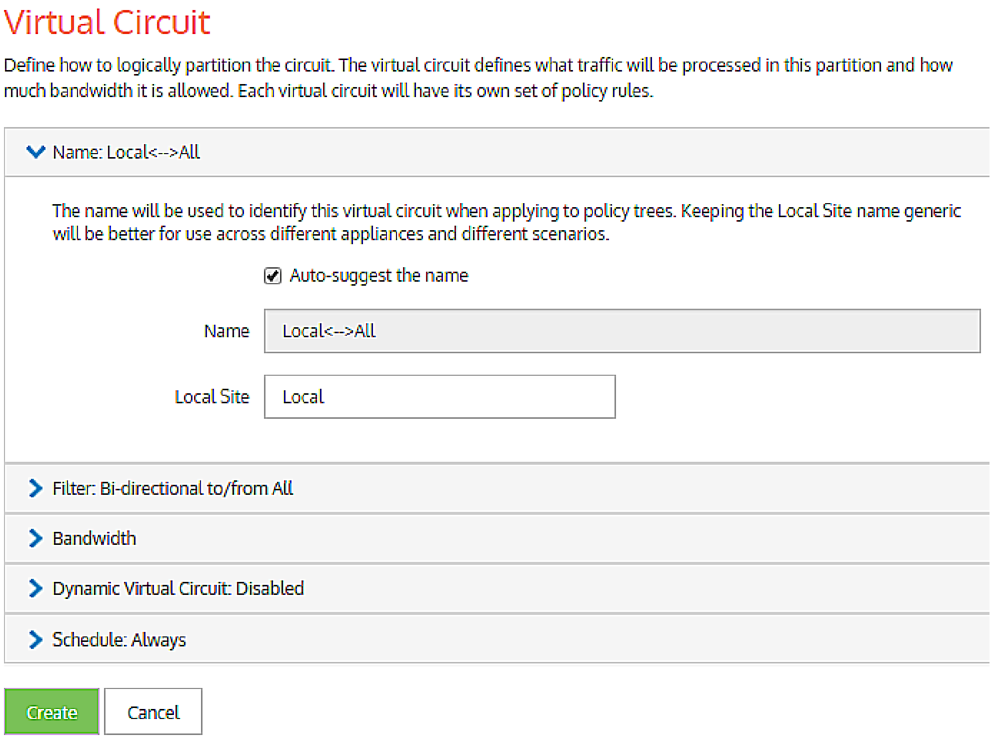

Tenant
Overview | Configured Appliances | Library | Not Deployed
Configured Appliances
Appliances
Optimizer Policy Tree
Bridge/Circuit Type Mapping
Create new virtual circuit ...
Create new circuit ...

Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different

- Internet - Circuit (1024 kbps on circuit type 'Internet')

2. Define the virtual circuit and click ‘Create and Add’.



Virtual Circuit

Define how to logically partition the circuit. The virtual circuit defines what traffic will be processed in this partition and how much bandwidth it is allowed. Each virtual circuit will have its own set of policy rules.

Name: Local<-->All

The name will be used to identify this virtual circuit when applying to policy trees. Keeping the Local Site name generic will be better for use across different appliances and different scenarios.

☑ Auto-suggest the name

Name: Local<-->All

Local Site: Local

Filter: Bi-directional to/from All

Bandwidth

Dynamic Virtual Circuit: Disabled

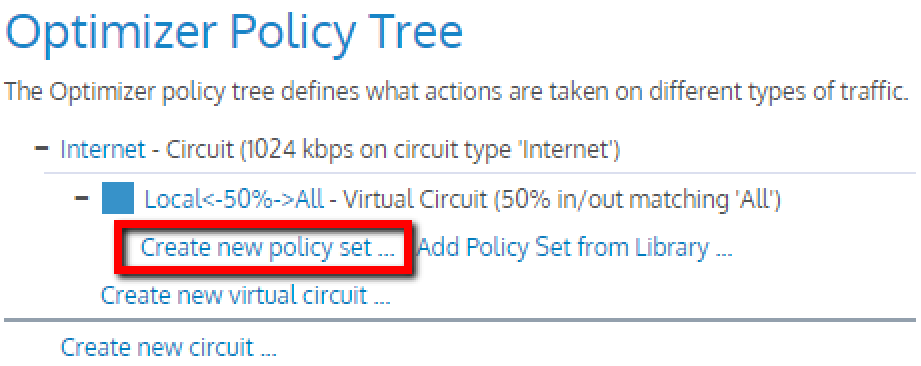
Schedule: Always

Similar to circuits, virtual circuits can be added from the library, if present.

10c. Policy/Policy Sets

Polices define what actions are to be taken on different types of traffic.

1. There are two options:
   a. Click **Create new policy set...** to create your own set of policies.



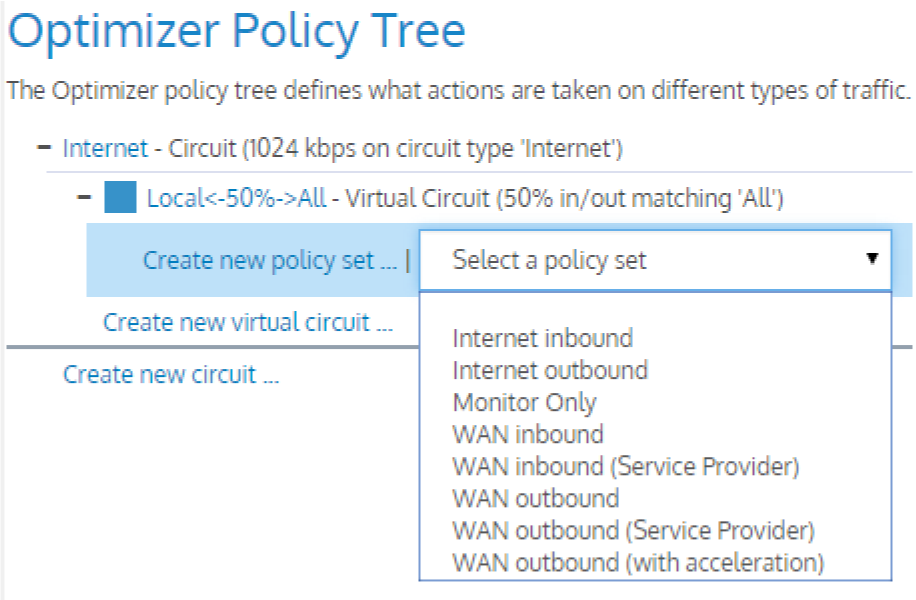
Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different types of traffic.

- Internet - Circuit (1024 kbps on circuit type 'Internet')
  - Local<-50%->All - Virtual Circuit (50% in/out matching 'All')

Create new policy set ...
Add Policy Set from Library ...
Create new virtual circuit ...
Create new circuit ...

b. Click **Add Policy Set from Library...** to select a pre-defined policy set template for a different type of traffic.

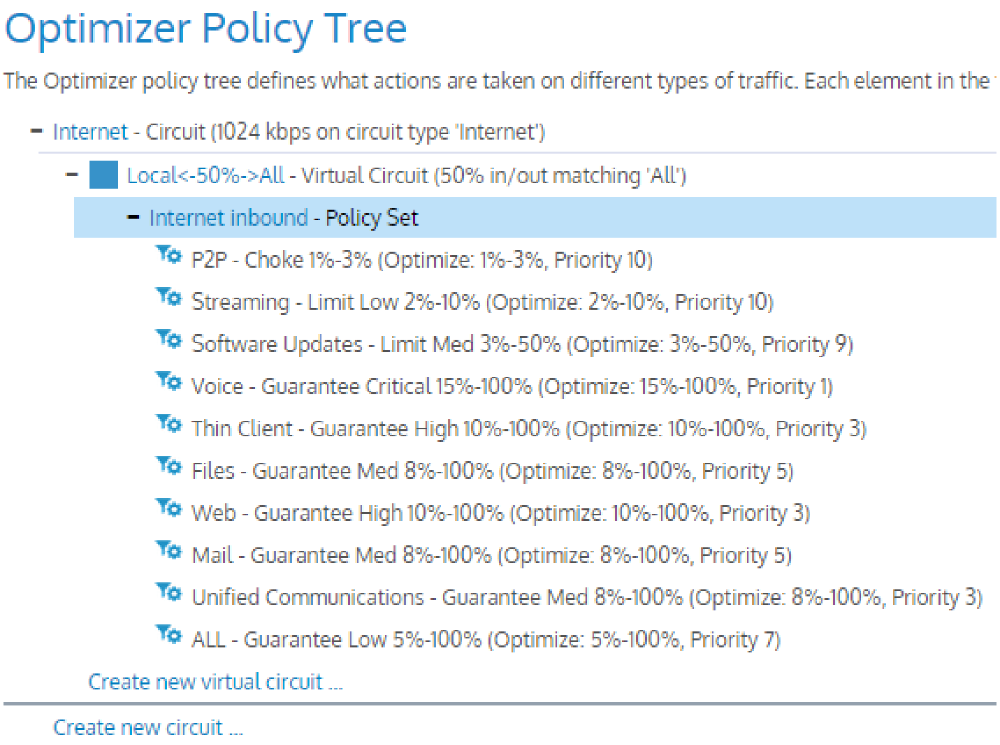


Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different types of traffic.

- Internet - Circuit (1024 kbps on circuit type 'Internet')
  - Local<-50%->All - Virtual Circuit (50% in/out matching 'All')
    - Create new policy set ... | Select a policy set ▼
      - Internet inbound
      - Internet outbound
      - Monitor Only
      - WAN inbound
      - WAN inbound (Service Provider)
      - WAN outbound
      - WAN outbound (Service Provider)
      - WAN outbound (with acceleration)
    - Create new virtual circuit ...
- Create new circuit ...

2. In this example, the Internet outbound policy set is selected and it automatically populates all the policies within this set into the virtual circuit:



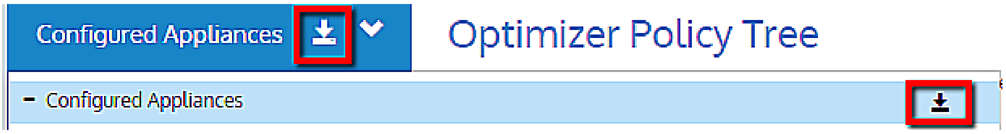
Optimizer Policy Tree

The Optimizer policy tree defines what actions are taken on different types of traffic. Each element in the

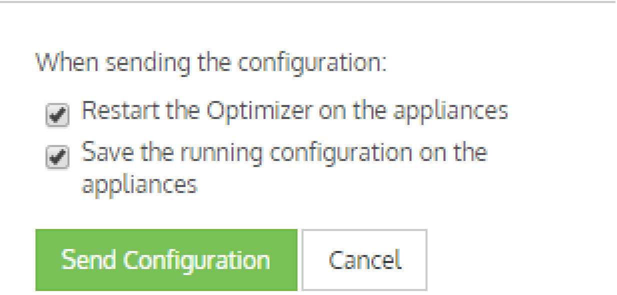
- Internet - Circuit (1024 kbps on circuit type 'Internet')
  - Local<-50%->All - Virtual Circuit (50% in/out matching 'All')
    - Internet inbound - Policy Set
      - P2P - Choke 1%-3% (Optimize: 1%-3%, Priority 10)
      - Streaming - Limit Low 2%-10% (Optimize: 2%-10%, Priority 10)
      - Software Updates - Limit Med 3%-50% (Optimize: 3%-50%, Priority 9)
      - Voice - Guarantee Critical 15%-100% (Optimize: 15%-100%, Priority 1)
      - Thin Client - Guarantee High 10%-100% (Optimize: 10%-100%, Priority 3)
      - Files - Guarantee Med 8%-100% (Optimize: 8%-100%, Priority 5)
      - Web - Guarantee High 10%-100% (Optimize: 10%-100%, Priority 3)
      - Mail - Guarantee Med 8%-100% (Optimize: 8%-100%, Priority 5)
      - Unified Communications - Guarantee Med 8%-100% (Optimize: 8%-100%, Priority 3)
      - ALL - Guarantee Low 5%-100% (Optimize: 5%-100%, Priority 7)
    - Create new virtual circuit ...
- Create new circuit ...

11. Push Configuration

Once all the desired changes have been made to the group, you can simply push the configuration by clicking on the download icon:



If multiple appliance groups exist, then you can push the configuration individually for an appliances group by clicking on the main Configured Appliances download button. This pushes the configuration to all the appliances groups and appliances within them. Pushing the configuration restarts the Optimizer and saves the configuration on the appliance:



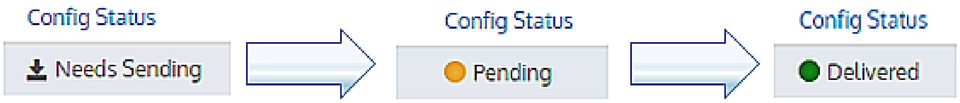
When sending the configuration:

☑ Restart the Optimizer on the appliances

☑ Save the running configuration on the appliances

When the configuration is being edited, the configuration status is **Needs Sending**. When the configuration is pushed, the status changes to **Pending**, and when the appliance receives the configuration, the status changes to **Delivered.**

Life cycle of configuration status:

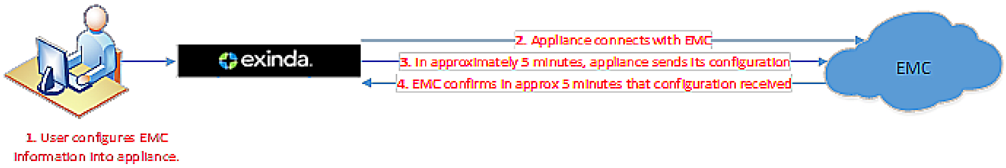


What Happens When an Appliance Calls in to EMC?

After EMC settings are configured on the appliance side ("Basic Configuration" on page 52), the appliance calls in to the EMC for the first time. There can be a delay of up to five minutes while the appliance sends its current configuration to the EMC. Once the full configuration is received, the EMC confirms the configuration, which may also take up to five minutes. The Bridge/Circuit Type mapping is not available on the EMC until the appliance has been online for about ten minutes. During this period, the EMC displays a message indicating that it is waiting for the appliance to call in.

© 2016 Exinda Networks Inc.

Once you move the appliance to a group, and you push configuration to the group, the appliance then receives the updated configuration when it next calls in to the EMC.

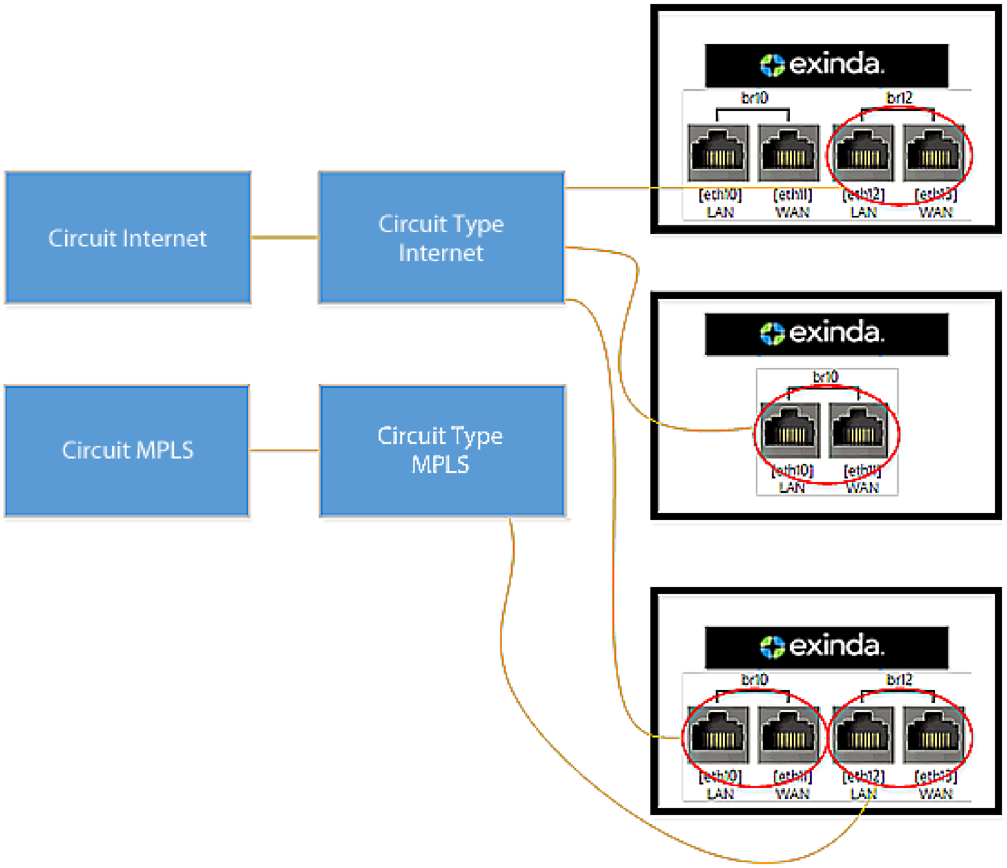

exinda.
2. Appliance connects with EMC
3. In approximately 5 minutes, appliance sends its configuration
4. EMC confirms in approx 5 minutes that configuration received
EMC
1. User configures EMC
information into appliance.

How to Configure Your Bridge

It is important to understand the relationship between bridges, circuits, and circuit types before you start creating policy. Consider the following:

- **Circuit** – defines the physical connections to the WAN or Internet and the inbound and outbound bandwidth and the named circuit type. On the appliance, the circuit specifies which named bridge or bridges it is bound to.
- **Circuit Type** – an abstract concept that creates a virtual binding between the circuits and the appliance bridges. Circuit Types represent the intended use of a circuit. This allows you to configure a circuit for multiple appliances without requiring the bridges on the appliances to have the same name, such as br10. This is favorable where the number of bridges or names of bridges or the cabling of the bridges is not consistent across the appliances.

For an appliance to receive the Optimizer Policy Tree configuration rooted with a particular circuit, the bridge on the appliance must be mapped to the same Circuit Type as that Circuit. For example, if the circuit is bound to circuit type "Internet", and the appliance bridge(s) is mapped to 'Internet', then that circuit configuration is sent to that appliance bound to the specific bridges.



Use Library Items to Create a Consistent Definition and Naming Strategy

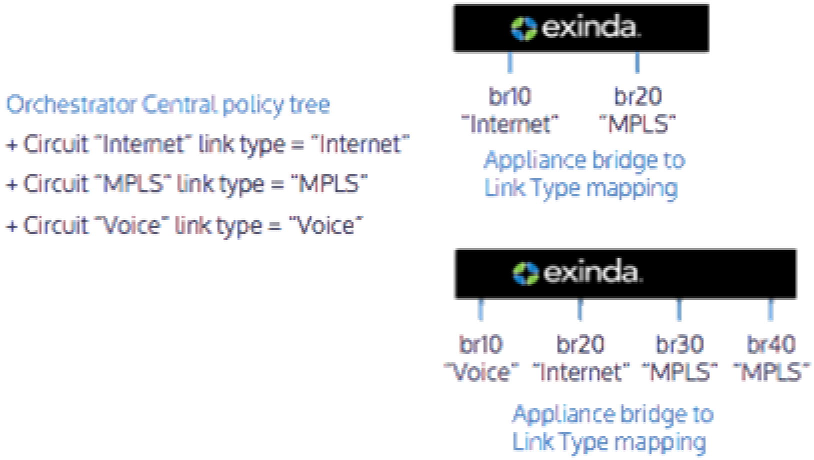
Current naming practices can make it complicated to track and understand the mappings between bridges, circuit types and circuits. Each bridge on an appliance is usually named with no relevancy to the purpose of the bridge . To simplify bridge configuration within the EMC, you should first focus on creating common Circuit Types and Circuits to create consistency throughout the appliances. By labeling circuits and circuit types within the library, and then mapping the library items to bridges, you can create an Optimizer Policy Tree that covers multiple scenarios.

For example, consider two different appliances with a different numbers of bridges and where they are cabled differently:

- The first appliance has two bridges, br10 and br20, where br10 is mapped to the "Internet" Circuit Type and br20 is mapped to the "MPLS' Circuit Type.
- The second appliance has four bridges, br10, br20, br30, and br40, where br10 is mapped to "Voice", br20 is mapped to "Internet", and br30 and br40 are mapped to "MPLS".

If you add the common Circuit Types used above to Library items, you can reuse the named Circuit Types when performing the bridge/circuit type mapping in the Optimizer Policy Tree.

© 2016 Exinda Networks Inc.

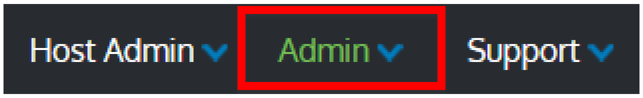

Orchestrator Central policy tree
+ Circuit "Internet" link type = "Internet"
+ Circuit "MPLS" link type = "MPLS"
+ Circuit "Voice" link type = "Voice"
exinda
br10 "Internet"
br20 "MPLS"
Appliance bridge to Link Type mapping
exinda
br10 "Voice"
br20 "Internet"
br30 "MPLS"
br40 "MPLS"
Appliance bridge to Link Type mapping

Basic Configuration

To configure the Exinda Management Center to communicate with the Exinda Network Orchestrator appliances, follow the workflow below. After you complete the steps, you are ready to create policy and send it to your appliance groups.

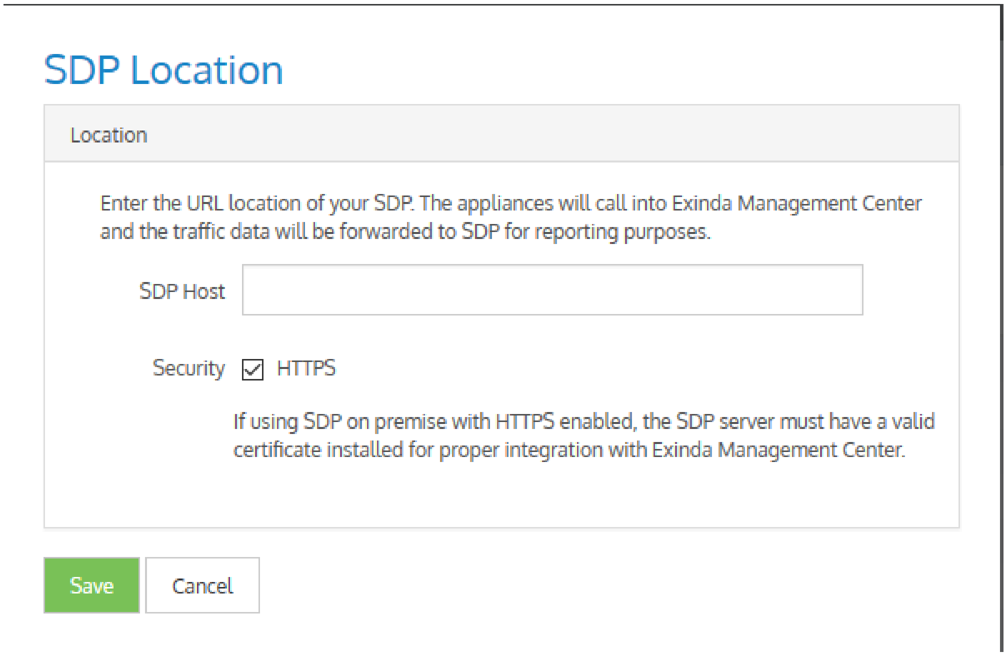
1. Identify the SDP Location on the Exinda Management Center (if forwarding data to an SDP server).

Configure the location of your SDP so that data from the appliances is forwarded to this SDP.



© 2016 Exinda Networks Inc.

At the top right of the interface, click **Admin > SDP Location** and specify the location of your SDP. *The "SDP Location" configuration pop-up opens.*



SDP Location

Location

Enter the URL location of your SDP. The appliances will call into Exinda Management Center and the traffic data will be forwarded to SDP for reporting purposes.

SDP Host

Security ☑ HTTPS

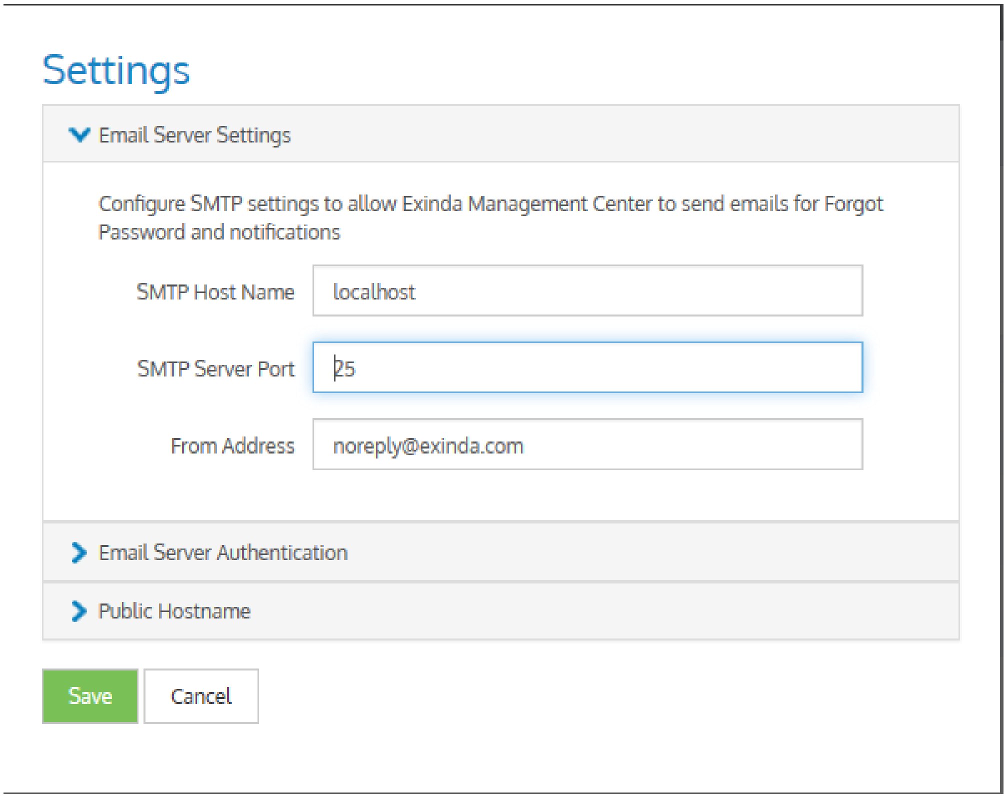
If using SDP on premise with HTTPS enabled, the SDP server must have a valid certificate installed for proper integration with Exinda Management Center.

All tenants will be associated with the same SDP.

2. Configure Administrator Email Settings

The mail server is used to send emails when a user needs to use the Forgot Password functionality.

At the top right of the interface, click **Admin > SMTP Server Settings** and specify the location of your Mail Server settings.



Settings

Email Server Settings

Configure SMTP settings to allow Exinda Management Center to send emails for Forgot Password and notifications

SMTP Host Name: localhost

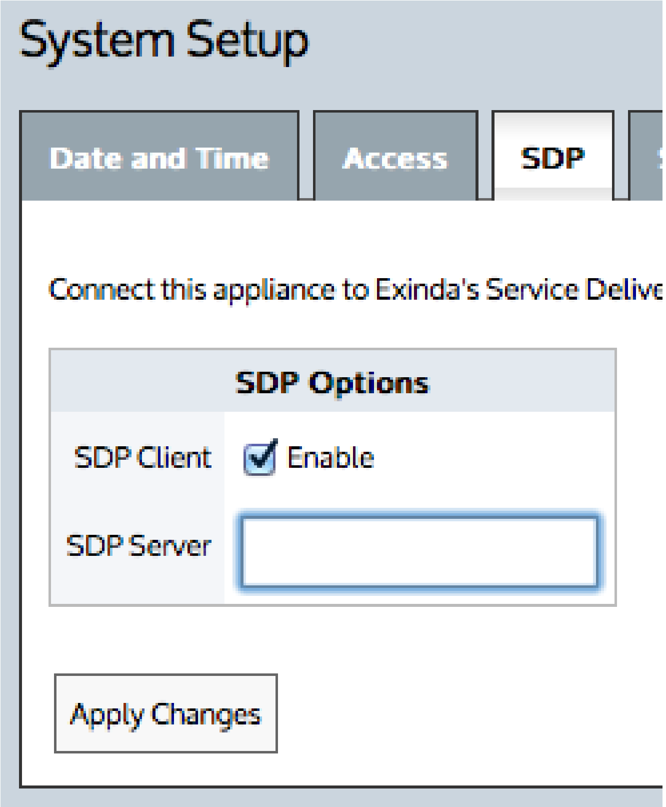
SMTP Server Port: 25

From Address: noreply@exinda.com

3. Configure your appliances to communicate with Exinda Management Center

This step requires configuration on the Network Orchestrator appliances.

On each of your appliances, set the SDP setting to your EMC location using **Configuration > System > Setup > SDP** tab.



Connect this appliance to Exinda's Service Delive

SDP Options

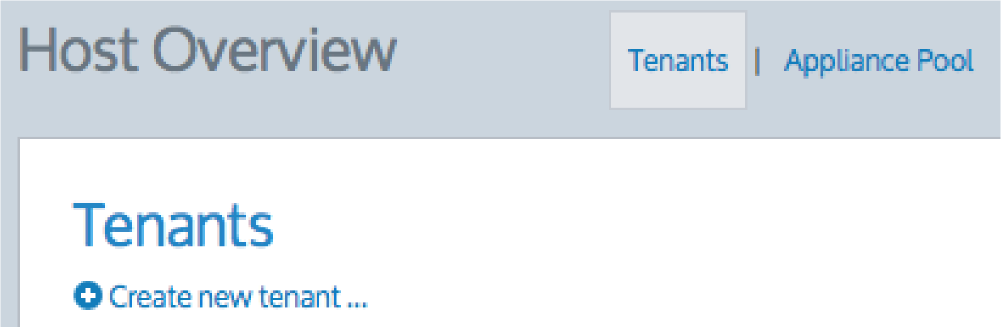
SDP Client	☑ Enable
SDP Server	

The appliance then calls into Exinda Management Center every 5 minutes to retrieve new configuration and to provide traffic data, which will be forwarded from Exinda Management Center to SDP.

4. Add Tenants

> **NOTE:**
>
> *This screen appears only if using an on-premises instance of EMC.*

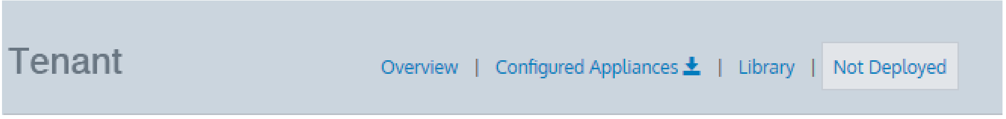
In the EMC web UI, click **Create new tenant** at the top of the tenant tree and specify the name of your tenant.



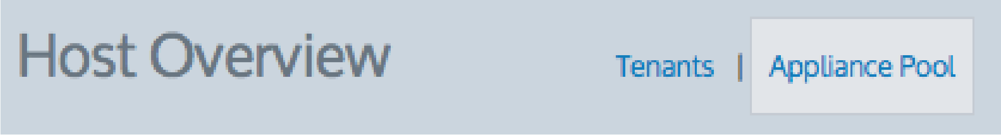
After you have created the tenant, click the tenant in the list to start managing the appliances in the tenancy.

5. Add Appliances to Tenants

Wait for your appliance(s) to call in. If using the Exinda-hosted service or an on-premises instance with a single tenant, the appliance appears in the Not Deployed group.

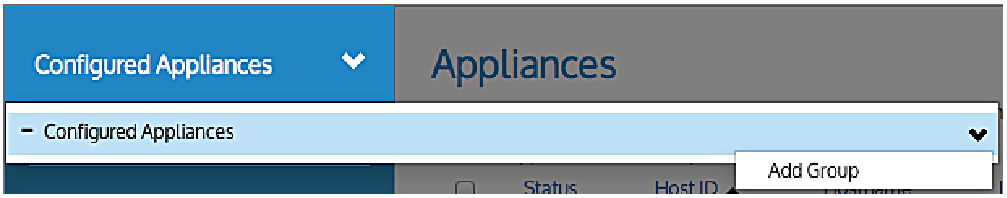


If you are using a multi-tenant on-premises instance, the appliance will appear in the **Appliance Pool**. Move the appliance from the **Appliance Pool** to **Unallocated** under the appropriate tenancy.

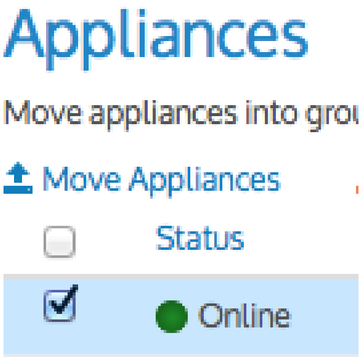


6. Create Appliance Groups within a Tenant (optional)

Create an appliance group hierarchy under Configured Appliances. Appliances can be added to these groups. All appliances under the same group will receive the same configuration. Groups can be created hierarchically. Go to the Configured Appliances area. Click the drop down caret on the blue menu heading. Click the drop down caret on the desired appliance group and select **Add Group**. Learn more.



Move the appliances from the Not Deployed group to the Configured Appliances group (or one of the appliance groups that you created). Only appliances in a configured appliances group can be configured by Exinda Management Center. Select an appliance in the **Not Deployed** list and click **Move Appliances**. Learn more.



Appliances

Move appliances into grou

When basic configuration is complete, you can begin creating policy in the "Optimizer Policy Tree" on page 61.

Chapter 3: Introduction to Configuring Policy

This chapter deals with defining policy for the traffic entering and exiting your network. See the following topics for more information:

Creating Policies for Appliance Groups

After basic configuration is complete, proceed to configure the options below.

1. IMPORTANT: Configure the local network object for each appliance.

The system uses the local network object to determine the location of all other network objects. The location of network objects is used to determine whether hosts and users are internal or external to the LAN behind your Network Orchestrator appliance. In the Configured Appliances area, select Local Network Objects in the menu. Click the appliance where you want to configure the local network object. Learn more.

2. Configure your network objects (Optional)

Network objects are used for identifying the traffic affected by the policy as well as for monitoring traffic. Consider the following:

- If you want to use a network object in the creation of a virtual circuit or policy, create a network object in the library. If you imported your network objects from your appliance, you may not need to create any network objects.
- If you want to send a network object to the appliance for monitoring purposes (not for policy creation), then create a network object in the configured appliance group, which also adds the network object to the library. Or create a network object in the library then add it to the configured appliances group.
- If you use a network object in the definition of a virtual circuit or policy for a given appliance group, then the network object is automatically added to the appliance group configuration. Learn more.

3. Configure custom applications (Optional)

Custom applications can be used for both identifying traffic affected by the policy, and for monitoring traffic. Consider the following:

- If you want to use a custom application in the creation of your virtual circuit or policy, create a custom application in the library. When you create or edit the Virtual Circuits or policies, your custom application becomes available for selection.
- If you want to send a custom application to the appliance for monitoring purposes, you need to add the application to a monitored application group.
- If you use a custom application in the definition of a virtual circuit or policy for a given appliance group, then the custom application is automatically added to the appliance group configuration. Learn more.

4. Configure schedules (Optional)

Schedules can be used to specify when policies or virtual circuits takes effect. If you want to use a schedule in the creation of your virtual circuit or policy, first create a schedule in the library. When you create or edit the virtual circuits or policies, your schedule can then be selected and automatically added to the appliance group configuration. Learn more

5. Configure the Optimizer Policy Tree on the Configured Appliances group (or on one of the appliance groups that you created)

Each object element of the Policy Tree is stored in the library for use by other appliance groups or other areas within the Optimizer Policy Trees. Learn more about the Optimizer Policy Tree.

⚠ **IMPORTANT**

When appliances are moved out of the Configured Appliances group to the Unallocated Appliances group or the Appliance Pool, the configuration that was applied using the edit forms is automatically removed from the appliances upon the next call into the Exinda Management Center.

6. Create named Circuit Types.

The circuit type specifies the intended use of a circuit, for example, "Internet", "Voice", or "MPLS". Circuits and appliance bridges are mapped to these circuit types. The circuit is sent to the appliances that have bridges mapped to the same circuit type as the circuit. Go to the library and create your required circuit types. Learn more.

7. Map the appliance bridges to the Circuit Types.

This determines the bridges to which the circuits are mapped on the appliances. Go to the configured appliances. Click Bridges/Circuit Type Mapping, and for each appliance specify the Circuit Type for each bridge. Learn more.

8. Create a circuit

Circuits specify the physical connections to the WAN or Internet. Create a circuit in the Optimizer Policy tree for the configured appliance group. Or create a circuit in the library and add it to the Optimizer Policy tree for the configured appliance group. Learn more

9. Create a virtual circuit

Virtual circuits define what traffic is processed in a partition and how much bandwidth it is allowed. Create a virtual circuit in the Optimizer Policy tree for the configured appliance group. Or create a virtual circuit in the library and add it to the Optimizer Policy tree for the configured appliance group. Learn more.

10. Add a policy set

Policy sets are groups of policies that will be added to the Virtual Circuits. There are pre-created policy sets in the library that correspond to the sets that result from running the wizard on the appliance.

Add a policy set to a configured appliance group Optimizer Policy tree virtual circuit. You can also create policy sets from the Optimizer Policy tree or in the library. Learn more.

11. Add or edit a policy (Optional)

Policies are the rules that control the traffic. When adding or editing a policy set, you can add or edit a policy. Learn more.

12. Send the Configuration to the Appliance Group

Changes are sent to the appliances within an Appliance Group only when you choose to send the configuration. Learn more.

Optimizer Policy Tree

All network behavior that you need to modify is specified by policies in the optimizer. This includes traffic shaping, prioritization, acceleration, and packet marking. These policies are arranged hierarchically in a tree so that you can assign different policy rules to different types of traffic on your network. The hierarchy consists of circuits, virtual circuits, policy sets, and policy rules. Note that policy sets are a concept within EMC only; they do not exist on Network Orchestrator appliances.

Policy sent to the appliance is dependent on Circuit Type

When the Optimizer Policy Tree is assigned to an appliance group, generally, all appliance groups that are nested under that group inherit the Optimizer Policy Tree. In which case, a message area above the Policy Tree indicates that the tree is inherited. If you do not want child appliance groups to inherit the tree, you can stop the inheritance.

All the appliances within a group will potentially receive that Policy Tree when the policy is sent. An appliance receives the Policy Tree configuration that corresponds to its bridge/circuit type mapping.

EXAMPLE

Consider a Policy Tree with three circuits, Internet, MPLS, and Voice, where the circuits map to Circuit Types of the same name. For example, Internet maps to a circuit type named "Internet". Now consider an appliance (within this Policy Tree's appliance group) that has its two bridges mapped to only two of these circuits: br10 to Internet, and br20 to MPLS. When the configuration is sent to this appliance, the circuit "Internet" is mapped to the appliance's bridge br10 and the circuit "MPLS" is mapped to the appliance's bridge br20. The "Voice" circuit is not be sent to the appliance as there is not a matching circuit type.

Policy sets can be reused in multiple Virtual Circuits

Policy sets are a concept within the EMC only. You can create a named policy set then apply the policy set to multiple virtual circuits. All virtual circuits using the policy set then have exactly the same policy.

Everything references a library item

Within a tenant, the EMC treats everything as a library item so that the configuration components can be reused. When you modify a library item, everywhere it is used is also affected. For example, when you create and reuse a virtual circuit, whenever that virtual circuit is changed, all instances of its use are also changed.

Required objects will automatically be queued to be sent

When policy rules or virtual circuits use objects in their definitions, such as network objects or schedules, then those objects are automatically added to the configuration that must be sent to the appliances.

All other uses of the Policy Tree and its components are the same as on the appliance itself. Read Optimizer Policy Tree on the previous page in the Exinda User Guide for more information of how the Policy Tree manages traffic.

Where do I find the Optimizer Policy tree?

Select your Configured Appliances groups (or any custom group under it), then select **Optimizer Policy Tree**.

To add a circuit to the Policy Tree

1. In the Optimizer Policy Tree, click **Create new circuit**. Learn more about Circuits.
   The circuit will be added to the Optimizer Policy Tree and to the library.
2. Or in the Optimizer Policy Tree, click **Add Circuit from Library**.

> **NOTE**
> ***The link is replaced with a drop-down list where you can select from a list of circuits in the library. However, note that the circuits that have already been used in the Policy Tree do not appear in the drop-down list. If the link is not present, there are no circuits in the library that have not already been included in the Policy Tree.***

Upon selecting a circuit, it will appear in the Optimizer Policy Tree.

To add a virtual circuit to the Policy Tree

Do *one* of the following:

- In the Optimizer Policy Tree, under the desired circuit, click **Create new virtual circuit**. Learn about Virtual Circuits.
  The virtual circuit will be added to the Optimizer Policy Tree and to the library.

- Or in the Optimizer Policy Tree, click **Add Virtual Circuit from Library**.

> NOTE
>
> *The link is replaced with a drop-down list where you can select from a list of Virtual circuits in the library. However, note that the circuits that have already been used in the Policy Tree do not appear in the drop-down list. If the link is not present, there are no Virtual circuits in the library that have not already been included in the Policy Tree.*

Upon selecting a virtual circuit, it will appear in the Optimizer Policy Tree.

To add a policy set to the Policy Tree

1. In the Optimizer Policy Tree, under the desired virtual circuit, click **Create new policy set**.
   The policy set will be added to the Optimizer Policy Tree and to the library.
2. Or in the Optimizer Policy Tree, click **Add Policy Set from Library**.

> NOTE
>
> *The link is replaced with a drop-down list where you can select from a list of policy sets in the library. If the link is not present, there are no Virtual circuits sets in the library that have not already been included in the Policy Tree.*

Upon selecting a policy set, it will appear in the Optimizer Policy Tree.

To add a policy rule to the Policy Tree

1. Click the policy set to which you would like to add the policy.
2. In the policy set form, create a policy or add a policy from the library.
3. Click **Update in Library**.

To reorder Virtual Circuits

In the Optimizer Policy Tree, drag and drop the virtual circuit to its new location.

To reorder a policy rule

1. Click the policy set that contains the policy that you would like to reorder.
2. In the policy set form, drag and drop the policy to its new location.
3. Click **Update in Library**.

To remove elements from the Policy Tree

For each element that you want to remove, click the 'x' at the far right.

> **NOTE**
> *You cannot delete elements from the Policy Tree if you are looking at a sub appliance group that inherits the Policy Tree. You must edit the Policy Tree in the appliance group that defined the tree.*

To disinherit an appliance group from a Policy Tree

1. When an appliance group inherits an Optimizer Policy Tree, there is a banner across the top indicating that it is inherited.
2. Click **Stop inheriting Policy Tree**.
   The tree is removed and you can start building up another Policy Tree.

Bridge to Circuit Type Mapping

For an appliance to receive the Optimizer Policy Tree configuration rooted with a particular circuit, the bridge for an appliance must be mapped to the same Circuit Type as that Circuit. That is, if the circuit is bound to circuit type 'Internet' and the appliance bridge(s) is mapped to 'Internet', then the circuit configuration sent to that appliance is bound to the specific bridges.

The Bridge to Circuit Type Mapping list shows each appliance in the appliance group. You can edit the Bridge to Circuit Type Mapping for each appliance. A warning icon appears next to each appliance that does not have any of its bridges mapped. This warns that the appliance will not be sent any part of the Optimizer Policy Tree configuration. Also, the warning icon will be shown in the blue menu (on the left) next to the Bridge to Circuit Type Mapping menu item, if there are any appliances with a warning icon.

Where do I find Bridge to Circuit Type Mappings?

The Bridge to Circuit Type Mappings are found in **Configured Appliances** (or a nested appliance group) **> Bridge to Circuit Type Mapping**

To edit an appliance's bridge to circuit type mapping

1. Click the **Host ID** or **Bridge to Circuit Type Mapping**.
2. For each bridge, select a circuit type from the drop-down list. If the desired named circuit type is not in the list, click **Create new circuit type in the library...** to create a new circuit type. Once created, it is then available in the drop-down list.
3. Click the **Update Mapping** button.

Why does it say Pending in the Bridge to Circuit Type Mapping column?

Pending means that the Exinda Management Center has not received the list of bridges from the appliance yet. The first time the appliance calls in, the Exinda Management Center requests bridge information from the appliance. Note that in general, there should not be much time between the first communication and the second communication with the bridge information.

NOTE

This may also occur if you are using an appliance with a firmware version prior to the 7.0.2 Update 1.

What triggers a warning?

- If none of the bridges are mapped to a circuit type, then a warning appears for the specific appliance.
- If there is one or more appliances with a warning, then a warning appears next to the Bridge to Circuit Type Mapping menu item.

What happens to the mappings when I move an appliance?

- The bridge retains its circuit type mappings when moving between appliance groups.
- If the appliance is moved to the **Not Deployed** area, then the circuit type mapping is removed.

Chapter 4: Introduction to Configuring Appliance Communications

This chapter deals with configuring network communications for your appliances. See the following topics for more information:

© 2016 Exinda Networks Inc.

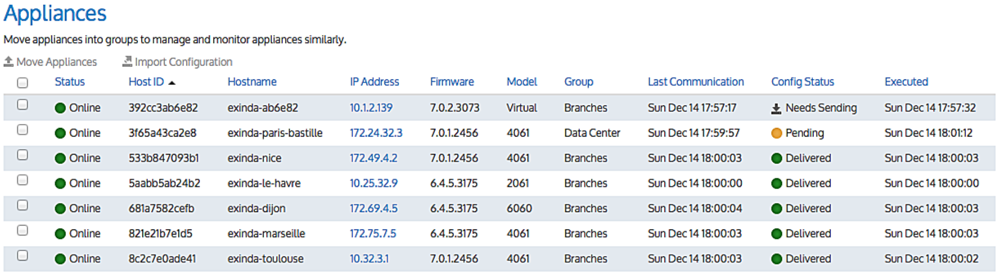
Managing your Network Orchestrator Appliances

The appliances list shows the appliances that are being managed in the Exinda Management Center. The list shows inventory details, online/offline communication status, and configuration status. You can move the appliances to configuration groups or to the not deployed (unallocated) group. You can also import the network object configuration and the policy configuration from an appliance into the library. You can launch the Web UI of the appliance by clicking on the IP address. Note that it is a simple launch of the UI. If the appliance is subject to NAT, then the Web UI will not be available.

The Status Column indicates the online or offline status and the Last Communication column shows the date and time of last communication. Note that the system shows an appliance as offline if it has not called in within 15 minutes, which covers three scheduled call-in periods.

The **Config Status** – column shows the state of the configuration and the date and time of the last configuration status change:

- **Needs Sending** – configuration applicable to the appliance has changed, however, you have not clicked the Send Configuration icon
- **Pending** – configuration applicable to the appliance has changed and you have clicked the Send Configuration icon, however, the appliance has not yet called in to receive the configuration
- **Delivered** – configuration has been delivered to the appliance.



Appliances

Move appliances into groups to manage and monitor appliances similarly.

□	Status	Host ID ▲	Hostname	IP Address	Firmware	Model	Group	Last Communication	Config Status	Executed
□	● Online	392cc3ab6e82	exinda-ab6e82	10.1.2.139	7.0.2.3073	Virtual	Branches	Sun Dec 14 17:57:17	Needs Sending	Sun Dec 14 17:57:32
□	● Online	3f65a43ca2e8	exinda-paris-bastille	172.24.32.3	7.0.1.2456	4061	Data Center	Sun Dec 14 17:59:57	● Pending	Sun Dec 14 18:01:12
□	● Online	533b847093b1	exinda-nice	172.49.4.2	7.0.1.2456	4061	Branches	Sun Dec 14 18:00:03	● Delivered	Sun Dec 14 18:00:03
□	● Online	5aabb5ab24b2	exinda-le-havre	10.25.32.9	6.4.5.3175	2061	Branches	Sun Dec 14 18:00:00	● Delivered	Sun Dec 14 18:00:00
□	● Online	681a7582cefb	exinda-dijon	172.69.4.5	6.4.5.3175	6060	Branches	Sun Dec 14 18:00:04	● Delivered	Sun Dec 14 18:00:03
□	● Online	821e21b7e1d5	exinda-marseille	172.75.7.5	6.4.5.3175	4061	Branches	Sun Dec 14 18:00:03	● Delivered	Sun Dec 14 18:00:03
□	● Online	8c2c7e0ade41	exinda-toulouse	10.32.3.1	7.0.1.2456	4061	Branches	Sun Dec 14 18:00:03	● Delivered	Sun Dec 14 18:00:02

Viewing Appliances in the Tenancy

There are several locations in the Exinda Management Center where you can see the list of appliances in your tenancy, each providing a different scope of which appliances are shown.

- Selecting **Not Deployed** shows only the appliances that have not been configured.

  Configuration cannot be applied to the appliances here. However, configuration can be imported into the library from appliances in the Unallocated Appliances list.
- Selecting **Configured Appliances > Appliances** shows the appliances that can be configured by the Exinda Management Center.

In order to apply configuration to an appliance, it must first be moved to the tenant's Configured Appliances group. Appliance groups can be added to the Configured Appliances group so that the appliances can be organized in a way that makes sense to you. Perhaps you want to organize by geography or by function (Data Center vs. Branches, or by circuit size). Groups can be nested. Configuration is applied by appliance groups, so all appliances in a group receive the same configuration.

- Selecting a nested group within **Configured Appliances > Appliances**, will show the subset of configured appliances that have been moved to that group (and any nested groups) in the configured appliance groups hierarchy.
- Selecting your **Overview > Appliances** will show all the appliances in your tenancy including the unallocated appliances.

Moving Appliances Within the Tenancy

If there is more than one tenant in the system

When appliances first appear in the system within an on-premises EMC deployment with more than one tenant, they are added to the Appliance Pool group. This location is intended for the host of a multi-tenant deployment of the Exinda Management Center. Since the appliance does not know to which tenant it belongs, it appears in the Appliance Pool. The host admin user then moves the appliance to the appropriate tenant.

> ***Best Practice:***
>
> ***It is recommended that you initially move appliances to the Not Deployed (Unallocated) Appliance group to let the admin user manage the appliances in the tenant.***

If there is only one tenant in the system

When appliances first appear in the system, they appear in the **Not Deployed** appliances group. From there they can be moved to the **Configured Appliances** group.

> **IMPORTANT**
>
> ***When appliances are moved out of the Configured Appliances group to the Unallocated Appliances group or the Appliance Pool, the configuration that was applied via the edit forms will be automatically removed from the appliances upon the next call into the Exinda Management Center.***

To move an appliance

1. Select the node in the Tenant tree that contains the appliance you need to move. For instance, it

could be in the:

- **Appliance Pool** groups (on-premises EMC deployments only)
- **Not Deployed Appliances** in the tenant
- **Configured Appliances** group (or one of its nested groups) in the tenant

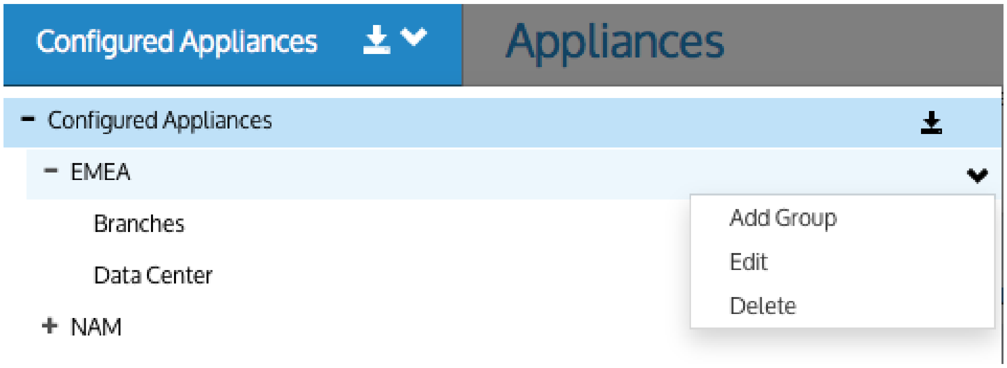
2. The system shows the list of appliances.

> **TIP**
>
> ***To look at the appliances in the Configured Appliances group (or one of its nested groups), you need to select the Appliances menu item.***

3. Select the checkbox next to the desired appliance(s).
4. Click **Move Appliances**.
5. Select the destination for the appliance(s).
6. Click the **Move Appliances** button.

To create a new appliance group

1. Click the appliance group header menu and click the menu icon of the group to which you want to add a group.

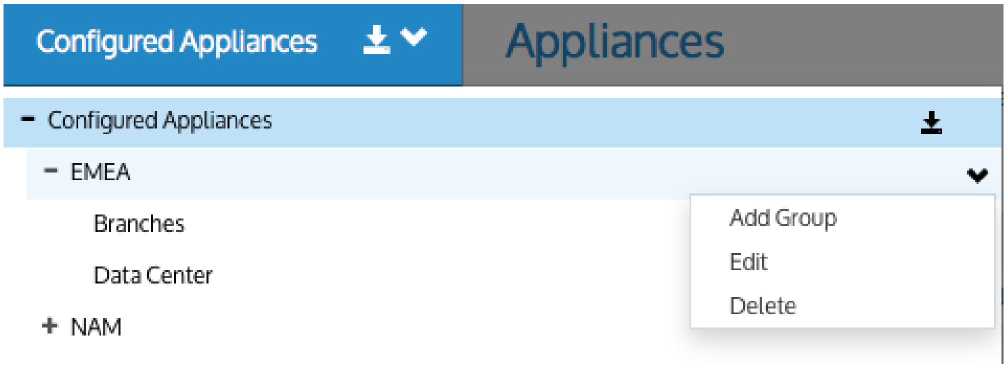


2. Click the menu icon of the group where you want to add a group.
3. Select the **Add Group** menu item.
   A new group is added, with the Edit mode enabled.
4. Type the name of the group and press **Enter** to commit the name.

To edit an appliance group name

1. Click the appliance group header menu and click the menu icon of the group that you want to rename.

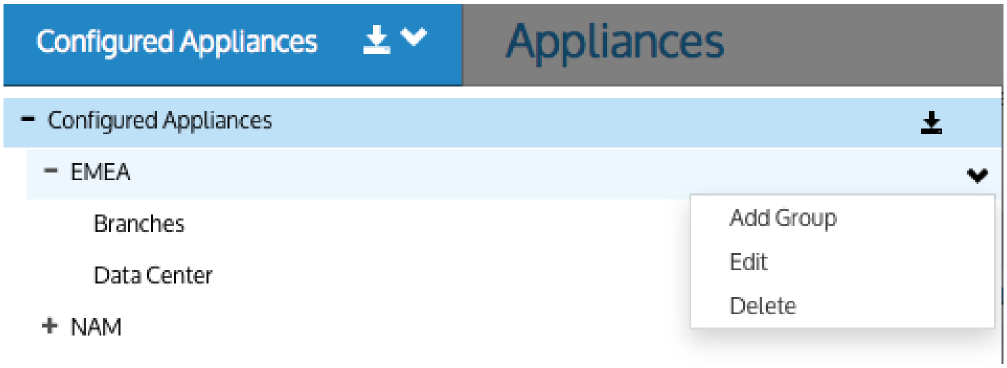
© 2016 Exinda Networks Inc.



2. Select the **Edit** menu item.
3. Type the name of the group to create the group.

To delete an appliance group

1. Click the appliance group header menu and click the menu icon of the group that you want to delete.



2. Select the **Delete** menu item.

> **NOTE**
> - *If there are appliances in the group or its sub-groups, then the group cannot be deleted.*
> - *If there is configuration on the group, but no appliances, it can be deleted.*

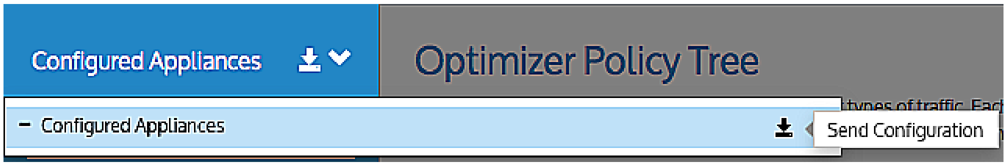
3. Confirm that you want delete the group.

Sending Configuration to the Appliances

Changes that you make in the Exinda Management Center are not sent to the appliances until you choose to send them. To do so, click the Send Configuration icon ⤓ next to the appliance group.

This sends the configuration to all the appliances in the group and any nested appliance groups the next time that each appliance calls into the system.

In the Configured Appliances section, click the named appliance group menu at the top of the blue menu, and then click the Send Configuration icon. When sending the configuration, you have the option to restart the optimizer on the appliances or save the configuration on the appliances. The next time the appliances call in, they receive the configuration, restart the optimizer, and save configuration as instructed.



Chapter 5: Introduction to Working with the Configuration Library Items

This chapter deals with the items that are configured in the Configuration Library. The Library contains all of the configurable items that you define in the EMC. Once defined, these items are available for reuse elsewhere in the configuration. See the following topics for more information:

© 2016 Exinda Networks Inc.

Using the Configuration Library

The Configuration Library allows to you create items and save them for reuse in different areas, much like a template. For instance, create a policy set once and then use it in multiple virtual circuits or in multiple Optimizer Policy Trees applied to different appliance groups.

The library items will appear in drop-down lists when configuring other items. For example, when creating a policy, you can select an application from a list; when creating a Optimizer Policy Tree, you can select a circuit from a list, or a virtual circuit from a list, or a policy set from a list, and so on.

Library items are categorized as follows:

- Circuits – Identifies the physical connections to the WAN or Internet by defining the inbound and outbound bandwidth and the named circuit type. The circuits within a tenant must have unique names.
- Circuit Types – An abstract concept used to identify the purpose of the circuit and appliance bridges and to create a logical binding between the circuits and the appliance bridges.
- Virtual Circuits – Logically divide or partition a circuit to define what traffic will be processed in this partition (and when), and how much bandwidth it is allowed.
- "Dynamic Virtual Circuits" on page 78 – Dynamic virtual circuits provide a means to configure fair sharing among the hosts, or to configure a limit to the number of hosts so that those hosts get preferential treatment.
- Policy Sets – Ordered list of policies that can be applied to one or more virtual circuits in one or more appliance groups.
- Policies – Define the actions to perform on specific targeted traffic.
- Network Objects – Represent hosts on a network and can include subnets, single hosts, or groups of both. Once on the appliance, network objects are used to determine if host and user traffic data are internal or external to the LAN behind your appliance.
- Applications – Classify traffic by layer 7 signatures OR by a combination of network objects, ports, protocols, and DSCP markings. You can then filter traffic generated by the applications to determine which policy to apply.
- Application Group – Preset and custom groups of applications to monitor and subsequently classify traffic and determine which policy to apply to traffic.
- Schedules – Define a specific timeframe of the week. When used in policies or virtual circuits, the schedule will affect traffic only within the identified timeframe.
- Application Performance Scores – Identify the applications operating on your network whose performance you need to monitor.
- Service Level Agreements – The Service Level Agreement (SLA) objects are used to monitor the availability of a particular IP site.

- VLANs – Virtual LAN (VLAN) Objects are used to logically separate hosts (or groups of hosts) on a functional basis rather than on a physical basis

Circuit Types

Circuit Types are used to identify the purpose of the circuit and the appliance bridges. When the purpose of the circuit and an appliance bridge align, then the circuit is bound to that bridge in the configuration that is sent to the appliances. Note that Circuit Types do not exist on appliances. Circuit Types abstract the binding between the circuits and the appliance bridges. Therefore, the appliances can be treated similarly even when they do not have the same number of bridges and when they are not connected in the same way.

Circuit Types are defined in the Configuration Library and are used by circuits and appliance bridge-to-circuit type mappings.

EXAMPLE

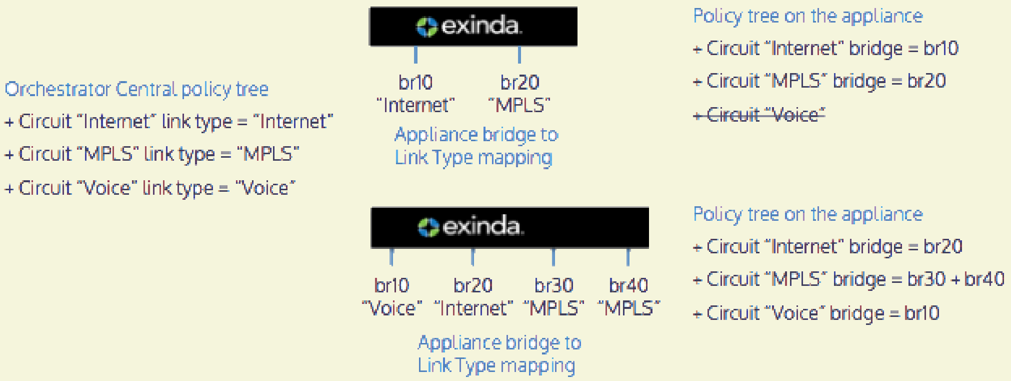
Consider a Policy Tree in the EMC with three circuits: one for each of "Internet", "MPLS", and "Voice".

Consider two different appliances with different numbers of bridges, and where they are cabled differently.

The first appliance has two bridges, br10 and br20, where br10 is mapped to "Internet" and br20 is mapped to the "MPLS".

A second appliance has four bridges, br10, br20, br30, and br40, where br10 is mapped to "Voice", br20 is mapped to "Internet", and br30 and br40 are mapped to "MPLS".

The Policy Tree rooted at a given circuit is sent to the appliances that share the same Circuit Type as the circuit. That is, the Policy Tree sent to the first appliance only has two circuits - circuit "Internet" bound to br10 and circuit "MPLS" bound to br20, whereas all three circuits are sent to the second appliance; circuit "Internet" bound to br20, circuit "MPLS" bound to br30 and br40, and circuit "Voice" bound to br10.


Orchestrator Central policy tree
+ Circuit "Internet" link type = "Internet"
+ Circuit "MPLS" link type = "MPLS"
+ Circuit "Voice" link type = "Voice"
exinda
br10
"Internet"
br20
"MPLS"
Appliance bridge to Link Type mapping
Policy tree on the appliance
+ Circuit "Internet" bridge = br10
+ Circuit "MPLS" bridge = br20
~~+ Circuit "Voice"~~
exinda
br10
"Voice"
br20
"Internet"
br30
"MPLS"
br40
"MPLS"
Appliance bridge to Link Type mapping
Policy tree on the appliance
+ Circuit "Internet" bridge = br20
+ Circuit "MPLS" bridge = br30 + br40
+ Circuit "Voice" bridge = br10

Where do I define the Circuit Types?

Circuit Type library items can be found in **Library > Circuit Types**.

To assign the Circuit Type to a circuit

See Circuits.

To assign Circuit Types to appliance bridges

See Appliance Bridge to Circuit Type Mappings.

Circuits

Circuits define physical connections to the WAN or Internet. A circuit defines the inbound and outbound bandwidth and the named circuit type. On an appliance, a circuit specifies the named bridge (or bridges) to which it is bound . In the Exinda Management Center, the binding to bridges is through a named Circuit Type. Circuit Types represent the intended use of a circuit. This allows you to configure a circuit for multiple appliances without requiring the bridges on the appliances to have the same name, such as br10. This is favorable where the number of bridges or names of bridges or the cabling of the bridges is not consistent across the appliances.

If multiple bridges on an appliance are mapped to the same Circuit Type, then all those bridges will be bound to the single circuit in the Policy Tree that is configured with that Circuit Type. To learn how Circuit Types are used to determine which circuits are sent to the appliances, read Circuit Types.

Circuits can be created in the Configuration Library directly and then later assigned to an Optimizer Policy Tree, Circuits can also be created in an Optimizer Policy Tree, from where the configuration is saved to the Configuration Library so that it can be used elsewhere. The circuits within a tenant must have unique names. When a circuit is modified, all uses of it are modified.

Circuits are part of the Optimizer Policy Tree. To learn how circuits, Virtual Circuits, policy sets, and policy rules work together, see Policy Tree.

Where do I find circuits?

Circuit library items can be found in **Library > Circuits**. The circuits that are applied to and are sent to appliances are found in the policy trees for each appliance group. Go to the **<desired appliance group> > Optimizer Policy Tree**.

To create a circuit in the Configuration Library

1. Click **Create new circuit**
2. In the **Name** section, type the name of the circuit.
   The name must be unique in the tenant.
3. In the **Bandwidth** section, type the **Inbound Bandwidth** and the **Outbound Bandwidth**.
   The bandwidths can be specified in kbps, Mbps, or Gbps.
4. In the **Bind to Circuit Type** section, select the **Circuit Type**.

© 2016 Exinda Networks Inc.

> **NOTE**
>
> *The circuit type represents the purpose of the circuit; it is a user created object. If the desired circuit type does not exist, you can click Create new circuit type in the library to create it. Learn more about Circuit Types.*

5. Click the **Create and Add** button.
   The circuit appears in the library list.

To create a new circuit directly in the Policy Tree

1. In a Policy Tree, click **Create new circuit**.
2. Similar to creating a circuit in the configuration library, specify the name, inbound and outbound bandwidth, and select the circuit type.
3. Click **Save**.
   The circuit is added to the Policy Tree and is also saved to the configuration library.

To add a circuit to a Policy Tree

1. In the Policy Tree, click **Add circuit from library**.
2. Select the desired circuit from the drop-down list.

Virtual Circuits

Virtual Circuits are created within Circuits and are used to logically divide or partition the circuit. The virtual circuit defines what traffic is processed in this partition, how much bandwidth it is allowed, and whether to enforce fair sharing among the network hosts. Traffic is evaluated against the definition of the virtual circuit. Traffic that does not fall within the virtual circuit is evaluated by the next virtual circuit and so on.

You have the option of creating a virtual circuit within the Configuration Library first, and then later assigning it to a circuit in the Optimizer Policy Tree, or you can create the virtual circuit directly within the Optimizer Policy Tree, which also saves it as a Library item . The virtual circuits within a tenant must have unique names. When a virtual circuit is modified, all instances of its use are modified.

To learn how circuits, virtual circuits, policy sets, and policy rules work together, see Policy Tree.

Where do I find Virtual Circuits?

Virtual Circuit library items can be found in **Library > Virtual Circuits**. The virtual circuits that will be sent to appliances are found in the policy trees for each appliance group. Go to the **<desired appliance group> > Optimizer Policy Tree**.

To create a Virtual Circuit in the Configuration Library

1. Click **Create new virtual circuit**

2. In the **Name** section, type a name for the virtual circuit.
   The name must be unique within the tenant.

> **NOTE**
>
> *If you want, you can leave the EMC to define a name for you, It does this based on the configuration of the virtual circuit.*

3. In the **Filter** section, select the combination of filters to apply to the virtual circuit.

> **NOTE**
>
> *The virtual circuit can partition the circuit by filtering the traffic based on these filters. You can apply any combination of these filters. Defined network object library items appear in the Network Object list, and you can also choose filters from the pre-defined application groups.*

   Optionally, type a value to limit the number of connections at one time on this virtual circuit.
4. In the **Bandwidth** section,type the desired bandwidth for this virtual circuit.
5. Also specify how to share bandwidth with other virtual circuits when there is insufficient bandwidth due to over subscription..
6. In the **Dynamic Virtual Circuit** section, set the options that provide the control you need.

> **TIP**
>
> *See "Dynamic Virtual Circuits" on page 78 for more information about configuring dynamic virtual circuits.*

7. In the **Schedule** section, set the time values for when the virtual circuit will be enforced.

> **NOTE**
>
> *Options in the list are determined by the library Schedules category*

8. Click the **Create** button.
   The virtual circuit is added to the Virtual Circuits Library category.

To create a new Virtual Circuit directly in the Optimizer Policy Tree

1. On the Optimizer Policy Tree, select an existing Circuit and click **Create new virtual circuit**.
2. Similar to creating a virtual circuit in the configuration library, specify the name,filters, bandwidth, and the schedule.

3. Click the **Create and Add** button.
   The virtual circuit is added to the Circuit within the Optimizer Policy Tree and is also saved to the Configuration Library.

To add a Virtual Circuit from the Library to a Policy Tree

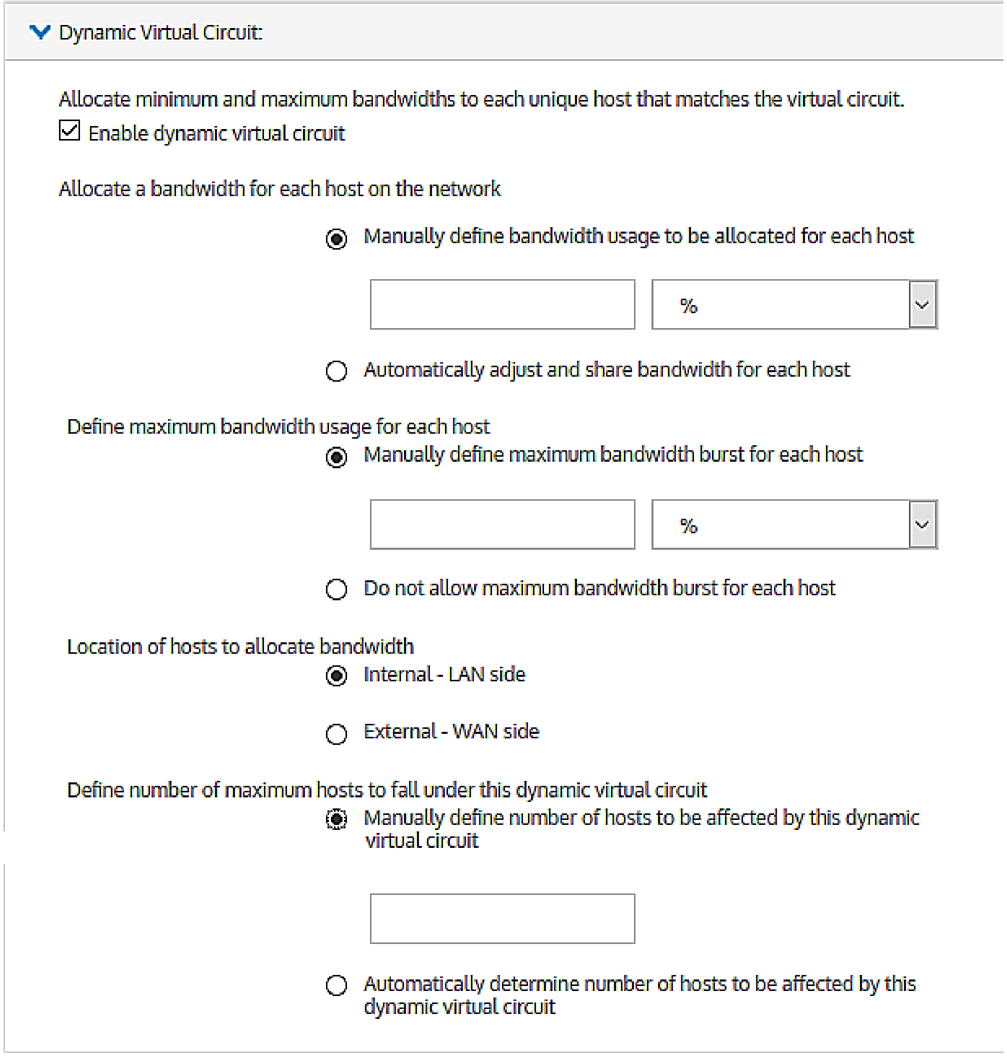
1. In the Optimizer Policy Tree, click **Add Virtual Circuit from library**.
2. Select the desired virtual circuit from the drop-down list.

Dynamic Virtual Circuits

You can use Dynamic Virtual Circuits to enforce fair sharing of bandwidth among the hosts, or to limit the number of hosts on the circuit to ensure that those hosts get preferential treatment.

- For fair sharing, you must specify how you would like the bandwidth in the virtual circuit to be shared among the hosts. You can fix the per host bandwidth and have the system calculate the number of allowed hosts. Note that if there are less than the allowed hosts, each active host can burst to gain more bandwidth (if you have configured the virtual circuit to allow bursting).
- For limiting the number of hosts, you can have the system calculate the amount of bandwidth that is then allowed to each host. You can specify an automatic calculation of the per host bandwidth and the number of allowed hosts. The system then divides the virtual circuit bandwidth by the number of active hosts.

The options available in the Exinda Management Center appear in the following screenshot:



Dynamic Virtual Circuit:

Allocate minimum and maximum bandwidths to each unique host that matches the virtual circuit.

☑ Enable dynamic virtual circuit

Allocate a bandwidth for each host on the network

● Manually define bandwidth usage to be allocated for each host

[ ] [% ▾]

○ Automatically adjust and share bandwidth for each host

Define maximum bandwidth usage for each host

● Manually define maximum bandwidth burst for each host

[ ] [% ▾]

○ Do not allow maximum bandwidth burst for each host

Location of hosts to allocate bandwidth

● Internal - LAN side

○ External - WAN side

Define number of maximum hosts to fall under this dynamic virtual circuit

● Manually define number of hosts to be affected by this dynamic virtual circuit

[ ]

○ Automatically determine number of hosts to be affected by this dynamic virtual circuit

Consider the following:

- Allocating bandwidth usage to each host on the network
  - By manually defining the bandwidth usage for each host, you are limiting the number of hosts that can be accommodated on the dynamic virtual circuit. You can do this by either defining an actual bandwidth or by defining a percentage of the available bandwidth. By default, though, the EMC can set no less than 10 kbps for any one host, so a hard limit to the maximum number of hosts is the total available bandwidth divided by 10 kbps. This setting allows you set higher bandwidth quotas for a limited number of hosts.
  - By allowing the EMC to automatically adjust and share bandwidth, you are letting as many hosts as can be accommodated within the available bandwidth on the dynamic virtual circuit. The minimum bandwidth that the EMC can provide is 10 kbps, the hard limit to the number of hosts is the total bandwidth divided by 10 kbps.

- Defining a maximum bandwidth usage for each host. When spare capacity exists on the dynamic virtual circuit because few hosts are active, you can allow the active hosts have greater bandwidth (to burst). You can set the burst rate limit as an actual bandwidth measure (kbps, Mbps, etc.) or specify a percentage of the available bandwidth. You can also disallow bursting.
- Specifying the location of the hosts: internal or external. This setting allows you specify whether the hosts on the dynamic virtual circuit located within the LAN or outside the LAN..
- Defining the maximum number of hosts. You can manually define the maximum number of hosts that can be accommodated on the dynamic virtual circuit, or you can let the EMC control how many hosts are allowed on the circuit.

Policy Sets

Policy sets are an ordered list of policies that can be applied to one or more virtual circuits in one or more appliance groups.

Policy sets can be created in the Policy Set Library directly and then later assigned to an Optimizer Policy Tree, or they can be created in an Optimizer Policy Tree. When saved in an Optimizer Policy Tree, they are also saved to the Configuration Library for use elsewhere. The policy sets within a tenant must have unique names. When a policy set is modified, all uses of it are modified.

There are a few default policy sets that you can use or modify. They correspond to the configuration defined when the wizard is run on the appliance. The different policy sets are due to varying answers to the wizard questions.

To learn how Circuits, Virtual Circuits, Policy Sets, and Policy Rules work together, see Policy Tree.

Where do I find policy sets?

Policy set library items can be found in **Library > Policy Sets**. The policy sets that will be sent to appliances are found in the policy trees for each appliance group. Go to the desired appliance group in the **Optimizer Policy Tree**.

To create a policy set in the Library

1. Click **Create new policy set**
2. In the **Name** section, type a name for the policy.
   The name must be unique within the tenant.
3. In the **Policies** section, add policies to the list.
   - You can select a policy from the library by clicking **Add policy from library**.
   - You can create a new policy by clicking **Create new policy**.

   Policies created in the policy set are added to the policy library.

   Learn more about how to create a policy.
4. To reorder the policies, drag and drop the policy rule to the desired location.

5. Click **Create and Add**.
   The policy set is added to the library list.

To create a new policy set directly in the Optimizer Policy Tree

1. In a Policy Tree, under the desired virtual circuit, click **Create new policy set**.
2. Similar to creating a policy set in the Configuration Library, specify a name and then add the policy rules to the list of policies.
3. Click **Save**.
   The policy set is added to the Optimizer Policy tree for the current appliance group and is also saved to the Configuration Library.

To add a policy set from the library to a Policy Tree

1. In the Policy Tree, under the desired virtual circuit, click **Add policy set from library**.
2. Select the desired policy set from the drop-down list.

Policy Library

Policies define what actions to perform on specific traffic. The policies can specify whether to optimize the traffic (by bandwidth shaping, acceleration, or packet marking), block the traffic (by discarding the packets), or monitor the traffic (by ignoring the packets).The traffic that the policy affects can be filtered by:

- Application or application group
- Hosts or subnets
- Hosts or subnets that are communicating with other specific hosts or subnets
- VLAN
- ToS/DSCP markings
- Time of day

Any combination of these filters can be applied. For example, the policy could target SAP traffic between a particular branch and headquarters that has particular ToS markings on a particular VLAN during work hours. Furthermore, you can add more than one filter. That is, the policy could target a particular branch site for Netflix and the same branch site for Silverlight.

Version Info:

Exinda Management Center 1.5.0 does not support policies for HTTP Redirect or HTTP Response.

When you create policies, they are added to the Policies Library. If you amend a policy definition, any changes made to it affect all Virtual Circuits that use that policy. To learn how circuits, Virtual Circuits, policy sets, and policy rules work together, see Policy Tree.

Where do I find policy rules?

Policy library items can be found in **Library > Policies**.

The policies that will be sent to appliances are found in the policy trees for each appliance group. Go to the desired appliance group's **> Optimizer Policy Tree**.

To create a policy in the Configuration Library

1. Click **Create new policy in the library** on the Policy Library page.
2. In the **Name** section, type a name for the policy.
   The name must be unique within the tenant.
3. In the **Action** section, specify what type of action the rule should take. Select *one* of the following:
   - **Optimize** – Selecting optimize causes a new action to appear in the UI where you can specify whether you want to apply bandwidth shaping, prioritization, acceleration, or packet marking.
   - **Discard** – Select discard to specify that you want to block a particular type of application by discarding the packets.
   - **Ignore** – Select ignore to specify that you want to allow packets to pass through without manipulation, that is, traffic monitoring only .
4. In the **Filter** section, specify the type of traffic to which you want to apply the policy.

   Set any of the following traffic attributes.
   - **Application** – Select traffic based on a predefined application or application group from the list. Custom applications that you have created in the library will appear in this drop-down list.
   - **Source/Direction/Destination** – Select traffic based on one end of a conversation belonging to a predefined network object or select traffic based on one way or two way conversations between two predefined network objects. For the source, select a network object that filters for the initiation of a conversation. For the destination, select a network object that filters for the destination of the conversation. If hosts are not specified, ALL network objects are assumed. Traffic direction is relative to the Exinda appliance.
   - **ToS/DSCP** – Select traffic based on particular ToS/DSCP markings in the IP header.
5. Click the **Create** button.
   The policy set will be added to the library list.

To create a new policy set directly in the Optimizer Policy Tree

1. In a Policy Tree, under the desired virtual circuit, click **Create new policy set**.
2. Similar to creating a policy set in the configuration library, specify the name, and add policy rules to the list of policies.

3. Click the **Save** button.
   The policy set is added to the Policy Tree and is also saved to the configuration library.

To add a policy set from the library to a Policy Tree

1. In the Policy Tree, under the desired virtual circuit, click **Add policy set from library**.
2. Select the desired policy set from the drop-down list.

This section of the manual deals with defining and applying the network objects used to manage aspects of your network. See the following topics for more information:

Network Objects

Network objects represent hosts on a network and can include subnets, single hosts, or groups of both. Once defined, a network object may be assigned to multiple appliance groups and is used on the Exinda appliances for monitoring. They can also be used to define other objects, such as policy rules and virtual circuits, to determine which policy actions to apply and to which subnets of the network. Once on the appliance, network objects are used to determine if host and user traffic data are internal or external to the LAN behind your appliance.

A network object can be created in the Library for later use in other components and appliance groups, or it can be created directly in the Optimizer Policy Tree, which also saves it to the Library. You can also import network objects into the Library from an appliance.

The location of a network object, that is, whether it is considered internal or external to the LAN behind the appliance, is determined by comparing it to the local network object assigned to an appliance. Learn more about local network objects.

Where do I find network objects?

Network Object library items can be found in **Library > Network Objects**.

To create a network object in the library

1. Click **Create network object in the library**.
2. In the **Name** section, type the name of the object.
   The name must be unique in the tenant.
3. In the **Subnets** section, type the **IP address** and the **Mask Length**.
4. Click **Add Another Subnet**to add another network subset.
5. Click the **Create** button.
   The network object is added to the library list.

NOTE

If the combination of IP address and mask length is incorrect, the system suggests a possible fix. Either change the information, or click the Create button to use the suggestion.

To import a network object into the library

If you have existing appliances that are already configured with network objects, you can import the network objects into the library in the Exinda Management Center from the Not Deployed list. Refer to Importing Network Objects for instructions.

To add a network object from the library to an appliance group

1. Click **Configured Appliances**, and then select the Appliance group to which you want to apply the network object.
2. Click **Network Objects**.
3. Click **Add Network Object from Library**.
4. Select one or more network objects to apply to the current appliance group, and then click **Add Network Object to <group_name>**.

To create a network object in an appliance group

1. Click **Configured Appliances**, and then select the Appliance group for which you want to create a new network object.
2. Click **Network Objects**.
3. Click **Create network object...**.
4. In the **Name** section, type the name of the object.
   The name must be unique in the tenant.
5. In the **Reporting** section, decide if you want to include the monitor information for this network object in the subnet reports. If you deselect the **Include in subnet reporting** option, the subnet information is not represented on the SDP server.
6. In the **Subnets** section, type the **IP address** and the **Mask Length**.
7. Click **Add Another Subnet**to add another network subset if necessary.
8. Click **Create**.
   The network object is added to the configuration for this appliance group, and it is also added to the Network Objects Library.

To use a network object in a policy rule definition

You can apply a network object filter to a policy to filter by subnet (communicating with other specific hosts or subnets). Use the instructions above to create the Network Object in the library, and then refer to Policy Library for further instructions. The Network Objects saved as Library items appear in the **Filter** section, under the **Source** list.

To use a network object in a virtual circuit definition

When defining virtual circuits to partition a circuit, you can apply Network Object library items to filter the traffic by subnet. Use the instructions above to create the Network Object in the library, and then refer to Virtual Circuits for further instructions.

To use a network object in an Application

When defining applications to classify traffic, you can apply Network Object library items to classify traffic based on a combination of Network Object, TCP Port, UDP Port, DSCP, and Protocols. Use the instructions above to create the Network Object in the library, and then refer to Applications for further instructions.

Local Network Objects

Local network objects define which part of the network is considered as the local area network relative to an appliance. When defining network objects in the Exinda Management Center, the local network object is used to determine if the network object is internal or external for a given appliance.

For reporting purposes, hosts and users are defined as internal or external by comparing the IP address with the network objects, and using the location of the network object.

> **EXAMPLE**
>
> Consider three sites, Chicago, Boston, and Dallas, where each site has an appliance and each appliance has a local network object. Do the following:
>
> - Create network objects to represent the Chicago site, the Boston site, and the Dallas site.
> - On the Chicago appliance, when compared to the appliance's local network object, the Chicago network object will be set to be internal, and the Boston and Dallas network objects will be external.
> - On the Boston appliance, the Boston network object will be set to be internal, and the Chicago and Dallas network objects will be external.

Where do I find local network objects?

Select your **Configured Appliances** groups (or any custom group under it), then click **Local Network Objects**

To edit a local network object

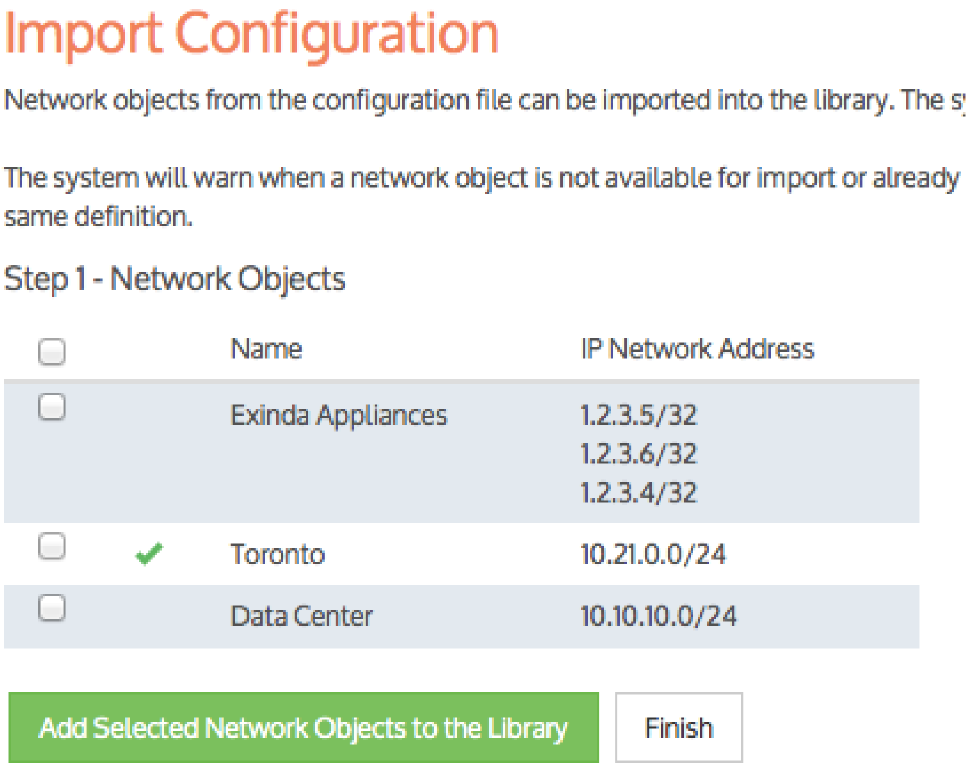
1. There is a local network object for each appliance in the group.
2. For the appliance, click the **Host ID**.
   The Local Network Objects form appears.
3. Type one or more **IP Network Addresses** and the **Mask Length**.
4. Click the **Save** button.

Importing Network Objects

If you have existing appliances that are already configured with network objects, you can import these network objects into the library (one at a time) from the Not Deployed list in the Exinda Management Center. When importing network objects, the importer indicates if the network object already exists in the library (or is included in another network object), or if it conflicts with another network object in the library. By importing your network objects, you can more quickly start building a library of objects to use. The system lets you know if the imported network object is already in the library or if the imported network object definition is a subset of a network object in the library. This allows you to quickly ensure consistency across multiple appliances.

To import network objects

1. From the **Not Deployed** appliance list in your tenant, select the checkbox for the appliance from which you want to import the network objects.
2. Click **Import Configuration**.



Import Configuration

Network objects from the configuration file can be imported into the library. The s

The system will warn when a network object is not available for import or already same definition.

Step 1 - Network Objects

☐		Name	IP Network Address
☐		Exinda Appliances	1.2.3.5/32 1.2.3.6/32 1.2.3.4/32
☐	✓	Toronto	10.21.0.0/24
☐		Data Center	10.10.10.0/24

3. Click **Import Network Objects**.
   A list of network objects, with their IP addresses, appears.

   If a network object has the same name as a network object in the library, the following indicate the status:

- ✓ – if the IP addresses are the same, the name has a green check mark before it.
- ⊆ – if all of the object IP addresses are contained within the one in the library, the name has a green subset symbol before it.
- ⚠ – if the imported network object has an IP address that is not in the network object with the same name in the library, the name has a warning icon before it.
  *You will need to resolve this conflict manually by modifying the network object in the **Library**.*

4. Select the network objects that you would like to import.
5. Click the **Add Selected Network Objects to the Library** button.
   The network objects are imported into the library. Note that neither the location (internal or external) of the network object, nor the reporting flag are imported.

Applications

Applications are used to monitor traffic or to identify which policy to apply to the traffic. Applications classify traffic by either layer 7 signatures OR a defined combination of network objects, ports, protocols, and DSCP markings.

The Exinda Management Center provides a comprehensive set of built-in Applications for you to use, These cannot be edited, but you can define Custom Applications.

If you want to send a custom application to the appliance for monitoring purposes (not for policy creation), there is not yet a way to send the application to the appliances for the sole purpose of monitoring. This feature will come soon. In the meantime, you can add the custom application as part of an ignore policy at the bottom of the optimizer tree that is sent to the appliances.

Note that if you use a custom application in the definition of a virtual circuit or policy for a given appliance group, then the custom application is automatically added to the appliance-group configuration

Applications can be defined in the Application Library directly, and then later assigned to an Optimizer Policy Tree. Applications can also be created in an Optimizer Policy Tree, in which case they are also saved to the Configuration Library for use elsewhere. All applications within a tenant must have unique names. When an application is modified, all uses of it are also modified.

Where do I find Applications?

Application library items can be found in **Library > Applications**. You can define custom applications for each appliance group. Go to the desired appliance group in the **Optimizer Policy Tree**.

How do I view built-in Applications?

Built-in application library items can be found in **Library > Applications > Built-in**. You can view built-in applications, but not edit.

To create a Custom Application in the Library

1. Click **Create new application in the library**.
2. In the **Name** section, type the name of the application.
   The name must be unique in the tenant.
3. In the **Definition** section, choose either the Layer 7 Signature, or select a combination of Network Object, Ports, DSCP and Protocols.
4. Click the **Create** button.
   The custom application will be added to the library list.

To create a new Application directly in the Optimizer Policy Tree

1. Click **Configured Appliances**, and then select the Appliance Group for which you want to create a new custom Application.
2. Click **Applications**.
3. Similar to creating a custom application in the Configuration Library, specify the name and then define the L7 Signatures OR set the other fields.
4. Click the **Create** button.
   The custom Application is added to the Optimizer Policy tree for this current Appliance Group and is also saved to the Library.

To add an Application from the library to an appliance group

1. Click **Configured Appliances**, and then select the appliance group to which you want to apply the network object.
2. Click **Applications**.
3. Click **Add Application from Library**.
4. Select one or more applications to apply to the current appliance group, and then click **application to <group_name>**.

To use a Custom Application in a policy rule definition

When creating a policy rule, you can use an custom Application to filter traffic to or from this application. The custom Applications appear in the Application list within the **Filter** section. Refer to Policy Rule for details.

Application Groups

Application groups are used to group together applications into a logical group. The application groups can be used to monitor the traffic or to create policy based on a category. For example, an application group named "Exinda" includes all applications related to Exinda monitoring or management, and all Exinda applications can be included as a single entity when creating policy.

The Exinda Management Center provides a comprehensive set of built-in Application Groups for you to use, but you can also define Custom Application Groups.

Although an application can be a member of multiple application groups, to prevent conflict it can only be a member of the application group that is currently monitoring traffic. For example, Skype cannot be added to both the Voice group and the Messaging group because EMC can gather data from only one monitored application group for reporting.

When an Application Group is created in the library, it is applied tenant-wide and is therefore available in every appliance group within an Appliance Group section. If an application group is set for monitoring and/or being used in the optimizer tree, then this application group is pushed to the respective appliances within the push configuration.

If a custom application is added to an application group, where the group does not exist in the configuration of the appliances, the application is first added to the appliances and then the group is imported.

In addition, the following limitations should be noted:

- If one application within a group is not supported by an appliance, then that application definition will not be sent to that specific appliance.
- If you try to add an application to an appliance with a firmware version does not support the application, the EMC displays an error for the appliance and the application is not imported. However, the appliance does import the application group along with other settings.

Where do I find Application Groups?

Application Group library items can be found in **Library > Application Group**.

*A lock icon in the **Monitoring** column indicates that an Application Group is in use and cannot, therefore, be deleted.*

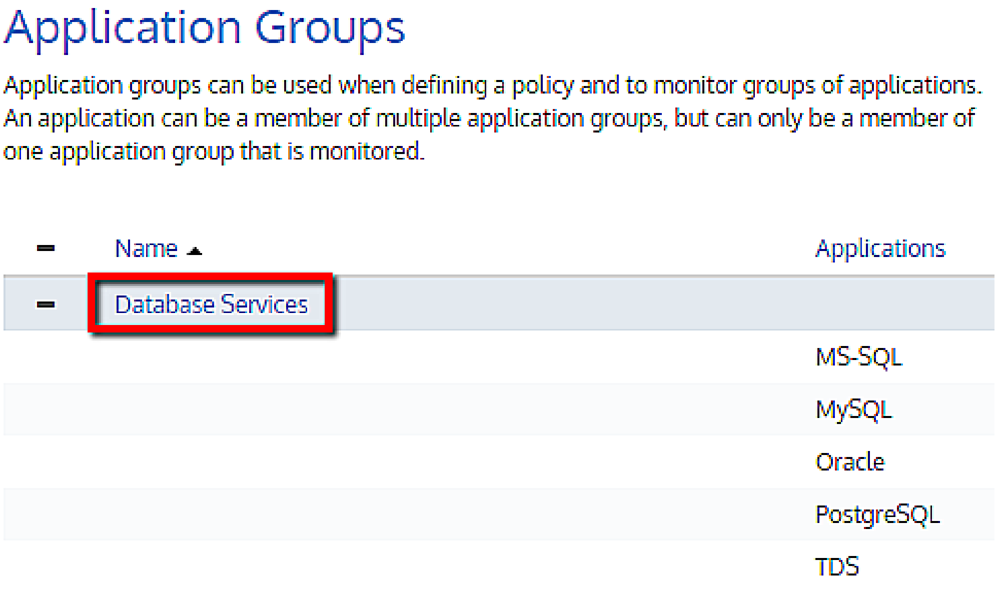
To use an Application Group in a policy rule definition

When creating a policy rule, you can use an Application Group to filter traffic to or from the applications within the group. The Application Groups appear in the Application list within the **Filter** section. Refer to "Policy Library" on page 81 for details.

How do I configure built-in Application Groups?

You can modify application groups either within the configured appliances or from the library.

1. Click the desired application group name to edit.

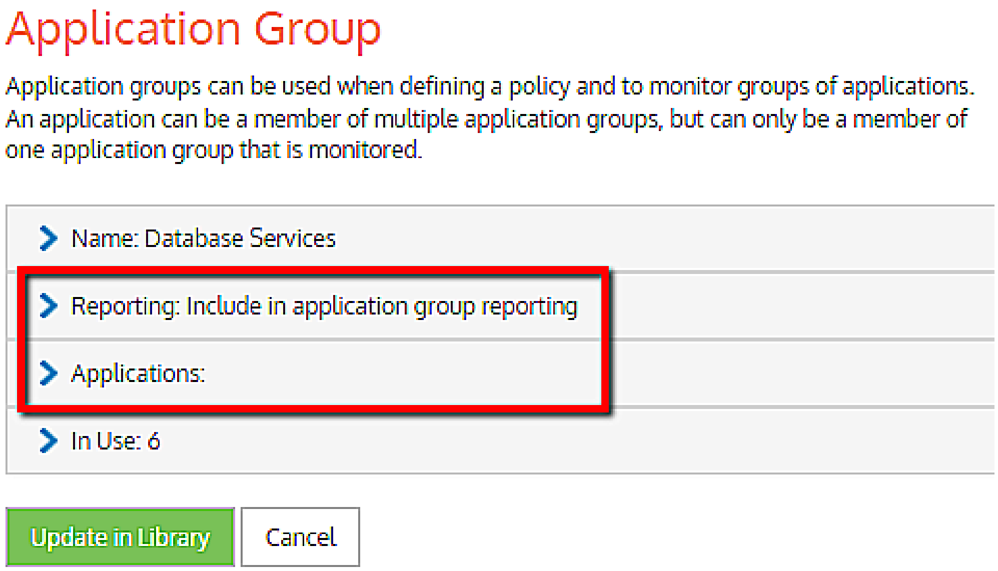


Application Groups

Application groups can be used when defining a policy and to monitor groups of applications. An application can be a member of multiple application groups, but can only be a member of one application group that is monitored.

	Name ▲	Applications
−	Database Services	
		MS-SQL
		MySQL
		Oracle
		PostgreSQL
		TDS

2. You can configure monitoring status and add or remove applications within this group.



Application Group

Application groups can be used when defining a policy and to monitor groups of applications. An application can be a member of multiple application groups, but can only be a member of one application group that is monitored.

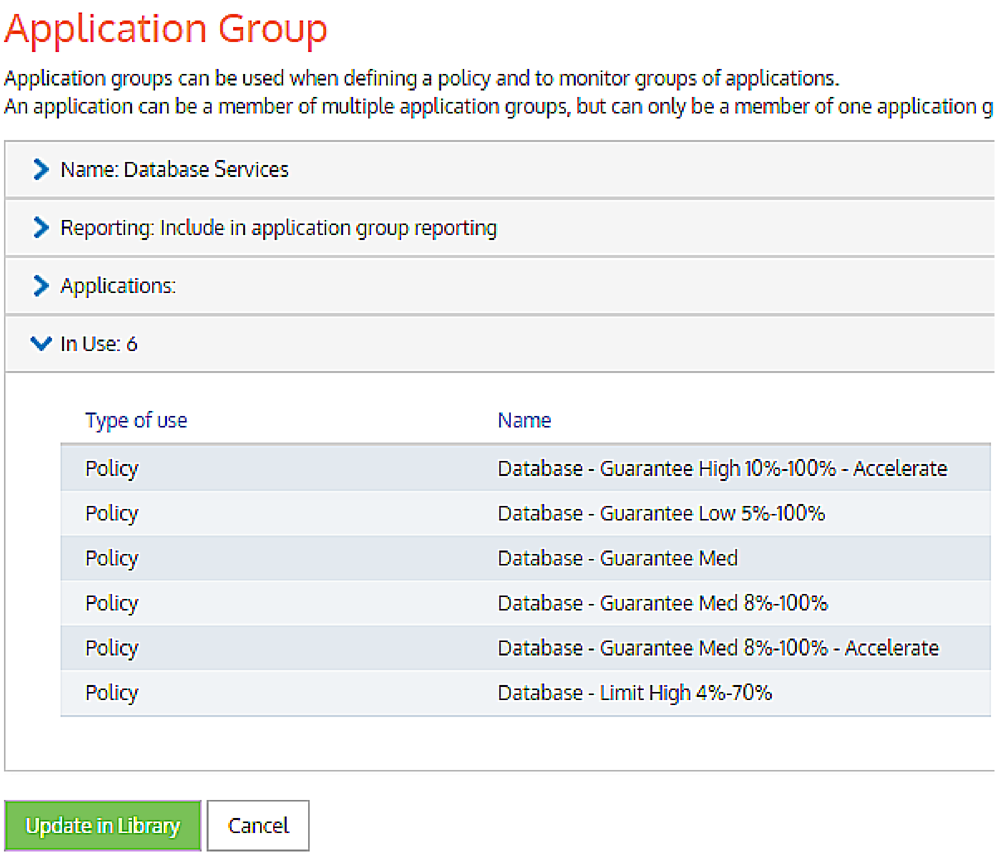
Name: Database Services

Reporting: Include in application group reporting

Applications:

In Use: 6

3. You could also view which policies are currently using this application group under **In Use**.



Application Group

Application groups can be used when defining a policy and to monitor groups of applications.
An application can be a member of multiple application groups, but can only be a member of one application g

Name: Database Services

Reporting: Include in application group reporting

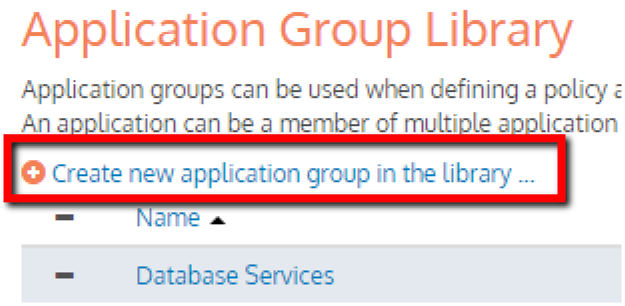
Applications:

In Use: 6

Type of use	Name
Policy	Database - Guarantee High 10%-100% - Accelerate
Policy	Database - Guarantee Low 5%-100%
Policy	Database - Guarantee Med
Policy	Database - Guarantee Med 8%-100%
Policy	Database - Guarantee Med 8%-100% - Accelerate
Policy	Database - Limit High 4%-70%

How do I create an custom application group?

1. Go to **Library > Application Groups** and click **Create new application group in the library...**



Application Group Library

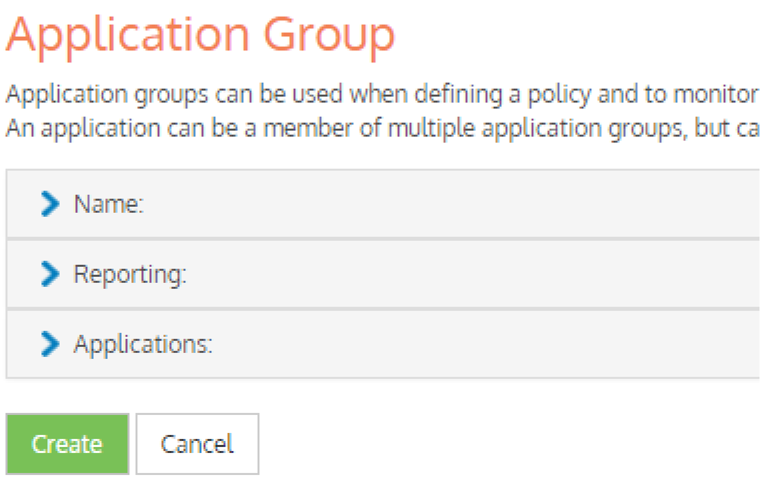
Application groups can be used when defining a policy a
An application can be a member of multiple application

Create new application group in the library ...

	Name ▲
—	Database Services

2. Provide a name, configure monitoring, if you want this group to be monitored, and add the applications to be part of this group.

© 2016 Exinda Networks Inc.

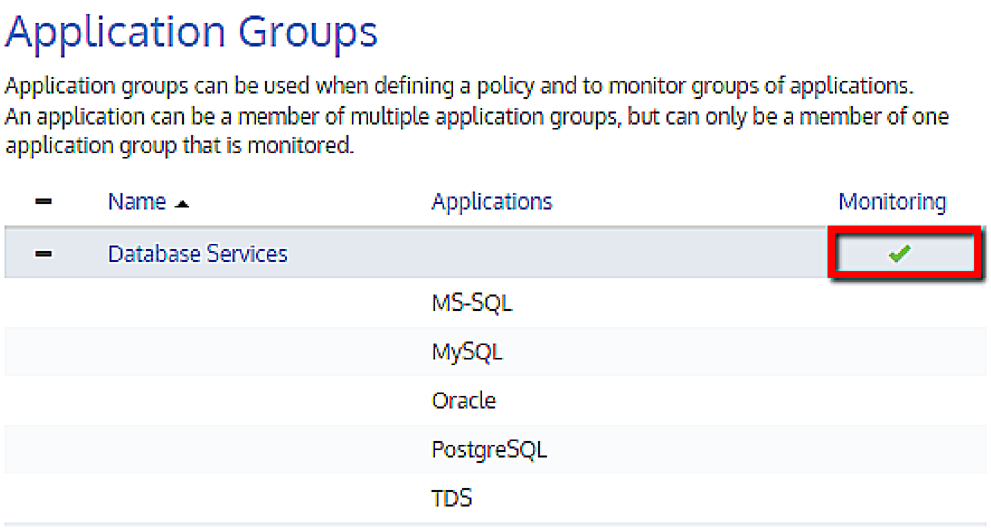


Application Group

Application groups can be used when defining a policy and to monitor
An application can be a member of multiple application groups, but ca

How do I know which application groups are enabled for monitoring?

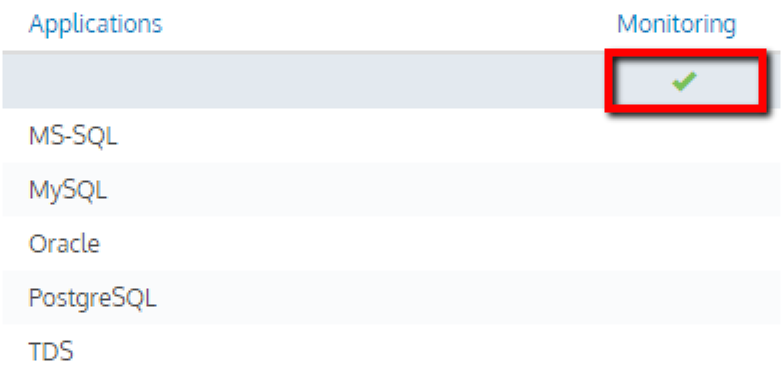
By default, all the built-in application groups are enabled for monitoring. On the main **Application Groups** page, you can view the specific groups that are set for monitoring.



Application Groups

Application groups can be used when defining a policy and to monitor groups of applications. An application can be a member of multiple application groups, but can only be a member of one application group that is monitored.

−	Name ▲	Applications	Monitoring
−	Database Services		✓
		MS-SQL	
		MySQL	
		Oracle	
		PostgreSQL	
		TDS	



Applications	Monitoring
	✓
MS-SQL	
MySQL	
Oracle	
PostgreSQL	
TDS	

You can always change the monitoring configuration by clicking on the application group name and changing it.

Schedules

Schedules define specific spans of time within a week, and are used to limit a policy or virtual circuit to a specific timeframe. For example, you might want to create a Schedule item that defines work hours for various locations. When creating policy, you can then use a Schedule to optimize particular traffic types during work hours.

Where do I find Schedules?

Schedule library items can be found in **Library > Schedules**.

The Schedule items can be applied to Policies and Virtual Circuits.

To create a Schedule in the Library

1. Click **Create new schedule in the library.**
2. In the **Name** section, type the name of the Schedule item.
   The name must be unique in the tenant.
3. In the **Times** section, select the days of the week and the Start and End times for this schedule.
2. To layer the time ranges, click **Add another time range**.
   For example, if you want to apply a schedule for Monday through to Friday from 9:00 to 17:00, but you need a different start and end time for weekends, you can add another range for Saturday and Sunday.
4. Click **Create**.
   The Schedule item is added to the Schedules Library category and is then available when defining Policies and Virtual Circuits.

Application Performance Scoring

Every organization has applications that are considered business-critical that need to be performing at their best at all times. Analyzing the performance of networked applications is a common task faced by network administrators. Often the root cause of poor performance by an application is not understood, and a common response is to undertake an expensive, often unnecessary upgrade of network capacity.

The Exinda appliance can monitor several properties of the TCP flows of an application and collect metrics. These metrics are compared to an established threshold and given a score between one and ten, known as the Application Performance Score (APS). The appliance can also monitor a single metric value within TCP flows for a specified application, known as Application Performance Metrics (APM).

This allows IT departments to use the Application Performance Score (APS) to determine what is performing well, and what is not. The APS and APM have thresholds that identify acceptable performance levels for the applications. When the metric values cross the configured threshold, notifications are sent alerting the necessary users so they can review the issue and make the necessary modifications to allow the applications to perform within the threshold level.

How the Application Performance Score is Calculated

The application performance score (APS) assesses the user network performance experience of business-critical applications. The score, ranging between 0 and 10, where 0 is poor and 10 is excellent, indicates whether the app is performing as well as expected or is performing poorly.

The APS can answer questions such as

- Are my important applications performing well from a network perspective for my network users?
- Has this been a persistent problem or is it getting worse?
- If an application is not performing well, what might be causing the problem?

Calculating the APS

The score includes input from one or more of the following metrics:

- Network delay – the time taken for data to traverse the network (on the wire)
- Server delay – the time taken for a server to respond to the request
- Normalized network delay – the time taken for data to traverse the network, where the delay is measured independent of the transaction size by assuming a normalized packet size of 1024 bytes
- Normalized server delay – the time taken for a server to respond to the request, where the delay is measured independent of the transaction size by assuming a normalized packet size of 1024 bytes

- Round-trip time – the time taken
- Jitter – the measure of variability of network delay, defined as one standard deviation of network delay
- Inbound loss – the percentage of packet loss on inbound traffic
- Outbound loss – the percentage of packet loss on outbound traffic

Each metric that contributes to the score has a threshold value set. These threshold values are set on the Exinda Appliance, and can be set manually or be determined automatically by the appliance as it observes the traffic over a period of time to determine a baseline threshold values.

Setting-up Application Performance Scores for Individual Applications

In the Exinda Management Center you can identify the applications whose performance you consider important to the operation of the organization. As you identify these applications, you can assign thresholds against their performance scores that can trigger alerts. As the performance drops below the threshold, specified users then receive email alerts to draw attention to the issue.

The broad process of setting-up performance scoring is to:

- Firstly, identify the application, define the APS and threshold, and add it to the Configuration Library. See Setting-up Application Performance Scores for Individual Applications above for more information.
- Secondly, assign the APS to the Configured Appliances, identify the network objects, and define a baseline period for determining the score. See Adding APS Library Items to the Appliances on page 99 for more information.

Creating Application Performance Score Library Items

Before you can start to monitor the performance of the important applications on your network, you need to identify those applications in the Configuration Library. The Configuration Library comes with definitions for a very large number of supported applications.

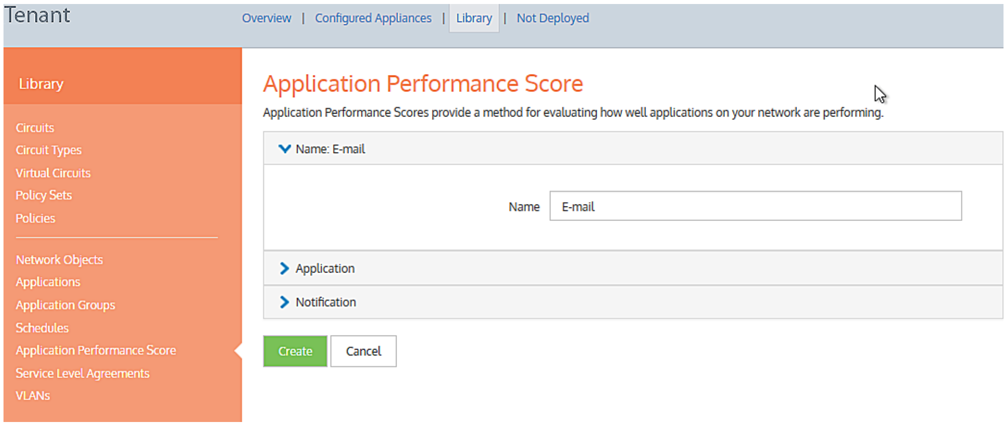
Procedure

1. In the EMC interface, click **Library > Application Performance Scores**.
2. On the right side, select the **Create new application performance…** link.

   The APS set up page opens.
3. Click on **Name**.

   The "Name" section expands.
4. In the **Name** field, provide a meaningful name for the new performance score.

> **NOTE:**
>
> ***In the screenshots that follow, the example given is of setting up a performance score for email services.***



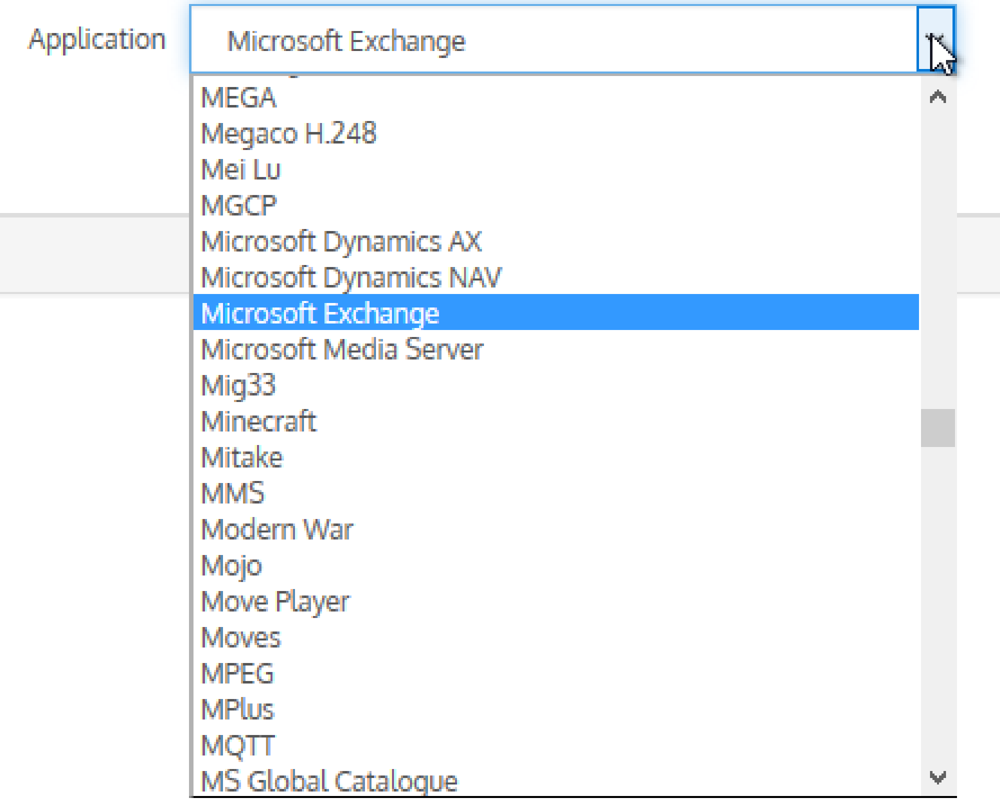
Application Performance Score

Application Performance Scores provide a method for evaluating how well applications on your network are performing.

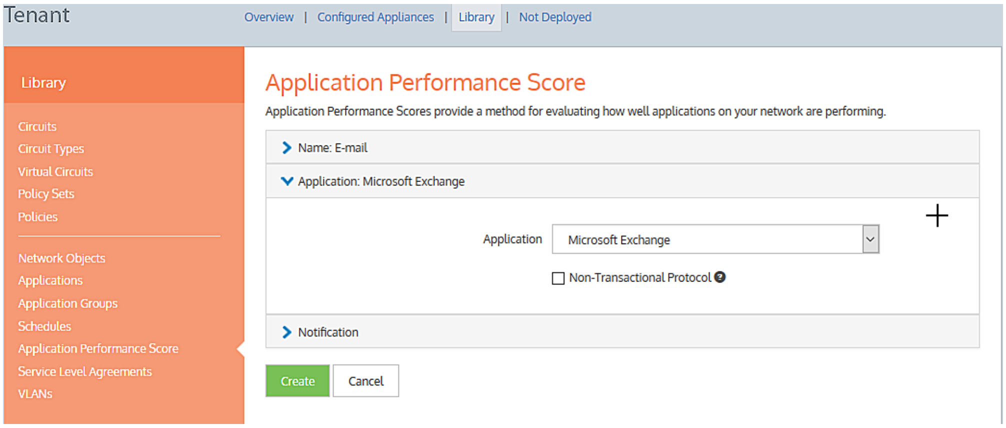
Name: E-mail

Name: E-mail

5. Click on **Application**.
   The "Application" section expands.
6. Click the down-arrow to open the **Application** drop-down list and select the application you need.



Application: Microsoft Exchange



Application Performance Score

Application Performance Scores provide a method for evaluating how well applications on your network are performing.

Name: E-mail

Application: Microsoft Exchange

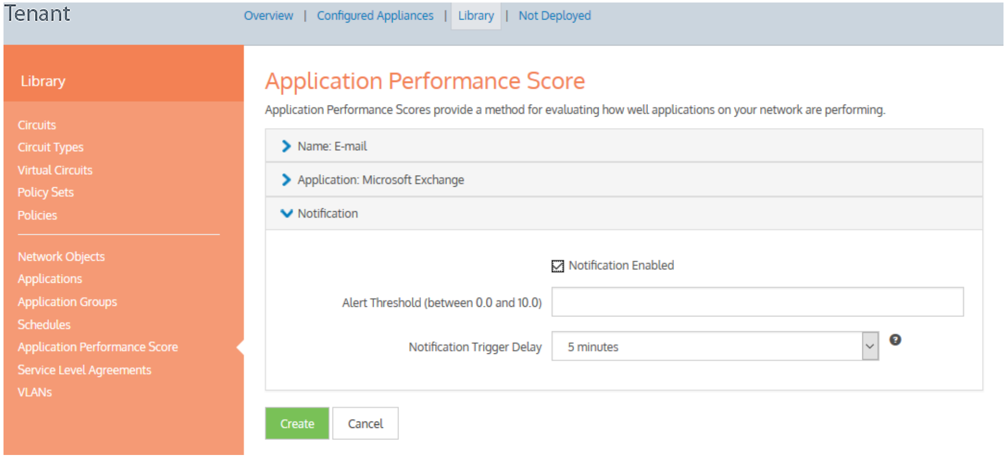
Application: Microsoft Exchange

□ Non-Transactional Protocol

IMPORTANT

Before proceeding, you should consider the type of protocol used by the application. If it uses a non-transactional protocol, you should select the checkbox. For more information, click the ? button.

7. Click **Notification**.
   The "Notification" configuration section expands.



Application Performance Score

Application Performance Scores provide a method for evaluating how well applications on your network are performing.

Name: E-mail

Application: Microsoft Exchange

Notification

☑ Notification Enabled

Alert Threshold (between 0.0 and 10.0)

Notification Trigger Delay: 5 minutes

8. Do **each** of the following:
   - If you need to be notified when the Alert Threshold is exceeded, select the **Notification Enabled** checkbox.
   - In the **Alert Threshold** field, type an alert level between 0.0 and 10.0.

   NOTE:

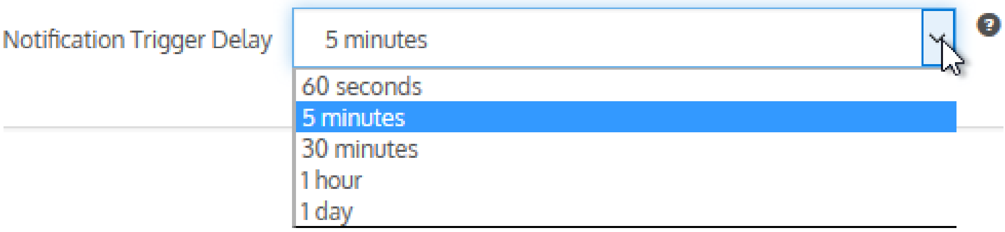
   The Alert Level is a measure of how important is the service the application provides. For example, an application that provides real-time communications would require a higher alert level than one whose responsiveness is not as critical.

   - For the **Notification Trigger Delay**, click the down-arrow and select the an acceptable delay period.

TIP

The notification is only triggered if the condition persists for the entire delay period.

Click the ? button for more information.



Notification Trigger Delay: 5 minutes

TIP

You can modify any of these settings later.

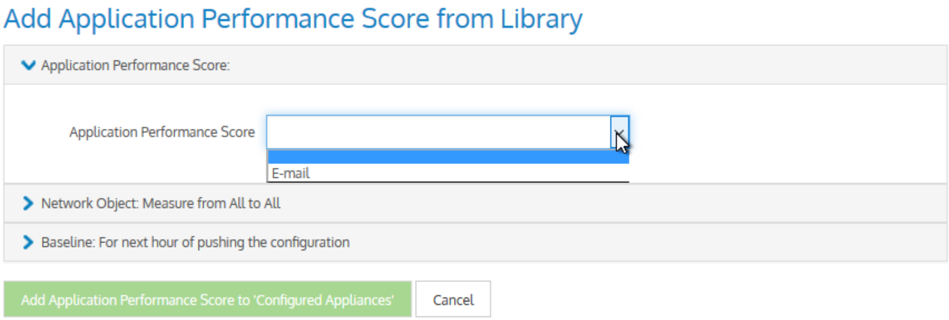
9. Click **Create**
   The screen refreshes to show an entry for the new performance score.
10. Repeat each of the preceding steps to define all of the APS definitions you need.

Adding APS Library Items to the Appliances

After completing the creation of the APS item definitions in the Configuration Library, you can then apply them to the appliances. When applying the scores, this is a global application; all appliances in the same appliance group receive the same configuration. After applying the scores, you must then push the configuration to the appliances in order to get any notifications.

Procedure

1. In the EMC interface, click **Configured Appliances > Application Performance Scores**.
2. On the right side, select the **Add application performance…** link.
   The "Add Application Performance Score from Library" pop-up appears.
3. Click **Application Performance Score**.
   The section expands.
4. Click the down-arrow to open the **Application Performance Score** drop-down list, and select the APS you need to apply.



Add Application Performance Score from Library

Application Performance Score:

Application Performance Score: E-mail

Network Object: Measure from All to All

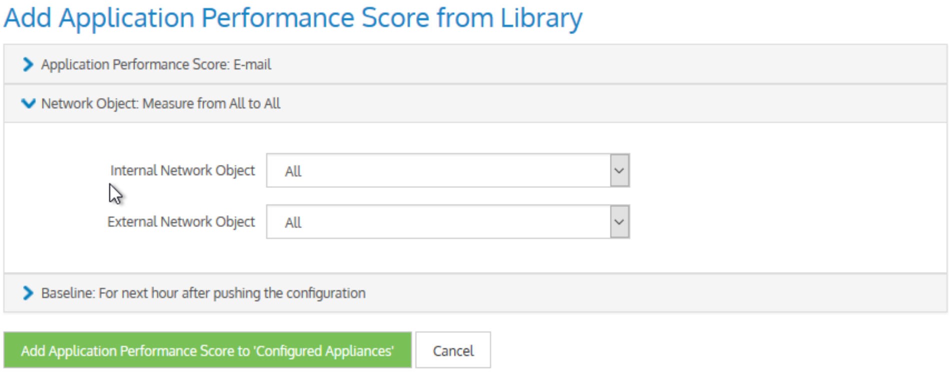
Baseline: For next hour of pushing the configuration

Add Application Performance Score to 'Configured Appliances'
Cancel

NOTE:

If you have appliances that do not have the most recent firmware, you may find that when you try to add an APS to the configured appliances the interface reference to the application Name is highlighted in red. If you allow your mouse cursor to hover over the red exclamation mark ❗, a tooltip opens with details about the issue.

5. Click **Network Object...**
   The section expands.



Add Application Performance Score from Library

Application Performance Score: E-mail

Network Object: Measure from All to All

Internal Network Object: All

External Network Object: All

Baseline: For next hour after pushing the configuration

Add Application Performance Score to 'Configured Appliances'
Cancel

6. Do *both* of the following:
   - Click the down-arrow to open the **Internal Network Object** drop-down list and select the object that fits your needs.

TIP

The internal objects are the Local Network Objects defined in the Configuration Library. The default is "All", but you can choose from any of the others that have been defined.

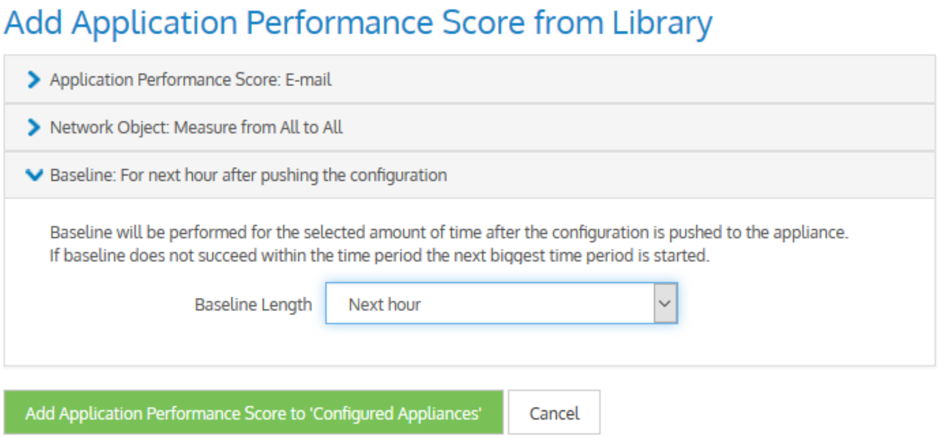
- Click the down-arrow to open the **External Network Object** drop-down list and select the previously Network Object that fits your needs.

When complete, the title of the Network Object section changes to summarize the the settings you have made.

7. Click **Baseline**.
   The section expands.

NOTE:

To establish a baseline for the performance of an application, its performance in the network must be monitored for period of time. The Baseline Length you define is the initial monitoring period, but if the baselining fails, the initial monitoring is automatically extended.



Add Application Performance Score from Library

Application Performance Score: E-mail

Network Object: Measure from All to All

Baseline: For next hour after pushing the configuration

Baseline will be performed for the selected amount of time after the configuration is pushed to the appliance.
If baseline does not succeed within the time period the next biggest time period is started.

Baseline Length: Next hour

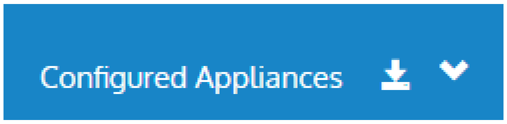
Add Application Performance Score to 'Configured Appliances'
Cancel

8. When finished, click **Add Application Performance Score to 'Configured Appliance'**.
   The screen refreshes to show an entry for the new performance score.
9. Repeat each of the preceding steps to apply all of the APS definitions you need.

IMPORTANT

When you have applied all of the APS items, you must push the configuration to the appliances.

10. At the top left of the interface, click anywhere the Configured Appliances area.



A listing of the appliance groups opens.

IMPORTANT

Choose to either apply the configuration changes to all appliances in the tenant, or to the appliances in a particular appliance group.

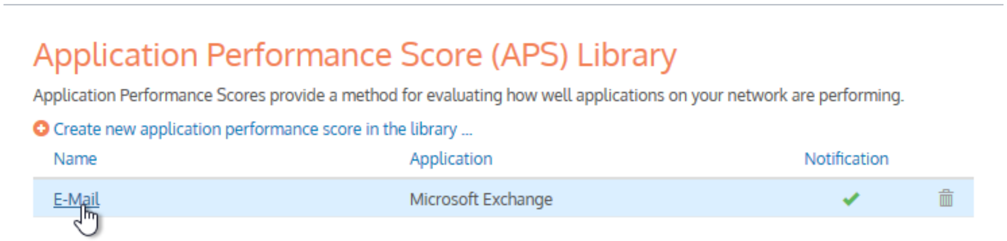
11. Click on the appropriate row.

Maintaining the Application Performance Scores in the Configuration Library

Over time, it may become necessary to modify the Application Performance Score items stored in the Configuration Library. When modifying an APS item, you are modifying its use wherever it has been applied.

Procedure

1. In the EMC interface, click **Library > Application Performance Scores**.
   A listing of the currently defined performance scores appears on the right.
2. In the **Name** column, click on the name of the APS item you need to modify.
   The configuration for the item opens.

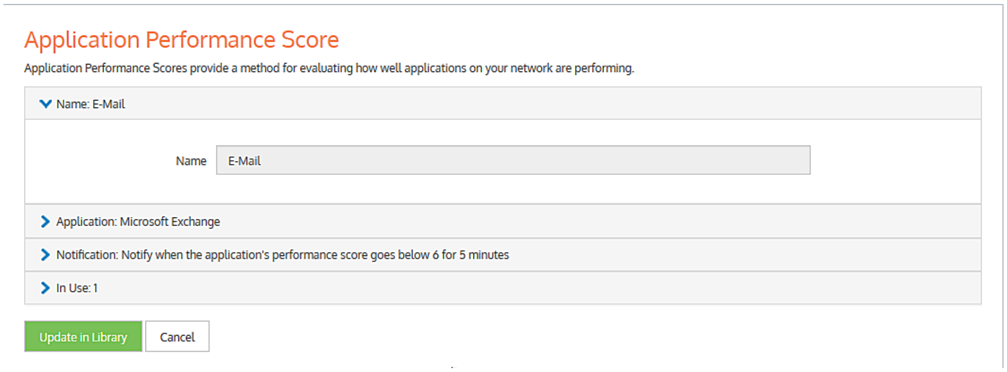


Application Performance Score (APS) Library

Application Performance Scores provide a method for evaluating how well applications on your network are performing.

Create new application performance score in the library ...

Name	Application	Notification	
E-Mail	Microsoft Exchange	✓	🗑



Application Performance Score

Application Performance Scores provide a method for evaluating how well applications on your network are performing.

Name: E-Mail

Name: E-Mail

Application: Microsoft Exchange

Notification: Notify when the application's performance score goes below 6 for 5 minutes

In Use: 1

3. Do the following, *as needed*:
   - Modify the APS **Name**.
   - Change the **Application**
   - Update the **Notification** definition
4. Before completing the modification, expand the **In Use** section to see how the APS items is currently being used.
5. When satisfied witht the changes, click **Update in Library**.
   The APS item list reopens.

Deleting an Application Performance Score from the Configuration Library

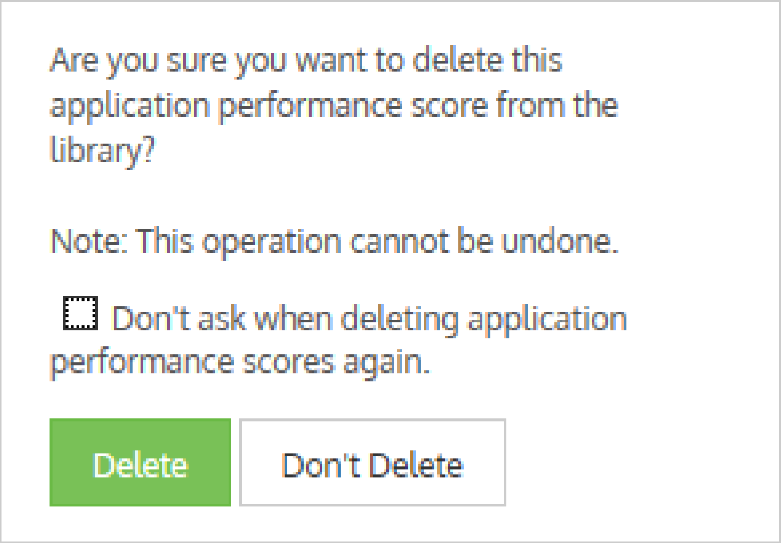
Over time, it may become necessary to delete an Application Performance Score item stored in the Configuration Library. You can only delete APS items if they are currently in use.

Procedure

1. In the EMC interface, click **Library > Application Performance Scores**.
   A listing of the currently defined performance scores appears on the right.

> **NOTE:**
> ***If the 🔒 icon appears at the extreme right of the row of the item you wish to delete, it means that the item cannot be deleted because it is in use. If you still need to delete, you will need to disable its use with the configured appliances.***

2. At the extreme right of the row containing the entry for the APS, click the 🗑 icon.
   A confirmation dialog opens.



Are you sure you want to delete this application performance score from the library?

Note: This operation cannot be undone.

□ Don't ask when deleting application performance scores again.

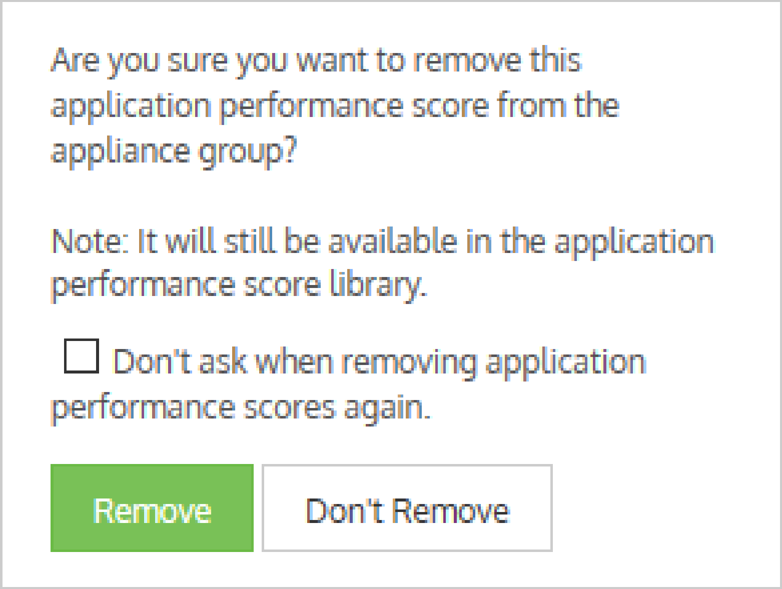
3. Click **Delete**.

Removing an Application Performance Score from the Configured Appliances

Should you find that a previously defined APS is no longer required, you can remove it from the appliance configuration. Removing an APS in this way does not remove it from the Configuration Library; the APS item remains there for future reuse. If you do want to remove it from the library, see Deleting an Application Performance Score from the Configuration Library on the previous page for more information, but you must remove an APS item from the appliance configuration before deleting it from the Configuration Library.

Procedure

1. In the EMC interface, click **Configured Appliances > Application Performance Scores**.
   The currently assigned APS items appear on the page.
2. In the **Name** column, find the entry for the APS item.
   At the extreme right of the row is an ✖ icon.
3. Click the ✖.
   A confirmation dialog box opens.



Are you sure you want to remove this application performance score from the appliance group?

Note: It will still be available in the application performance score library.

☐ Don't ask when removing application performance scores again.

4. Click **Remove**.
   The item is removed from the page.

Service Level Agreements

The Service Level Agreement (SLA) library objects are used to monitor the availability of particular IP addresses. By creating an SLA object, you identify the IP address to monitor. The Exinda Management Center then sends one ICMP ping every 10 seconds to the IP address. You can specify the ping packet size to use. You can also specify when an alert is triggered by defining the ping latency threshold and the duration by which the ping latency threshold was exceeded. An alert is triggered when the latency of the SLA site exceeds the latency threshold for longer than the specified duration.

Where do I find Service Level Agreements?

The Service Level Agreements library items can be found in **Library > Service Level Agreements**.

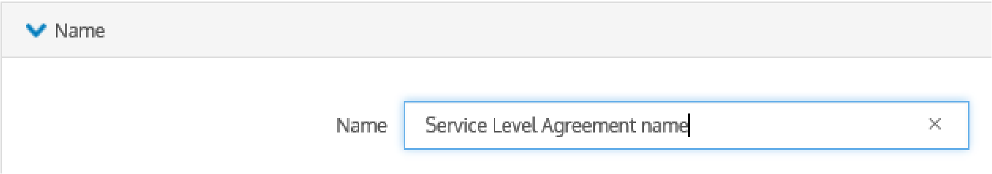
Or,

Configured Appliances > Service Level Agreements.

> **NOTE**
>
> ***You can create a Service Level Agreement through both the Library and Configured Appliances interfaces. However, to apply an SLA to an appliance, you must do this in the Configured Appliances interace.***

Setting up a Service Level Agreement

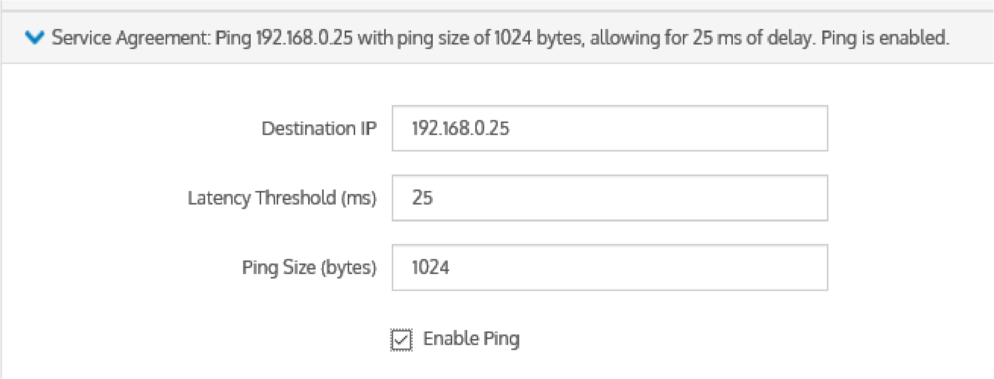
1. Click **Create new service level agreement in library...**
   The screen refreshes.
2. In the **Name** field, type a meaningful name for the new Service Level Agreement.



Name

Name: Service Level Agreement name

3. Click **Service Agreement** and do *each* of the following:
   - In the **Destination** field, type the IP address of the server whose availability you need to monitor.
   - In the **Latency Threshold (ms)** field, type a value for the response time.
   - In the **Ping Size (bytes)** field, type a packet size, for example, 1024.
   - Select the **Enable Ping** checkbox.



Service Agreement: Ping 192.168.0.25 with ping size of 1024 bytes, allowing for 25 ms of delay. Ping is enabled.

Destination IP: 192.168.0.25

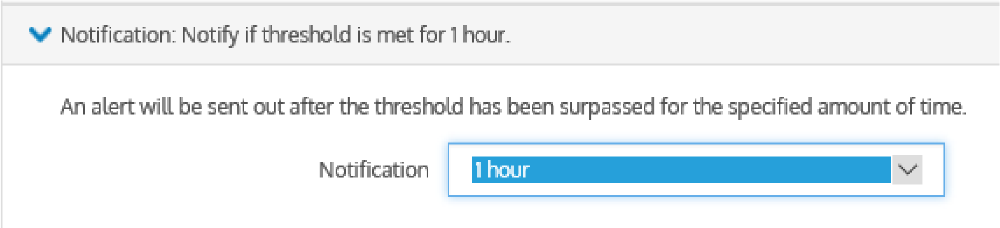
Latency Threshold (ms): 25

Ping Size (bytes): 1024

☑ Enable Ping

4. Click **Notification**, and select a delay period from the drop-down list.

> **TIP**
>
> *The default delay is 1 hour. If this setting fits your needs, you do not need to change anything here.*



Notification: Notify if threshold is met for 1 hour.

An alert will be sent out after the threshold has been surpassed for the specified amount of time.

Notification: 1 hour

The options are:

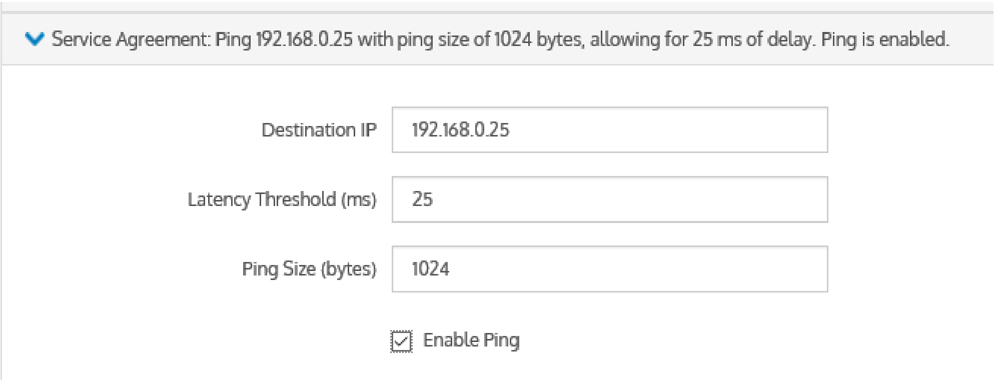
- 0 – Disabled – *this disables the alert*
- 30 seconds
- 60 seconds
- 5 minutes
- 30 minutes
- 1 hour – *the Default setting*

5. Click **Create**.

Modifying a Service Level Agreement

With the exception of renaming the SLA library item, you can modify all aspects of the item. Do the following, *as needed*:

1. In the **Service Level Agreement** list, click the name of the SLA you need to modify.
2. To modify the modify the destination and ping definition, click **Service Agreement** and amend the following:
   - If you need to change the destination, click in the **Destination** field and edit the IP address.
   - If you need to change the latency threshold, click in the **Latency Threshold (ms)** field and edit the value.
   - If you need to change the ping size, click in the **Ping Size (bytes)** field and edit the value.
   - If you need to disable the ping, deselect the **Enable Ping** checkbox.



Service Agreement: Ping 192.168.0.25 with ping size of 1024 bytes, allowing for 25 ms of delay. Ping is enabled.

Destination IP: 192.168.0.25

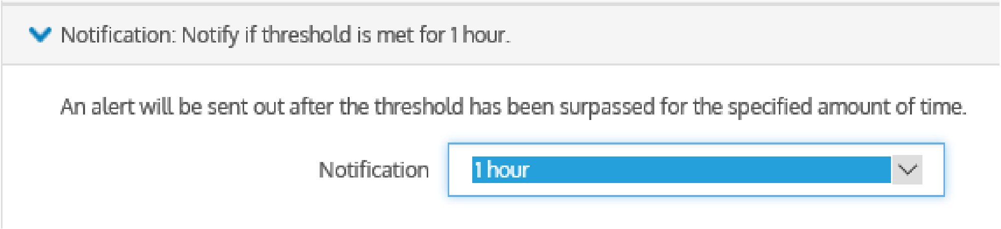
Latency Threshold (ms): 25

Ping Size (bytes): 1024

☑ Enable Ping

To modify the notification, click **Notification**, and select a delay period from the drop-down list.

© 2016 Exinda Networks Inc.



Notification: Notify if threshold is met for 1 hour.

An alert will be sent out after the threshold has been surpassed for the specified amount of time.

Notification: 1 hour

The options are:

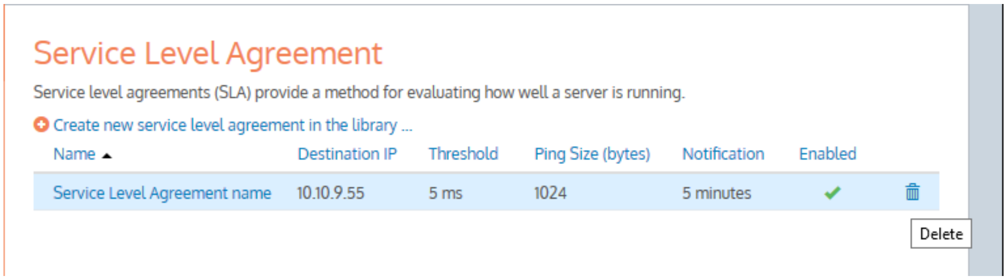
- 0 – Disabled – *this disables the alert*
- 30 seconds
- 60 seconds
- 5 minutes
- 30 minutes
- 1 hour – *the Default setting*

3. Click **Update in Library**.

Deleting a Service Level Agreement

> **NOTE**
>
> ***You cannot delete a service level agreement if it is in use. If so, a Lock 🔒 icon appears to the right of the library object entry.***

1. From the Library, select **Service Level Agreements**.
2. In the list of SLA library objects, find the SLA you need to delete.



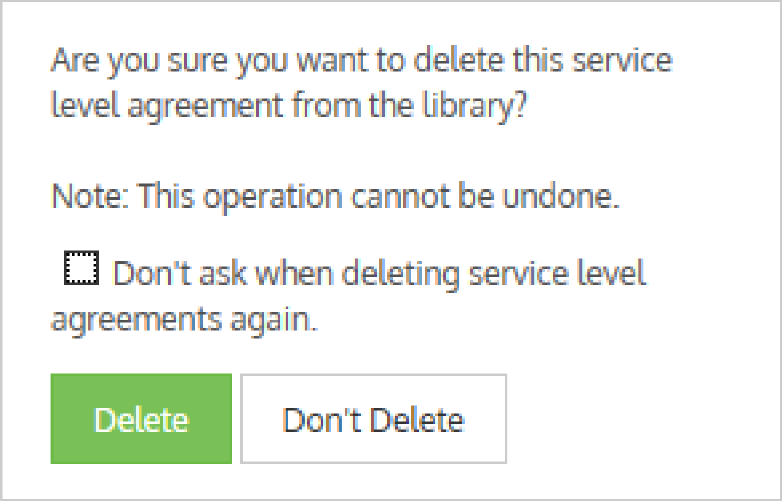
Service Level Agreement

Service level agreements (SLA) provide a method for evaluating how well a server is running.

Create new service level agreement in the library ...

Name ▲	Destination IP	Threshold	Ping Size (bytes)	Notification	Enabled	
Service Level Agreement name	10.10.9.55	5 ms	1024	5 minutes	✓	🗑

3. To the right of the object entry, click the Delete 🗑 icon.
You are asked to confirm the deletion.



Are you sure you want to delete this service level agreement from the library?

Note: This operation cannot be undone.

□ Don't ask when deleting service level agreements again.

4. Click **Delete**.

VLANs

Virtual LAN (VLAN) Objects are used to logically separate hosts (or groups of hosts) on a functional basis rather than on a physical basis. Once VLAN Objects are defined, they can be used in Optimizer policies to filter traffic. By default, the Exinda appliance has a single VLAN defined called "ALL", which matches all traffic (regardless if that traffic is part of a VLAN or not). Additional VLAN Objects can easily be added.

All the defined VLAN objects are shown in the table. Each VLAN object can be edited or deleted by clicking the appropriate button in the table. The ALL VLAN object is protected and cannot be edited or deleted.

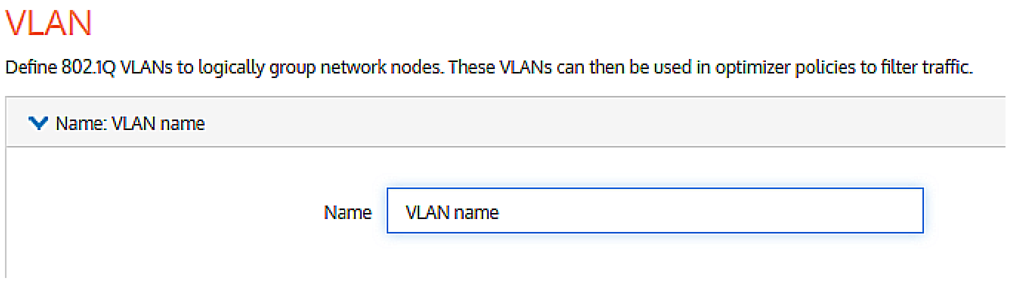
Where to configure VLANs?

Click **Library > VLANs**.

To add a new VLAN object

1. Click **Create new VLAN in the library...**.
   The screen refreshes to display the VLAN configuration options.
2. In the **Name** field, type a meaningful name for the VLAN.

© 2016 Exinda Networks Inc.



VLAN

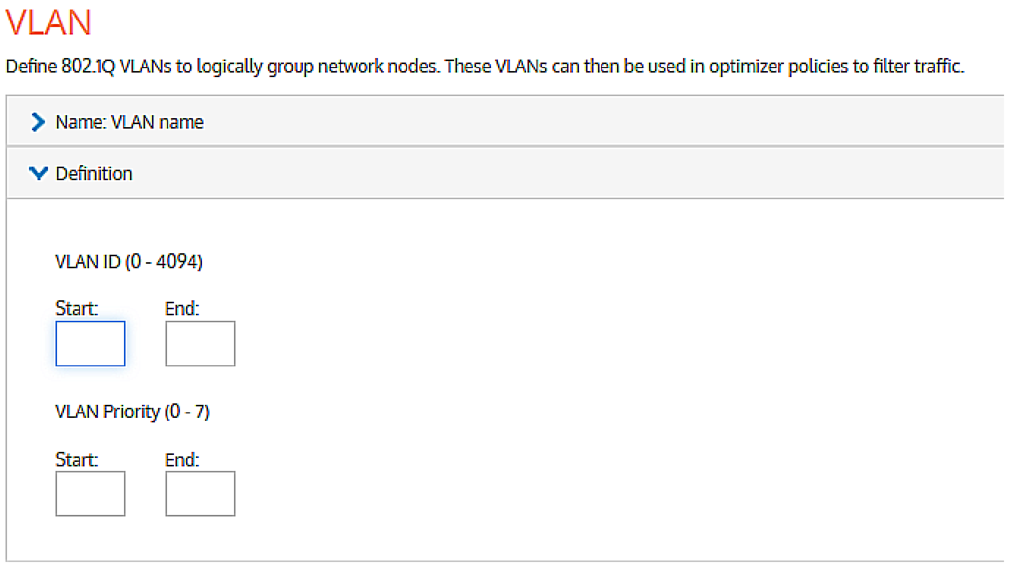
Define 802.1Q VLANs to logically group network nodes. These VLANs can then be used in optimizer policies to filter traffic.

3. Click **Definition**, and do *each* of the following:
   a. In the VLAN Start and End fields, type the range of VLAN IDs that must appear in the VLAN.

> **NOTE**
>
> ***The absolute range is 0–4094. This would equate to all VLAN IDs being in the VLAN. Leaving both fields blank would give the same result. To define a lesser range, type a range somewhere within the absolute range. To isolate one VLAN, type its ID value in both the Start and End fields.***

   b. In the VLAN Priority Start and End fields, type range of values for this VLAN.

> **NOTE**
>
> ***You can define priorities within a maximum range of 0–7. This would equate to all priorities being assigned to the VLAN. Leaving both fields blank would give the same result. To define a lesser range, type a range somewhere between the maximum range. To define just one priority, type the same value in both the Start and End fields.***



VLAN

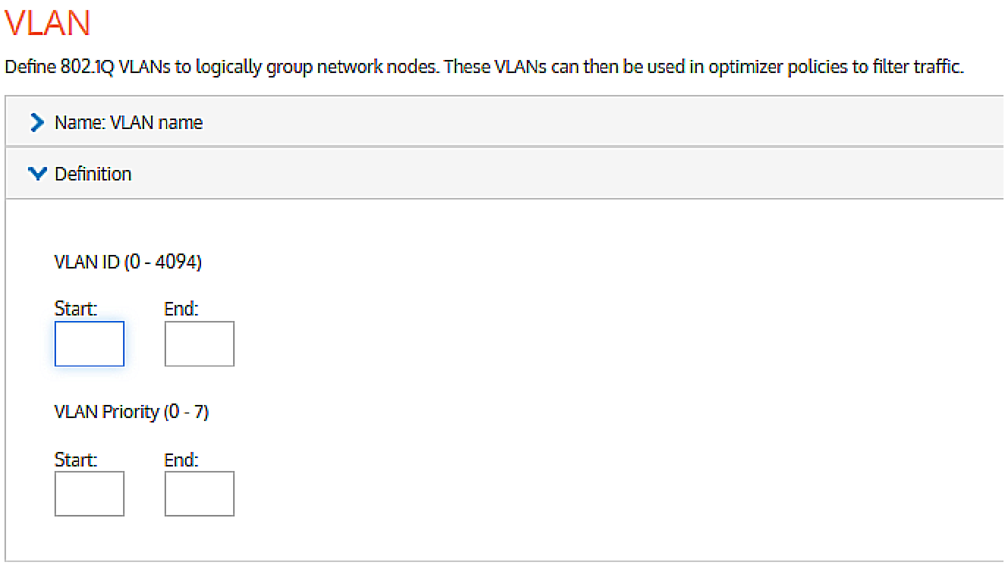
Define 802.1Q VLANs to logically group network nodes. These VLANs can then be used in optimizer policies to filter traffic.

4. Click **Create**.

Modifying a VLAN

With the exception of renaming the VLAN library item, you can modify all other aspects of the item. Do the following, *as needed*:

1. In the **VLANs** list, click the name of the VLAN you need to modify.
2. To modify the VLAN definition, click **Definition** and amend the following:
   - If you need to change the VLAN ID range , edit the entries in the Start and End fields.
   - If you need to change the VLAN priority, edit the Start and End fields.



VLAN

Define 802.1Q VLANs to logically group network nodes. These VLANs can then be used in optimizer policies to filter traffic.

VLAN ID (0 - 4094)

Start: End:

VLAN Priority (0 - 7)

Start: End:

3. Click **Update in Library**.

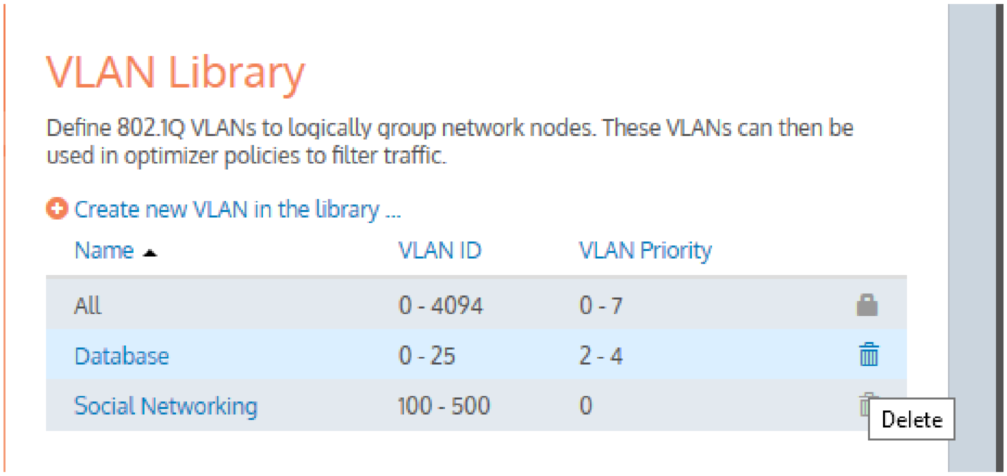
Deleting a Service Level Agreement

NOTE

You cannot delete a VLAN if it is in use. If so, a Lock icon appears to the right of the library object entry. Note also that the default "ALL" VLAN cannot be deleted.

The "All" VLAN is available by default and cannot be deleted

1. From the Library, select **VLANs**.
2. In the list of VLAN library objects, find the VLAN you need to delete.



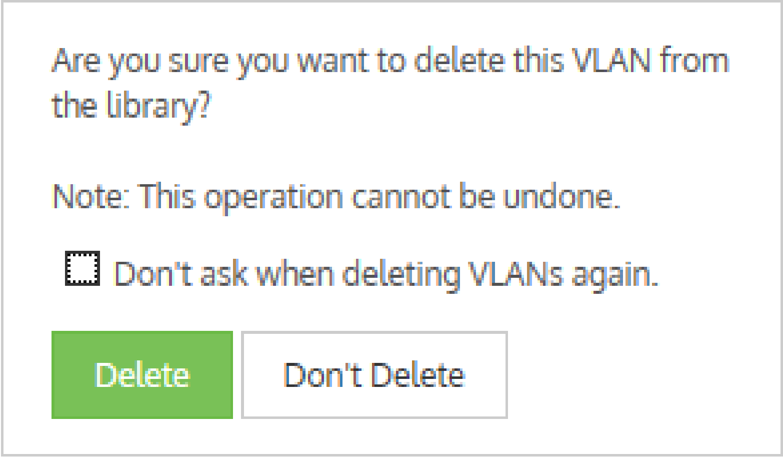
VLAN Library

Define 802.1Q VLANs to logically group network nodes. These VLANs can then be used in optimizer policies to filter traffic.

Create new VLAN in the library ...

Name ▲	VLAN ID	VLAN Priority	
All	0 - 4094	0 - 7	🔒
Database	0 - 25	2 - 4	🗑
Social Networking	100 - 500	0	🗑

3. To the right of the object entry, click the Delete 🗑 icon.
   You are asked to confirm the deletion.



Are you sure you want to delete this VLAN from the library?

Note: This operation cannot be undone.

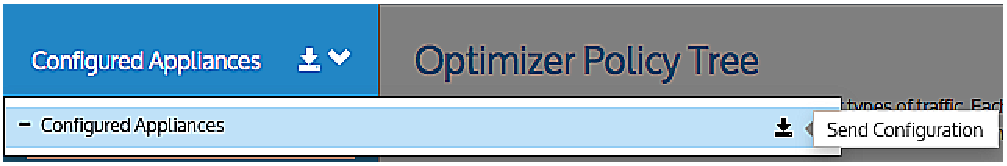
□ Don't ask when deleting VLANs again.

4. Click **Delete**.

Appendix A: Configuring your Appliances through the CLI

You can use the Command Line Interface (CLI) to push specific commands to the current Appliance Group for instances where the Exinda Management Center User Interface does not support such configuration (e.g., VLAN configuration).

However, if you are sending commands that are sensitive to the order in which they are executed, ensure you click the **Send Configuration** icon after each command to ensure the correct order of operations is followed. For example, configure the Optimizer Policy Tree and send the configuration to the appliances.



Then send the CLI commands to restart the optimizer and send that to the appliances. Note that you do not need to wait for the appliances to receive the configuration before issuing the next set of configuration or commands.

See the following for information about each of the CLI commands:

© 2016 Exinda Networks Inc.

© 2016 Exinda Networks Inc.

Service

You can use the **`service`** command to manage Application Acceleration modules:

Managing a service

```
service <service> {start|stop|restart|enable|disable}
```

To start, stop, or restart the service:

```
service <service> {start|stop|restart}
```

To enable or disable the service:

```
service <service> {enable|disable}
```

> **NOTE**
>
> ***Not all modules support `enable` and `disable`.***

Viewing a service

To see the status of a service:

```
show service <service>
```

TCP Acceleration

You can use the **`acceleration tcp`** command configure TCP acceleration settings.

Configuring TCP Acceleration

```
acceleration tcp {cc|discovery|dual-bridge-bypass|keep-alive|transport|window-scale}

[no] acceleration tcp {discovery|dual-bridge-bypass|keep-alive}
```

To set the WAN side congestion control algorithm:

```
acceleration tcp cc
{cubic|hybla|highspeed|veno|reno|bic|vegas|htcp|yeah|illinois|scalable|lp|westwood}
```

To enable appliance auto-discovery:

```
[no] acceleration tcp discovery
```

To enable accelerated traffic to be processed on only one bridge:

```
[no] acceleration tcp dual-bridge-bypass
```

- When enabled, acceleration will be processed on only one bridge, which is good for backhauled settings. Default is enabled.
- When disabled, accelerated traffic can be handled on any bridge, which is good for aggregated link settings with asymmetric routes.

To manage keep-alive settings:

```
[no] acceleration tcp keep-alive {enable|timeout}
```

- `enable` - Enables the sending of keep-alive packets on the WAN. The timeout specifies when to activate the keep-alives if enabled.
- `timeout` - Specifies the amount of time, in seconds, that a connection may be idle before sending keep-alive packets is enabled. Keep-alive packets are sent once per minute until either a response is received, or 5 minutes passes. If five minutes passes without a response the connection is terminated.

To set the transport mode:

```
acceleration tcp transport {transparent|tunnelled}
```

To set the window scaling factor, which determines how large the TCP window is allowed to grow per connection:

```
acceleration tcp window-scale <factor>
```

- `<factor>` - 0 - 14. The default is 5, which equates to a TCP window of 2MB. Increasing one step in the factor doubles the TCP window size.
- `0` - 64k
- `1` - 128k
- `2` - 256k
- `3` - 512k
- `4` - 1M
- `5` - 2M
- `6` - 4M
- `7` - 8M
- `8` - 16M
- `9` - 32M
- `10` - 64M
- `11` - 128M
- `12` - 256M
- `13` - 512M
- `14` - 1G

WAN Memory

You can use the **`accleration wm`** command to configure WAN Memory acceleration settings.

Configuring WAN Memory settings

```
acceleration wm {cache|enable|persistence|reduction}
no acceleration wm {enable|persistence enable|reduction}
```

To enable WAN Memory byte-level caching:

```
acceleration wm enable
```

To manage the WAN Memory cache:

```
acceleration wm cache {clear|sync}
```

- `cache clear [<amount>]`—Clear the contents of the cache by expiring 100% of it's contents or a specified amount, specified as a percentage or absolute bytes.
- `cache sync` — Enable WAN Memory cache synchronization across all appliances in the cluster.

To clear or enable disk cache persistence on next restart:

```
acceleration wm persistence {clear|enable}
```

- `persistence clear` - Clear the persistent information
- `persistence enable` - Enable persistent storage

To enable LZ-compression or small matching:

```
acceleration wm reduction {lz-compression|small-matcher} enable
```

SMB Acceleration

You can use the **`acceleration smb`** command to configure SMB acceleration settings.

Configuring adaptive response settings

```
acceleration smb {application|cache|enable|v1|v2}
```

To enable or disable SMB acceleration.

```
[no] acceleration smb enable
```

To add applications supported by the SMB module:

```
[no] acceleration smb application <application>
```

To clear the SMB disk cache:

```
acceleration smb cache clear
```

SMB1 commands

```
acceleration smb v1 {enable|meta-cache|prefetch|read-ahead|write-behind}
```

To enable or disable SMB1 acceleration:

```
[no] acceleration smb v1 enable
```

To enable or disable SMB1 meta-caching:

```
[no] acceleration smb v1 meta-cache
```

To set the amount to pre-fetch:

```
acceleration smb v1 prefetch <prefetch-kbytes>
```

- `prefetch <prefetch-kbytes>` - Value in kbytes must be between 0 and 8192.

To enable or disable SMB1 read-ahead :

```
[no] acceleration smb v1 read-ahead
```

To enable or disable SMB1 write-behind :

```
[no] acceleration smb v1 write-behind
```

To enable or disable SMB1 signing :

```
[no] acceleration smb v1 signing enable
```

SMB2 commands

```
acceleration smb v2 {enable|signing enable}
```

To enable or disable SMB2 acceleration:

```
[no] acceleration smb v2 enable
```

To enable or disable SMB2 signing :

```
[no] acceleration smb v2 signing enable
```

Viewing acceleration settings

```
show acceleration smb {applications|signed-servers|v1|v2}
```

To list the applications that support SMB:

```
show acceleration smb applications
```

To list the SMB signed servers:

```
show acceleration smb signed-servers
```

To display the configuration for SMB1:

```
show acceleration smb v1 config
```

To display the SMB1 connections:

```
show acceleration smb v1 connections [list [detailed]]
```

- `smb v1 connections` - Display the connections.
- `smb v1 connections list` - Display the connections with sources and destinations of the connections.
- `smb v1 connections list detailed` - Display the connections, the sources and destinations of the connection, and the client/server operating systems and shared file directories.

To display the configuration for SMB2:

```
show acceleration smb v2 config
```

To display the SMB2 connections:

```
show acceleration smb v2 connections [list]
```

- `smb v2 connections` - Display the connections.
- `smb v2 connections list` - Display the connections with sources and destinations of the connections.

SSL Acceleration

You can use the **`acceleration ssl`** command to configure the SSL acceleration settings.

Configure SSL acceleration

```
acceleration ssl {enable|flush|reset|server}
```

To enable [or disable] SSL acceleration:

```
[no] acceleration ssl enable
```

Configure SSL acceleration servers

To create an SSL server to accelerate with:

```
acceleration ssl server <server-name>
```

To configure the SSL server:

```
acceleration ssl server <server-name> {address|certificate|client-auth-
cert|port|revocation|sni|validation}
```

- `address <address>` - Specify the IPv4 address of the server to accelerate to.
- `port <number>` - Specify the port number of the application running on the server to accelerate to.
- `sni <sni-extension>` - Specify the Server Name Indication (SNI) extension. This command is used when the server has multiple SSL certificates with a SNI specified.
- `certificate <certificate-name>` - Select the certificate to use for re-encryption of the SSL session.

© 2016 Exinda Networks Inc.

- `client-auth-cert <certificate-name>` - Select the certificate for client authentication on the SSL server.
- `validation {certificate|none|reject}` - Specify the type of validation to apply to the server's certificate.
  - `certificate <certificate-name>` - Accept specific certificate for validation of the SSL server. SSL Acceleration accepts and processes the connection only if the server's certificate matches the specific certificate named in the Client Auth Certificate field. Otherwise, the connection is not processed.
  - `none` - Accept any certificate. SSL Acceleration accepts and processes the connection even if the server's SSL certificate is invalid or expired.
  - `reject` - Reject any certificate. SSL Acceleration does not processes the connection under any circumstances. The connection is still accelerated, but is not SSL accelerated.
- `revocation [none|oscp-aia|ocsp-server]` - If validation none is specified, then use this command to specify the revocation type.
  - `none` - No check is performed. The client auth certificate is used regardless of whether the certificate is revoked or not.
  - `oscp-aia` - The Online Certificate Status Protocol (OCSP) Authority Information Access (AIA) check is performed. The method uses the location of the authority embedded in the certificate to check for the certificate's revocation status. Note that if the AIA location is not specified in the certificate when this option is chosen, then the certification revoke check will not happen.
  - `ocsp-server` - The Online Certificate Status Protocol (OCSP) check is performed. This method presents an OCSP Server URI field where you can type the location of the authority to check for the certificate's revocation status.

To reset a disabled SSL acceleration server:

```
acceleration ssl reset <server-name>
```

To flush OCSP response cache of the SSL acceleration server:

```
acceleration ssl flush <server-name>
```

Viewing SSL acceleration server configuration

To show currently configured SSL acceleration servers:

```
show acceleration ssl server <server-name>
```

CLI: Edge Cache Acceleration

You can use the **`acceleration edge-cache`** command to configure Edge Cache acceleration. Edge Cache enables single-sided caching of Internet-based content, including web objects, videos and software updates. Edge Cache requires only one Exinda appliance.

When web objects are downloaded from the Internet or across WAN links, Edge Cache stores them at the edge of the network. When subsequent requests come for the same material, the content is quickly delivered from Edge Cache, without the need to re-download the data over the WAN. The result is the ability to experience LAN speeds of WAN objects, and provide users with a better network experience.

Edge Cache also supports HTTPS sites allowing the appliance to be a forward proxy and decrypt content for caching. This is important as more and more applications and services are moving to the cloud. These SaaS-based applications are typically delivered over HTTPS and so to be effective, Edge Cache must support caching this HTTPS traffic.

Version Info:

As of version 7.0.2, Edge Cache can cache HTTPS content, as well as HTTP content.

Configuring Edge Cache

```
acceleration edge-cache {administrator-email|application|cache|connect-timeout|enable-
https|https-black-list|https-cert|https-list-type|https-white-list|never-cache|never-
direct|object-size|peer|range-offset}

no acceleration edge-cache {application|enable-https|https-black-list|https-white-
list|never-cache|never-direct|peer}
```

To specify the maximum and minimum size of objects to store:

```
acceleration edge-cache object-size {maximum|minimum> <size>
```

`<size>` – The size parameter should use SI units e.g. 100M or 512k.

To specify how long Edge Cache should wait for a response when fetching objects from the server:

```
acceleration edge-cache connect-timeout <seconds>
```

To add or remove an HTTP URL or domain that should be blacklisted (i.e. should never be cached):

```
[no] acceleration edge-cache never-cache <URL or domain>
```

To add or remove HTTP applications that should be cached:

```
[no] acceleration edge-cache application <application>
```

`application <application>` - Note: Only applications that use the HTTP protocol are supported.

To enable [or disable] HTTPS caching:

```
[no] acceleration edge-cache enable-https
```

To specify the signing certificate to use to create dynamic SSL certificates during HTTPS caching:

```
acceleration edge-cache https-cert <cert-name>
```

To specify an HTTPS black-list of IPs or domains:

```
acceleration edge-cache https-list-type black-list
```

Specifies that Edge Cache will use a black-list for determining what sites can not be cached. All others will be allowed.

```
acceleration edge-cache https-black-list {dest-domain|dest-ip|src-domain|src-ip}
```

- `src-domain <domain>` - The domain that initiated the conversation.
- `src-ip <ip>` - The IP that initiated the conversation. The IP can include a mask.
- `dest-domain <domain>` - The domain that was the destination of the conversation.
- `dest-ip <ip>` - The IP that was the destination of the conversation. The IP can include a mask.
- Note: Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://)

To remove a domain or IP from the black-list:

```
no acceleration edge-cache https-black-list <internal ID>
```

`https-black list <internal ID>` – To determine the internal ID, type: `no acceleration edge-cache https-black-list ?`, which presents the list of HTTPS black-list sites in the format: Internal ID, Type, Value

To specify an HTTPS white-list of IPs or domains:

```
acceleration edge-cache https-list-type white-list
```

- Specifies that Edge Cache will use a white-list for determining what sites can be cached. No others will be allowed.

```
acceleration edge-cache https-white-list {dest-domain|dest-ip|src-domain|src-ip}
```

- `src-domain <domain>` - The domain that initiated the conversation.
- `src-ip <ip>` - The IP that initiated the conversation. The IP can include a mask.
- `dest-domain <domain>` - The domain that was the destination of the conversation.
- `dest-ip <ip>` - The IP that was the destination of the conversation. The IP can include a mask.
- Note: Domains are resolved using the DSN. Ensure the domains are in the format that are required by DNS (i.e. without https://)

To remove a domain or IP from the white-list:

```
no acceleration edge-cache https-white-list <internal ID>
```

- `https-white list <internal ID>` - To determine the internal ID, type: `no acceleration edge-cache https-white-list ?`, which presents the list of HTTPS whit-list sites in the format: Internal ID, Type, Value

To clear the object cache:

```
acceleration edge-cache cache clear
```

To configure an Edge Cache peer:

If you have an upstream proxy in your environment, you can configure it as a proxy peer to ensure that Edge Cache can fetch content from the Internet.

```
[no] acceleration edge-cache peer <hostname> [http-port|icp-port|option]
```

- `<hostname>` - The hostname of the peer object memory.
- `http-port <port>` - The HTTP port for the peer command
- `icp-port <port>` - The ICP port for the peer command
- `option default` - Use the default peer options
- `option proxy-only` - Do not cache objects from this peer.
- `option no-query` - This peer does not support ICP
- `option weight=n` - Specify the peer priority. Peers with higher priority will be consulted first.
- `option round-robin` - Specify that peers should be consulted in round-robin order.
- `option closest-only` - Only forward closest parent ICP misses.
- `option originserver` - Specify that this peer is an origin server

To never fetch a file directly; always use the peer:

```
[no] acceleration edge-cache never-direct
```

To prevent delays when skipping ahead during video downloads:

```
acceleration edge-cache range-offset <limit>
```

Viewing configuration settings

To show the current Edge Cache configuration settings:

```
show acceleration edge-cache
```

NCP Acceleration

You can use the **`acceleraton ncp`** command to enable Novell NCP acceleration.

Configuring NCP acceleration

To enable Novell NCP acceleration:

```
[no] acceleration ncp enable
```

Prepopulation

You can use the **`acceleration prepopulation`** command to configure prepopulation objects.

Configuring prepopulation

```
acceleration prepopulate <name> {location|password|recursive|start|stop|username}
```

To specify the location of the cache:

```
acceleration prepopulate <name> location {cifs|http} <server> <path>
```

- `prepopulate <name>` - Specify a name for prepopulation object
- `location cifs <server> <path>` - Specify the server and path for the cifs source material
- `location http <server> <path>` - Specify the server and path for the http source material

To specify the credentials to access the server:

```
acceleration prepopulate <name> username <username>
```

```
acceleration prepopulate <name> password <pwd>
```

- `password <pwd>` - Specify the clear text password

To recursively fetch all the files in the specified directory, as well as those in sub-directories:

```
[no] acceleration prepopulate <name> recursive
```

To start or stop prepopulating:

```
acceleration prepopulate <name> {start|stop}
```

To remove a prepopulation object:

```
no acceleration prepopulate <prepopulate-name>
```

```
acceleration prepopulate clear <prepopulate-name>
```

```
acceleration prepopulate clear all - Remove all prepopulation objects
```

Active Directory

You can use the **`active`** command to configure Active Directory (AD) settings on the appliance. Note that more steps may need to be taken outside the appliance to install and configure the Exinda Active Directory Connector.

Configuring Active Directory on the appliance

```
active {port|renumerate}
```

To set the listen port for the Active Directory daemon:

```
active port <port number>
```

To force the Active Directory service to re-send information:

```
active renumerate {all|logins|users}
```

- `renumerate all` - Re-fetch the entire list of users and logins.
- `renumerate logins` - Re-fetch the entire list of logins from all clients.
- `renumerate users` - Re-fetch the entire list of users from all clients.

© 2016 Exinda Networks Inc.

Managing the Active Directory service

```
service add
```

To manage the active directory services, such as starting, stopping, restarting:

```
service add {stop|start|restart|enable|disable}
```

- `add start` - Start the service
- `add stop` - Stop the service
- `add restart` - Restart the service
- `add enable` - Enable the service
- `add disable` - Disable the service

Viewing the service

To show the current active directory service details:

```
show service add
```

Adaptive Response

You can use the **`adaptive`** command to specify rules based on data transfer which dynamically populate Network Objects. These Dynamic Network Objects may then be used when configuring Optimizer Policies.

This functionality allows the system administrator to create policies which automatically restrict a user’s bandwidth once a set transfer limit has been exceeded within a specified period of time. Users are identified by IP address.

Configuring adaptive response settings

```
adaptive {clear|update-time|limit}
```

To reset Adaptive Response network objects and clear all IPs from destination network objects:

```
adaptive clear
```

To specify the frequency in which the adaptive response evaluates the rules:

```
adaptive update-time <seconds>
```

- `update-time <seconds>` - The duration in seconds between rule evaluation processing. By default, Adaptive Response evaluates rules every 5 minutes and adds or deletes IP addresses to dynamic network objects according to the defined rules.

To specify the transfer limit for the adaptive response rules:

```
adaptive limit <name> {alert|amount|direction|duration|enable|except|network-object|time-
allotment}
```

- `<name>` - The name of the adaptive response rule.
- `alert <percent>` - Configure an alert to be sent when the transferred traffic is a particular percentage of the defined limit.
- `amount <quota>` - Specify the quota (limit) amount in MB.
- `time-allotment <minutes>` - Specify the quota (limit) amount in minutes.
- `direction {both|inbound|outbound}` - Specify the direction used when calculating the quota.
- `duration {daily|weekly|monthly}` - Specify the period for the quota calculation. After the duration, the quota resets.
- `enable` - Enable this named adaptive response object.
- `except network-object {internal|external} <network object name>` - Specify a network object to be excluded from the adaptive response limit calculation. The network is specified as either internal or external. The network object is specified by name.
- `network-object source <src> destination <dst>` - Specify a source network object to use as a list of users for whom to apply to quota. This can be a static network object (such as a subnet) or dynamic network object (such as an Active Directory group). Specify a name for the dynamic network object that will be created, which will hold the list of users that have exceeded their quota.

EXAMPLE

Monitor traffic in the Shoppers network object. Once they have used 40 MB or 2 hours, whichever is first, then they are moved to the Shoppers-Over-Quota network object. Consider this a daily limit. That is, they can come back tomorrow and use the network again.

adaptive limit shopper-wifi-access amount 40

adaptive limit shopper-wifi-access time-allotment 120

adaptive limit shopper-wifi-access duration daily

adaptive limit shopper-wifi-access network-object source Shoppers destination Shoppers-Over-Quota

adaptive limit shopper-wifi-access direction both

adaptive limit shopper-wifi-access enable

Viewing the adaptive response configuration

To show the adaptive response service status:

```
show service adaptive
```

Alarms

You can use the **stats** command to configure alarms. Alarms are used to notify the administrator when certain thresholds are reached.

Configuring alarms

```
stats {alarm|chd|clear-all|export|sample}
```

To configure alarms based on sampled or computed statistics:

```
stats alarm {asymmetric_route|auto_neg|bridge_direction|bridge_link|cifs_signed|

concurrent_accel|cpu_util_indiv|diag|disk_io|exinda_connlimit|exinda_cpu_indiv|

exinda_paging|fs_mnt|if_collisions|intf_util|mapi_encrypted|memory_pct_used|pagign|

redundant_power|redundant_storage|rx_dropped|rx_errors|startup|tx_errors}
```

EXAMPLE

Enable the interface errors alarm.

```
stats alarm if_collisions enable
```

To configure computed historical data points:

```
stats chd
```

EXAMPLE

Enable the calculations of 5-minute web reduction samples

```
stats chd web_reduction_fiveminutes enable
```

To clear data for all samples and CHDs, and status for all alarms:

```
stats clear-all
```

To export statistics to a file:

```
stats export csv {cpu_util|exinda_cpu|memory|paging} {after|before|filename}
```

- `cpu_util` - Export the CPU utilization of the appliance
- `exinda_cpu` - Export the CPU utilization of the appliance
- `memory` - Export the memory utilization of the appliance
- `paging` - Export the paging data of the appliance
- `after <yyyy>/<mm>/<dd>` - Export only statistics collected after the specified date

- `before <yyyy>/<mm>/<dd>` - Export only statistics collected before the specified date
- `filename <filename>` - Specify the filename for the exported data

To configure sampled statistics:

```
stats sample
```

EXAMPLE

Configure the QoS sample interval to 120 seconds

```
stats sample qos interval 120
```

Anonymous Proxy

You can use the **`anonymous-proxy`** command to manage the anonymous proxy settings.

Configuring Anonymous Proxy

```
anonymous-proxy {enable|renumerate|url}
```

To enable fetching of anonymous proxy updates:

```
[no] anonymous-proxy enable
```

To refetch the entire list of anonymous proxy IDs:

```
anonymous-proxy renumerate
```

To set the url of where to fetch the anonymous proxy list:

```
anonymous-proxy url <url>
```

Viewing Anonymous Proxy Details

To view the anonymous proxy details:

```
show anonymous-proxy

Anonymous Proxy Detection

URL: http://updates.exinda.com/aplist.alist.gz

Last Check: 2014/07/18 20:26:16

Last Update: 2014/07/18 20:19:02

Last Status: success: downloaded proxy list

Enabled: yes
```

APM

You can use the **apm** command to create, modify or remove an Application Performance Metric (APM) object. An APM object measures a single metric of an application which traversing the network.

Configuring APM

EXAMPLE

```
apm <name> {metric|network-object|alert|threshold|delay}
```

To create a new apm object for a specified application:

```
apm <name>

        metric {normalized-network-delay|normalized-server-delay|network-delay|

        server-delay|round-trip-time|transaction-delay|

        normalized-transaction-delay|bytes-lost|tcp-connections-started|

        tcp-connections-aborted|tcp-connections-ignored|tcp-connections-refused}

        application <application>
```

- `<name>` - The name of your newly created APM object.
- `<application>` - The application that the APM object should monitor.
- `metric network-delay` - The time taken for data to traverse the network.
- `metric server-delay` - The time taken for a server to respond to a request.
- `metric transaction-delay` - The total delay time for a transaction (network delay + server delay).
- `metric normalized-network-delay` - The time taken for data to traverse the network when you consider a normalized packet size, which by default is 1024 bytes.
- `metric normalized-server-delay` - The time taken for a server to respond to a request when you consider a normalized packet size.
- `metric normalized-transaction-delay` - The total delay time for a transaction when you consider a normalized packet size.
- `metric round-trip-time` - The time taken for a packet to travel from a device, cross the network, and return.
- `metric bytes-lost` - The number of bytes lost due to retransmissions.
- `metric tcp-connections-started` - The number of TCP connections initiated.

- `metric tcp-connections-aborted` - The number of connections that were aborted. The connection is reset after being established. RST from client or server.
- `metric tcp-connections-ignored` - The number of connections that expired in the SYN-SENT state and no response was received from the server. Therefore the connection was not established.
- `metric tcp-connections-refused` - The number of connections that were reset while in the SYN-SENT state, that is, before the connection was established.

To specify an internal or external Network Object to filter the traffic when calculating the application performance:

```
apm <name> network-object {internal|external} <network-object-name>
```

- `internal` - Use the named network object that is marked as internal.
- `external` - Use the named network object that is marked as external.
- `<network-object-name>` - The name of the network object to use as the filter.

To enable or disable a configured alert when the metric rises above a configured threshold for a specified delay:

```
[no] apm <name> alert enable
```

To specify the threshold that will trigger the named alert:

```
apm <name> threshold <value>
```

- `<value>` - When the calculated APM value exceeds and continues to exceed this threshold value for the duration specified by the apm <name> delay command, the alert will be triggered, assuming the alert is enabled.

To specify the delay before triggering the alert, that is the duration that the apm value must exceed the threshold before triggering the alert:

```
apm <name> delay {60, 300, 1800, 3600, 86400}
```

To use a normalized packet size for all apm calculations:

```
monitor apm transaction normalize <value>
```

- `<value>` - When packet sizes are variable, it may help to normalize the packet sizes for more accurate comparisons. The normalize value specifies the number of bytes used to normalize the calculation of the normalized delays. The default vlaue is 1024. The maximum values is 1048576.

To disable the normalization calculations:

```
monitor apm transaction normalize 0
```

Application Groups

You can use the **`application-group`** command to create a new application group.

Configuring Application Groups

```
[no] application-group <application-group-name> {application|monitor}

application-group <application-group-name> clear
```

To create an application group or add or remove an application to the application group:

```
[no] application-group <application-group-name> application {application-name}
```

- `application {application-name}` - When creating an application group, you must specify an application to go in the group. By calling this command for an existing application group name, the specifiedapplication will be added (or removed) from the application group.

To enable or disable monitoring of an application group:

```
[no] application-group <application-group-name> monitor
```

To clear all configuration from an application group, which will leave the application group object with no applications specified within it:

```
application-group <application-group-name> clear
```

EXAMPLE

Create an application group called 'Web' and add some applications to it.

```
application-group Web application http
application-group Web application https
application-group Web application http-ALT
application-group Web application squidproxy
```

Applications

You can use the **`application`** command to create a new application definition.

Configuring Applications

```
[no] application <application name> {network-object|port|portrange|protocol-
only|signature}
```

To create an application by network object or to remove the network object from the application definition:

```
[no] application <application name> network-object <network-object-name>
```

- `network-object <network_object_name>` - Define the application by network object.

To create an application by port number and protocol (or to remove the port number and protocol from the application definition):

```
[no] application <application-name> [network-object <network-object-name>] port <port
number> protocol {protocol}
```

- `port <port-number>` - Define the application by a particular port number.
- `protocol {protocol}` - Define the application by protocol. e.g. 6in4, ah, egp, esp, ggp, gre, icmp, icmpv6, igmp, igp, ip, ipencap, ipip, ospf, pup, sctp, st, tcp, udp, vrrp
- `network-object <network-object-name>` - Can be optionally specified.

To create an application by port range and protocol (or to remove the port range and protocol from the application definition:

```
[no] application <application-name> [network-object <network-object-name>] portrange <port_
number_low> <port_number_high> protocol {protocol}
```

- `network-object <network-object-name>` - Can be optionally specified.

To create an application by only specifying a protocol (or to remove the protocol only setting from the application definition):

```
[no] application <application-name> protocol-only {protocol}
```

To create an application using an L7 application signature (or to remove the L7 signature from the application definition):

```
[no] application <application-name> signature <l7_signature> [signature_options]
```

- `signature <l7_signature>` - Specify a L7 signature that the appliance can recognize. Type application <application-name> signature ? to get a list of L7 signatures that the appliance can recognize.
- `[signature_options]` - Some of the L7 signatures have optional settings.

To remove all configuration for a specified application:

```
application <application name> clear
```

To remove an application:

```
no application <application-name>
```

Example: Define an application called FTP that uses TCP ports 20 and 21 with the L7 signature, ftp.

```
application FTP portrange 20 21 protocol tcp
application FTP signature ftp
```

Viewing Application Definitions

To view an application's definition:

```
show application <application-name>
```

APS

You can use the **aps** command to create and manage Application Performance Score (APS) objects. You can baseline the application traffic is automatically set the metric thresholds. You can also create an alert to notify you when an APS score drops below a configurable threshold.

Configuring Application Performance Score Objects

```
aps <name> {application|network-object|non-trans-protocol}
```

To create a new aps object for a specified application:

```
aps <name> application <application>
```

To delete an aps object:

```
no aps <name>
```

To filter the traffic that will be included in the aps calculation to a specific subnet or application server:

```
aps <name> network-object {internal|external} <network-object-name>
```

- `<network-object-name>` - The name of a defined network object.
- `internal` - Use the named network object that is marked as internal.
- `external` - Use the named network object that is marked as external.

To specify whether application is a transactional or non-transactional protocol:

```
[no] aps <name> non-trans-protocol
```

EXAMPLE

Protocols that send information between the client and server at arbitrary times (non-transactional), such as Citrix XenApp servers and Microsoft Remote Desktop

To set the APS thresholds

There are several metrics that can be used in the application performance score calculation. Thresholds for at least one of these metrics must be set, as the score is calculated by comparing the observed traffic to the set threshold. You can either have the system calculate thresholds based on observed traffic, or you can manually set your desired thresholds.

```
aps <name> {baseline|metric}
```

To specify the length of time for used for the baseline:

```
aps <name> baseline period <seconds>
```

- `period <seconds>` - Acceptable values are 3600 seconds (1 hour), 86400 seconds (1 day), 604800 seconds (1 week).

To start or stop the baselining operation for an aps:

```
[no] aps <name> baseline enable
```

To set the aps metric threshold values:

```
aps <name> metric {network-delay|network-jitter|network-loss|norm-network-delay|norm-server-
delay|round-trip-time|server-delay} threshold <value>
```

- `network-delay threshold <duration (ms)>` - Set the network delay threshold (ms)
- `network-jitter threshold <duration (ms)>` - Set the network-jitter threshold (ms)
- `network-loss threshold <percent>` - Set the network loss threshold in percentage. This is the amount of retransmitted packets (inbound or outbound)
- `norm-network-delay threshold <duration (ms/kb)>` - Set the normalized network delay threshold (ms/kb)
- `norm-server-delay threshold <duration (ms/kb)>` - Set the normalized server delay threshold (ms)
- `round-trip-time threshold <duration (ms)>` - Set the round trip time threshold (ms)

Configuring APS alerts

Alerts can be created (as SNMP or E-Mail) that will trigger when the aps value falls below a configured value for a specified duration. For example, if the application performance score drops below 7 and stays below 7 for 30 minutes, send an alert.

```
aps <name> alert {threshold|delay|enable}
```

To set the threshold at which the alarm should trigger.

```
aps <name> alert threshold <aps-threshold>
```

- `threshold <aps-threshold>` - This is a value in the range [0-10].

To set the duration (in seconds) for which the aps value needs to remain below the set threshold before the alert is triggered:

```
aps <name> alert delay {60,300,1800,3600,86400}
```

- `delay {60,300,1800,3600,86400}` - The values are in seconds (1 minute, 5 minutes, 30 minutes, 1 hour, and 1 day).

To enable or disable the alarm:

```
[no] aps <name> alert enable
```

Viewing APS alerts

To show all aps objects:

```
show aps
```

To show details of a specific aps object:

```
show aps <name>
```

Windows Authentication

You can use the **`windows authentication`** command to configure local user accounts.

Configuring windows authentication settings

```
[no] windows authentication credentials <domain-name> {username|password|enable}
```

To add or remove the domain:

```
[no] windows authentication credentials <domain-name>
```

To add or remove the username & pasword for logging in to the domain:

```
[no] windows authentication credentials <domain-name> {username|password}
```

- `username <username>` - Set the username for the specified domain
- `password <password>` - Set the password for the specified domain

To enable or disable the Windows authentication credentials.

```
[no] windows authentication credentials <domain-name> enable
```

Bridge

You can use the **`bridge`** command to enable or disable bridges. The interfaces available for a bridge are determined by the appliance model and installed expansion cards. Once enabled, an interface is created for the bridge which can used in other commands (e.g., "interface")

Configuring a Bridge

```
[no] bridge <bridge> {ageing-time|forward-time|hello-time|max-age|mq|priority|spanning-
tree|enable}
```

To enable or disable the specified bridge.

```
[no] bridge <bridge> enable
```

To specify the ageing time for this bridge:

```
bridge <bridge> ageing-time <ageing-time>
```

To specify the forwarding time for this bridge:

```
bridge <bridge> forward-time <forward time>
```

To specify the hello time for this bridge:

```
bridge <bridge> hello-time <hello time>
```

To specify the max age for this bridge:

```
bridge <bridge> max-age <max age>
```

To specify the priority for this bridge:

```
bridge <bridge> priority <priority>
```

To enable or disable the Spanning Tree Protocol for this bridge:

```
[no] bridge <bridge> spanning-tree enable
```

To set the bridge interface to provide QoS based on queue mode:

```
bridge <bridge-name> mq mode [auto-license|multi|single]
```

- `mq mode auto-license`—Single- or multi-queue is automatically selected based on the license.
- `mq mode multi`—QoS uses a multi-queue network interface configuration.
- `mq mode single`—QoS uses a single-queue network interface configuration.

To specify the bandwidth at which the bridge auto-license mode switches from single-queue to multi-queue:

```
bridge <bridge-name> mq switch-bandwidth <bandwidth>
```

Viewing Bridge Configuration

To show current bridge configuration use the following command:

```
show bridges
```

Bypass

You can use the **`bypass`** command to indicate which bridge mode you want during normal operations and following a failure. During a failure, the appliance can stop traffic as if the ethernet cables are not connected, or the appliance can fail-to-wire where the traffic passes through the box unaffected and unmonitored.

Configuring Bypass Settings

```
bypass bridge {all|<bridge_name>} {auto-failover|running|failure}
```

To set the bypass mode when in the running (non-failure) state:

```
bypass bridge {all|<bridge-name>} running {active|bypass|no-link}
```

- `running active` - Active or normal operation.
- `running bypass` - Bypass or fail-to-wire mode.

- `running no-link` - No link mode where the ethernet cables are disconnected.

To set the bypass mode for the failure state. Bypass pairs can be placed into either bypass (fail-to-wire) or no-link (ethernet cables disconnected) state.

```
bypass bridge {all|<bridge-name>} failure {bypass|no-link}
```

- `failure bypass` - Bypass or fail-to-wire mode.
- `failure no-link` - No link mode where the ethernet cables are disconnected.

> **NOTE**
>
> ***Depending on the hardware appliance and the type of interface cards installed, fail to wire or bypass settings may be configured globally or per bridge. Not all bypass options are available on all hardware.***

To configure the bypass settings to automatically failover to the failure settings in the event of a failure or to remove auto-failover:

```
[no] bypass bridge {all|<bridge_name>} auto-failover
```

Configuring Watchdog Auto-reboot

To enable or disable the system watchdog. The watchdog will reboot the Exinda appliance in the event of failure:

```
[no] watchdog enable
```

Certificates and Keys

You can use the **`crypto`** command to import keys and certificates.

Configuring Certificates and Keys

```
crypto certificate [generate|import|setkey]

crypto key import
```

To import a certificate or key in PEM format:

```
crypto {certificate|key} import <name> pem data "<pem-data>"
```

- `import <name>` - The name of the certificate or key.
- `pem data <pem-data>` - The PEM data. Ensure to quote the PEM data.

To generate a self-signed certificate:

```
crypto certificate generate self-signed <cert-name> instance {<instance-name>|exinda-
autogen}
```

To assign a key to a certificate:

```
crypto certificate setkey <certificate_name> {key|test}
```

Clustering and HA

You can use the **cluster** command to configure clustering.

Configure the Interface for the Cluster Service

```
cluster {interface|master|sync}
```

To configure a cluster internal or external address:

```
cluster interface <inf>
```

- Any interface not bound to a bridge or used in another role (e.g. Mirror or WCCP) may be used. This command will need to be run on each node in the cluster, and each with a unique cluster internal address.

```
cluster interface <inf> ip address <address> <netmask>
```

- This command should also be executed on all cluster nodes, using the same cluster external address.

To configure the master cluster:

```
cluster master interface <inf>
```

```
cluster master address vip <address> <netmask>
```

- The role of the node (master or slave) is shown in the CLI prompt. Once the cluster is up, configuration changes should only be made on the cluster master. Configuration changes made on the master will be sent to slave nodes.

To control how data is synchronized between cluster members:

```
[no] cluster sync {all|acceleration|monitor|optimizer|compression}
```

- `sync all` - Acceleration, monitor and optimizer data are synchronized. This is disabled by default.
- `sync acceleration`- Synchronize acceleration data only
- `sync acceleration redirect-only` - Do not accelerate any connections; only perform monitoring
- `sync monitor` - Synchronize monitor data only
- `sync optimizer` - Synchronize optimizer data only
- `sync compression` - Configure cluster compressions settings
- `sync compression threshold` - Set the size of the data block that will trigger compression
- `sync compression threshold <value>` - Set the compression value (default is 2048)

- `sync compression zip` - Enable zip compression between cluster nodes
- `sync compression zip level <value>`- Set the zip compression level, where 1 is the fastest, largest compressed block and 9 is the slowest, smallest compressed block and best compression. When zip compression is enabled, the level value defaults to 9 until changed. Note that the larger compression block requires less bandwidth, but results in smaller blocks and requires more CPU power.

Viewing cluster configuration and status

To show a brief overview of the current cluster configuration:

```
show cluster global brief
```

To show cluster sync status information:

```
show cluster sync {acceleration|optimizer|monitor|compression}
```

- `sync acceleration`- Show acceleration sync status
- `sync redirect-only` - Synchronize redirect data only
- `sync monitor` - Synchronize monitor data only
- `sync optimizer` - Synchronize optimizer data only
- `sync compression` - Show cluster compression information

To display all the appliances in the cluster:

```
show appliances
```

Community

Use the **`community`** command to configure Exinda appliance community settings. An Exinda Community is a collection of Exinda appliances in a user’s network. Appliances that are part of the same community can accelerate to/from each other. Exinda appliances can automatically discover other appliances in its community.

Configure the Exinda community

```
community {compatibility|delete-db|group|node}
```

To configure the community group that this appliance belongs to:

```
community group <number>
```

To manually add remote appliances to the community group:

```
community node <name> address <address> port <port>
```

- `node <name>` — The name of the remote node (e.g. hostname)
- `address <address>` — The IPv4 address of the remote appliance

- `port <port>` — The port to connect to.

To delete the cache of other community members that this node remembers:

```
community delete-db
```

To enable backward compatibility to allow appliances running ExOS version 6.4.0 and earlier in the same community:

```
community compatibility pre-v6.4.0 enable
```

- Backward compatibility is enabled by default.

Configuration

Use the **`configuration`** command to manipulate the configuration database, ushc as backup, copy, merge, and view system configuration.

Configure the Exinda community

```
configuration {copy|delete|fetch|jump-start|merge|move|new|revert|rename|switch-
to|text|upload|write}
```

To copy, move, or delete a configuration file:

```
configuration {copy|delete|move}
```

- `copy <source-filename> <destination-filename>` - Copies the file from the source-filename to the destination-filename
- `delete <filename>` - Deletes the filename
- `move <source-filename> <destination-filename>` - Moves the file from the source-filename to the destination-filename

To download a configuration file or a text-based configuration file from a remote host:

```
configuration [text] fetch <url or scp://username:password@hostname/path/filename>
```

- `fetch <url or SCP>` - Fetch the file from the specified location
- `text fetch <url or SCP>`- Fetch the text-based file

To upload a configuration file to a remote host:

```
configuration upload {active|<filename>} <URL or
scp://username:password@hostname/path/filename>
```

- `upload active <url or scp>` - Upload the activve configuration file to a remote host
- `upload <filename> <url or scp>` - Upload a configuration file to a remote host

To re-run the initial configuration wizard:

```
configuration jump-start
```

To modify the active running configuration

```
configuration {merge|revert|switch-to}
```

- `merge <filename>` - Merges the common settings from a given configuration file into the running configuration
- `revert saved` - Reverts the running configuration to the last saved configuration
- `switch-to <filename>` - Loads a configuration file and makes it the active configuration

To create a new configuration file, specifying optional factory default options:

```
configuration new <filename> factory {keep-basic | keep-connect}
```

- `factory` - Create a new file with only factory defaults
- `factory keep-basic` - Keep licenses and host keys
- `factory keep-connect` - Keep configuration necessary for connectivity (interfaces, routes, and ARP)

To generate a new text-based configuration file from this systems configuration:

```
configuration text generate {active | file <filename>}
```

To save the running configuration:

```
configuration write {local|to <filename>}
```

- `write` - Saves the running configuration (same as 'write memory')
- `write local` - Saves the running configuration locally (same as 'write memory local')
- `write to <filename>` - Saves the running configuration to a new file under a different name

To manipulate a stored text-based configuration file:

```
configuration text file <filename> {apply|delete|rename|upload}
```

- `apply {fail-continue} {verbose}`
  - Executes the commands in the specified file; shows only error output and stops on first error
  - `fail-continue` - Continues execution even if one command fails
  - `verbose` - Displays all the commands being executed and their output, instead of just those that have errors
- `delete` - Deletes the specified file
- `rename <filename>` - Changes the name of the specified file
- `upload <upload-url>` - Uploads the file to a remote host

Viewing configuration file details

```
show configuration {files|full|running|text}
```

To display the contents of a configuration file:

```
show configuration {files|full|running}
```

- `configuration` - Shows the contents of the currently active configuration file
- `configuration files <filename>` - Shows the contents of the named file
- `configuration running [full]` - Shows the contents of the currently running configuration file
- `full` - Does not exclude commands that set default values

To display names of available configuration files with status:

```
show configuration [text] files
```

- `files` - Shows the list of available configuration files
- `text files` - Shows the list of available text-based configuration files

crypto

You can use the **`crypto`** command to import keys and certificates.

Managing keys and certificates

```
crypto {certificate|key}
```

To import a certificate or key in PEM format:

```
crypto {certificate|key} import <name> pem data "<pem-data>"
```

- `import <name>` - The name of the certificate or key.
- `pem data <pem-data>` - The PEM data. Ensure to quote the PEM data.

To generate a self-signed certificate:

```
crypto certificate generate self-signed <cert-name> instance {<instance-name>|exinda-
autogen}
```

To assign a key to a certificate:

```
crypto certificate setkey <certificate_name> {key|test}
```

CSV Reports

You can use the **`report csv`** command to configure CSV reports.

Configuring CSV reports

```
report csv <name> {basic flows|frequency {on-demand|scheduled}|email}
```

To enable reporting of flow records:

```
report csv <name> basic flows
```

- `flows` - Only flows are currently supported for csv files.

To configure the on-demand or scheduled frequency for the csv report:

```
report csv <name> frequency scheduled {daily|weekly|monthly}
```

```
report csv <name> frequency on-demand {last_60_minutes|last_24_hours|last_7_days|last_30_
days|last_12_months|current_hour|today|this_week|this_month|this_year|last_
hour|yesterday|last_week|last_month|last_year}
```

> **NOTE**
>
> *CSV reports cannot be scheduled to generate hourly.*

To set the e-mail address that the scheduled csv should be e-mailed:

```
report csv <name> email <email address>
```

- `email <email-address>` - Specify the e-mail address. Optional for on-demand CSV reports.

To remove the configured csv report:

```
no report csv <name>
```

EXAMPLE

Create a daily CSV export that e-mails yesterday's CSV flows to test@exinda.com.

```
report csv CSV_1
report csv CSV_1 basic flows
report csv CSV_1 email test@exinda.com
report csv CSV_1 frequency scheduled daily
```

Debug

You can use the `debug` command to generate diagnostic dumps and captures. Generated files will be available for download on the Web UI. Then you can use the `file` command to delete, upload, or e-mail it.

Generating diagnostics files

```
debug generate {capture {interface|filter|timeout} | dump}
```

To delete a tcpdump file:

```
file tcpdump delete <file-name>
```

To generate a packet capture diagnostic file:

```
debug generate capture {interface|filter|timeout}
```

- `interface <interface-name>` - Select an interface to run the TCP dump on. E.g. br1, eth1, or ALL. Note that when you select ALL for the Interface, only those interfaces which are link up are included.
- `timeout <duration>` - Specify the duration (in seconds) that the capture should run.
- `filter` - Specify a filter to apply to the capture. More information on tcpdump filters is available at www.tcpdump.org

To generate a sysdump diagnostic file :

```
debug generate dump
```

Manipulating diagnostics files

```
file debug-dump {delete|email|upload}

file tcpdump {delete|upload}
```

To delete a diagnostic dump file:

```
file debug-dump delete <file-name>
```

To e-mail a diagnostic dump file:

```
file debug-dump email <file-name>
```

To upload a diagnostic dump file:

```
file debug-dump upload <file-name> <upload-url>
```

To delete a tcpdump file:

```
file tcpdump delete <file-name>
```

To upload a tcpdump file:

```
file tcpdump upload <file-name> <upload-url>
```

EXAMPLE

Capture 5 seconds of traffic on Bridge br10, then upload to a server via scp

```
> debug generate capture interface br10 timeout 5

Starting capture... (Press ctrl-c to end capture)

Stopping capture... Generated capture file: capture-exinda-hq-20110405-055920.tar.gz

> file tcpdump upload capture-exinda-hq-20110405-055920.tar.gz \

scp://admin@foo.com/tcpdumps
```

Email

You can use the **`email`** command to configure email settings.

Configuring email settings

```
email {auth|autosupport|dead-letter|diag-max-size|domain|mailhub|mailhub-
port|notify|return-addr|return-host|send-test}
```

To configure authentication options for sending email:

```
email auth {enable|password|username}
```

- `enable` - Enable authentication for sending email
- `password <password>` - Set password to use in SMTP authentication
- `username <username>` - Set username to use in SMTP authentication
- `ssl enable` - Set use of Secure Sockets Layer (SSL) for SMTP authentication
- `starttls enable` - Set the use of the advanced SSL option of using STARTTLS

To set handling of automatic support email:

```
email autosupport {enable|event}
```

- `enable` - Send automatic support notifications via email
- `event <event-type>` - Specify which events will trigger sending autosupport notification emails, e.g. cpu-util-high

To configure settings for saving undeliverable emails:

```
email dead-letter {enable|cleanup}
```

- `enable` - Enable saving undeliverable emails
- `cleanup max-age <duration>` - Delete any dead.letter files older than the specified age. The age format is: #d#h#m#s. For example, 1d2h3m4s or 3d.

To set the maximum attachment size for diagnostic emails:

```
email diag-max-size <size-in-MB>
```

To override the domain from which emails appear to come:

```
email domain <hostname-or-IP-address>
```

To set the mail relay to be used to send emails:

```
email mailhub <hostname-or-IP-address>
```

To set mail port to be used to send emails:

```
email mailhub-port <port-number>
```

To set handling of events and failures via email:

© 2016 Exinda Networks Inc.

```
email notify {event|recipient}
```

- `event <event-type>` - Specify which events will trigger sending notification emails, e.g. APM
- `recipient <email-address> class {failure|info}` - Specify which email addresses will receive email notifications upon a failure event or an informational event
- `recipient <email-address> detail` - Specify that the email notifications sent to the email addresses will be in the detailed format

To set the username in the return address of the email notifications:

```
email return-addr <username>
```

To include a hostname in the return address of the email notifications:

```
email return-host
```

To send a test email to all configured event and failure recipients:

```
email send-test
```

Factory Default

You can use the **`factory default`** command to restore settings to the factory defaults.

Restoring to factory default

```
factory default [keep-basic] [keep-connect] [keep-monitor]
```

To restore your appliance to factory defaults:

```
factory default [keep-basic] [keep-connect] [keep-monitor]
```

- `keep-basic` - Restores to factory defaults and preserves basic configurations.
- `keep-connect` - Restores to factory defaults and preserves connectivity.
- `keep-monitor` - Restores to factory defaults and preserves monitoring data.

> **NOTE**
>
> ***Network settings will be preserved.***

Firmware Update

You can use the **`image`** command to manage firmware updates.

Managing firmware images

```
image {fetch|install|delete|boot|move}
```

To download a system image from a remote host:

```
image fetch <download-URL> [{original|filename}]
```

- `<download-URL>` - URL or scp://username:password@hostname/path/filename
- `original` - Keep the same file name that the image had on the server
- `filename <filename>` - The name that the image will be saved with locally
- Without specifying original or filename, the image will be stored as webui.img.

To install an image file onto a system partition:

```
image install <image-filename> [location][progress][verify]
```

- `location <partition-number>` - The location in which to install the image specified as a partition number
- `progress {track|no-track}` - Show the install progress or not
- `verify {check-sig|ignore-sig|require-sig}` - Verify the image before installing
  - `check-sig` - Require the image to have a valid signature or no signature
  - `ignore-sig` - Ignore missing or invalid signature
  - `require-sig` - Require the image to have a valid signature installed

NOTE

A reboot is required after the installation is complete.

To delete an inactive system image from the hard disk:

```
image delete <image-filename>
```

To configure from where the appliance will boot from when re-booted:

```
image boot {location <partition-number>|next}
```

- `location <partition-number>` - Specify the partition to boot from
- `next` - Specify to boot from the partition following the current partition

```
no image boot next
```

To move or rename an inactive system image on the hard disk:

```
image move <src-image-filename> <dst-image-filename>
```

- `<src-image-filename>` - Name of the image to move or rename
- `<dst-image-filename>` - New name to give the image

© 2016 Exinda Networks Inc.

Hostname

You can use the **hostname** command to set the appliance's host name.

Configuring Hostname

```
hostname <hostname>
```

To configure the appliances host name:

```
hostname <hostname>
```

EXAMPLE

Set the host name of this appliance to "exinda_1".

```
hostname exinda_1
```

Interface

You can use the **interface** command to configure the interface address and other IP networking settings.

NOTE

- ***To set global IP network settings (e.g. default gateway) use the "ip" command.***
- ***To configure a role for an interface (e.g. Cluster, Mirror or WCCP) use associated role command (cluster, mirror or wccp)***
- ***To configure bridge settings, use the "bridge" command.***

Configuring Interface address

```
interface <inf> ip address

interface <inf> ipv6 {address|enable}

interface <inf> {dhcp|alias|comment|duplex|speed|mtu|shutdown}
```

To add or remove an IPv4 address and netmask for the specified interface.

```
[no] interface <inf> ip address <IPv4 addr> <netmask>
```

- `netmask` - Specify the netmaks as dotted quad format (e.g. 255.255.255.0) or as a netmask length after a slash (e.g. /24)

To enable IPv6 on the specified interface:

```
[no] interface <inf> ipv6 enable
```

To add or remove an IPv6 address for the specified interface:

```
[no] interface <inf> ipv6 address <IPv6 addr>/<len>
```

- `<IPv6 addr>/<len>` - e.g. 2001:db8:1234::5678/64

To enable IPv6 stateless address autoconfiguration (SLAAC) on the specified interface:

```
[no] interface <inf> ipv6 address autoconfig [default | privacy]
```

- `default` - Enables learning default routes
- `privacy` - Enabled autoconfiguration privacy extensions

To enable DHCP on the specified interface:

```
interface <inf> dhcp
```

To renew DHCP on the specified interface:

```
interface <inf> dhcp renew
```

To configure an IPv4 alias on the specified interface:

```
interface <inf> alias <alias index> ip <IPv4 addr>
```

To add a comment to the specified interface:

```
interface <inf> comment <comment>
```

To configure the duplex of the specified interface:

```
interface <inf> duplex {half|full|auto}
```

To configure the speed of this interface:

```
interface <inf> speed {10|100|1000|auto}
```

EXAMPLE

Set the speed and duplex interface settings for eth2.

```
interface eth2 speed 100

interface eth2 duplex full
```

To configure the MTU of this interface:

```
interface <inf> mtu <mtu>
```

To disable the specified interface:

```
interface <inf> shutdown
```

Viewing interface running state and configuration

To display information about the running state for the interfaces:

```
show interfaces [<inf>] [brief]
```

- `<inf>` - Optionally, indication that you want information for a single interface; otherwise information for all interfaces will be shown
- `brief` - Optionally, indicate that you want brief details; otherwise the information will be detailed.

To display the current configuration for all interfaces:

```
show interfaces configured
```

To display a summary of the running state for all interfaces, including bridge and role information:

```
show interfaces summary
```

IP

You can use the **`ip`** command to configure IP network settings.

NOTE

- ***To configure interface specific settings (e.g. address or spedd/duplex/mtu), use the "interface" command.***
- ***To configure the IPv6 settings, use the "ipv6" command.***

Configuring IP network settings

To configure a default IPv4 gateway:

```
ip default-gateway {<IPv4 address>|<interface>}
```

- `<IPv4 address>` - Set the next hop IP address
- `<interface>` - Set the interface name

To configure a DNS server:

```
ip name-server <IPv4 or IPv6 address>
```

To configure the kernel neighbour table size:

```
ip neighbour size <size>
```

To ensure a static host mapping for the current hostname:

```
ip map-hostname
```

To add a domain name to use when resolving hostnames:

```
ip domain-list <domain-name>
```

To add a static IPv4 route:

```
ip route <network-prefix> [{<netmask>|<mask-length>} <next hop IP address or interface name>
```

- `<network-prefix>` - IP address
- `<netmask>` - e.g. 255.255.255.0
- `<mask-length>` - e.g. /24

To configure global DHCP settings:

```
ip dhcp {default-gateway|hostname|primary-intf|send-hostname}
```

- `dhcp default-gateway yield-to-static` - Configure DHCP settings for the default gateway. Do not install a default gateway from DHCP if there is already a statically configured one.
- `dhcp hostname <homename>` - Specify the hostname to be sent durign DHCP client negotiation (if send-hostname is enabled)
- `dhcp primary-intf <interface-name>` - Set the interface from which non-interface-specific configuration (resolver and routes) will be accepted via DHCP
- `dhcp send-hostname` - Enable the DHCP client to send a hostname during negotiation

To configure netflow export, see Netflow.

```
ip flow-export
```

EXAMPLE

Configure eth1 with address 192.168.0.98 /24, gateway 192.168.0.1 and Bridge br1 enabled.

```
interface eth1 ip address 192.168.0.98 /24

ip default-gateway 192.168.0.1

bridge br1 enable
```

EXAMPLE

Enable IPv6 autoconfig (SLAAC) on interface eth1

```
interface eth1 ipv6 address autoconfig
```

EXAMPLE

Configure a DNS server

```
ip name-server 192.168.0.1
```

IPMI

You can use the **IPMI** command to configure access to the appliances baseboard management controller (BMC). When access is configured, an IPMI client may be used to remote power on/off the appliance, query sensors, and access the serial-over-lan console.

Configuring IPMI

```
ipmi {enable|ip|dhcp|username|sel|seltime|power}
```

To enable IPMI access:

```
[no] ipmi enable
```

To configure a static IPMI IPv4 adress or default gateway:

```
[no] ipmi ip address <IPv4 address> [<netmask>]
```

- `<netmask>` - A netmask can be specified in long (e.g. 255.255.254.0) or short (e.g /23) format. If no netmask is specified a default of /24 is used.

```
[no] ipmi ip default-gateway <IPv4 address>
```

To use DHCP to configure the IP address and default gateway:

```
[no] ipmi dhcp
```

To configure IPMI authentication:

```
[no] ipmi username <user> password <password>
```

To enable sending BMC System Event Log (SEL) events to the appliance log:

```
[no] ipmi sel enable
```

To set the SEL time to that of the appliance on startup:

```
[no] ipmi seltime enable
```

To control the power of a remote appliance which has enabled IPMI access as above:

```
ipmi power address <address> username <username> password <password> control
{on|off|cycle|reset|status}
```

- `on` - Power on the chassis
- `off` - Power off the chassis - no clean shutdown of the OS
- `cycle` - Power off for a minimum of 1 second, and then power on
- `reset` - Hard reset of the appliance
- `status` - Display the power status of the chassis

EXAMPLE

Enable the IPMI interface with 172.16.0.71 IP address and 255.255.254.0 netmask.

```
ipmi enable

ipmi ip address 172.16.0.71 255.255.254.0

ipmi ip default-gateway 172.16.1.254

ipmi username admin password exinda
```

© 2016 Exinda Networks Inc.

Viewing Configuration & Status

To show the current IPMI configuration:

```
show ipmi
```

To show the power status of a remote IPMI device:

```
show ipmi power <address> username <username> password <password>
```

IPv6

You can use the **ipv6** command to configure IPv6 specific settings.

Configuring IPv6 settings

```
ipv6 {enable|default-gateway|dhcp|route|host|map-hostname|neighbor}
```

To enable IPv6 for the entire system:

```
[no] ipv6 enable
```

To configure global DHCPv6 settings:

```
[no] ipv6 dhcp {primary-intf|stateless}
```

- `primary-intf <interface-name>` - Set the interface from which non-interface-specific (resolver) configuration will be accepted via DHCPv6
- `stateless` - Enable stateless DHCPv6 requests (i.e. Get only DNS configuration - not an IPv6 address)

To add an IPv6 default gateway:

```
[no] ipv6 default-gateway <IPv6 address or interface>
```

To add an IPv6 static route:

```
[no] ipv6 route <network prefix> <next hop IPv6 address or interface>
```

To add a static hostname/IPv6 address mapping:

```
[no] ipv6 host <hostname> <IPv6 address>
```

To add a static IPv6 hostname mapping for the current hostname:

```
[no] ipv6 map-hostname
```

To configure a static IPv6 neighbor MAC (link layer) address mapping:

```
[no] ipv6 neighbor <IPv6 address> <interface> <MAC address>
```

LDAP

You can use the **ldap** command to configure the Exinda appliance to authenticate user login attempts with a remote LDAP (including Active Directory) server.

Configuring LDAP settings

```
ldap {base-dn|bind-dn|bind-password|group-attribute|group-dn|host|login-
attribute|port|referrals|scope|ssl|timeout-bind|timeout-search|version}
```

To configure the LDAP user search base:

```
ldap base-dn <string>
```

To configure the distinguished name (DN) to bind to the server:

```
ldap bind-dn <string>
```

To specify the password for binding to the server:

```
ldap base-password <string>
```

To specify the name of the group membership attribute:

```
ldap group-attribute {<string>|member|uniqueMember}
```

- `group-attribute <string>` - Specify a custom attribute name
- `group-attribute member` - groupOfNames of group membership attribute
- `group-attribute uniqueMember` - groupOfUniqueNames membership attribute

To specify the distinguished name of the group required for authentication:

```
ldap group-dn <string>
```

To specify the hostname or IP address of the LDAP server:

```
ldap host <hostname or IP address>
```

- `host <hostname or IP address>` - IPv4 and IPv6 addresses can be used.

To specify the attribute that contains the login name:

```
ldap login-attribute {<string>|uid|sAMAccountName}
```

- `login-attribute <string>` - Specify a custom attribute name
- `login-attribute uid` - LDAP login name
- `login-attribute sAMAccountName` - Active Directory login name

To specify the port of the LDAP server:

```
ldap port
```

To enable LDAP referrals:

```
ldap referrals
```

To specify to scope of the LDAP search:

```
ldap scope {one-level|subtree}
```

- `scope one-level` - Search only the object's immediate children
- `scope subtree` - Search all descendants

To configure the SSL and TSL settings:

```
ldap ssl {cert-verify|mode {none|ssl|tls}|ssl-port}
```

- `ssl cert-verify` - Enable LDAP SSL/TLS certificate verification
- `ssl mode none` - Do not use SSL or TLS to secure LDAP
- `ssl mode ssl` - Secure LDAP using SSL over the SSL port
- `ssl mode tls` - Secure LDAP using TLS over the default server port
- `ssl ssl-port <port>` - Set the LDAP SSL port number

To specify the number of seconds before LDAP times out for binding to a server:

```
ldap timeout-bind <seconds>
```

To specify the number of seconds before a search for user information on the LDAP server times out:

```
ldap timeout-search <seconds>
```

To configure the version of LDAP that is supported:

```
ldap version {2|3}
```

- `version 2` - LDAP version 2 and earlier
- `version 3` - LDAP version 3 and current LDAP/Active Directory servers

License

You can use the **`license`** command to fetch, install, delete licenses and enable or disable the auto-licensing service.

Configuring a License

```
license {fetch|install|delete|auto|send-status}
```

To download and install the latest license key from the Exinda licensing server:

```
license fetch
```

To install a new license:

```
license install <license-key>
```

To delete an existing license:

```
license delete <license-id>
```

© 2016 Exinda Networks Inc.

- `<license-id>` - Licenses are identified by their ID which can be found with the "show licenses" command.

To enable or disable the auto-license feature:

```
[no] license auto enable
```

- `enable` - When enabled, the appliance will automatically fetch and install any new available licenses. It checks every 24 hours and is enabled by default.

To send WAN memory, Edge Cache disk and reduction statistics and optimizer status to the licensing server:

```
license send-status
```

Viewing Licenses

To show currently installed licenses:

```
show licences
```

Link State Mirroring

You can use the **`link-state`** command to configure link state mirroring. If link state mirroring is enabled, bridge port states will be synchronized. For example, if one port's link is down, the other port will be manually forced into the link down state. If link state mirroring is enabled, it applies to all bridge interfaces.

Configuring Link State Mirroring

```
ipmi {enable|ip|dhcp|username|sel|seltime|power}
```

To enable link state mirroring:

```
[no] link-state enable
```

To set the delay in ms before an interface is forced into the down state or is returned to the up state:

```
link-state {down-delay|up-delay} <duration_ms>
```

To show the current link state configuration:

```
show link-state
```

Logging

You can use the **`logging`** command to configure logging parameters and to show the system logs. You can use the **`show log`** command to view the logs files. The appliance logs activities to a set of system log files.

Configuring logging parameters

```
logging {files|local|receive|fields|format|level|trap|<hostname or IP-address>}
```

To specify when to rotate the log files:

```
logging files rotation {criteria {frequency|size|size-pct} | force}
```

- `rotation criteria frequency {daily|weekly|monthly}` - Rotate log files on a fixed schedule.
  - `daily` - Once per day at midnight.
  - `weekly` - Once per week
  - `monthly` - On the first day of every month
- `rotation criteria size <megabytes>` - Rotate the log files when the log file surpasses a specified size threshold.
- `rotation criteria size-pct <percentage>` - Rotate the logs when they surpass a specified percentage of the disk size.
- `rotation force` - Force an immediate rotation of the log files.

To specify the maximum number of old log files to keep:

```
logging files rotation max-num <number>
```

To delete log files:

```
logging files delete {current|oldest}
```

- `delete current` - Delete the current active log file
- `delete oldest [<number>]` - Delete one or more of the oldest log files. If deleting more than one file, specify the number of files to delete.

To specify the minimum severity level of log messages saved on the local disk:

```
logging local {none|emerg|alert|crit|err|}warning|notice|info|debug|override}
```

- `none` - Disable logging
- `emerg` - Emergency: system is unstable
- `alert` - Action must be taken immediately
- `crit` - Critical conditions
- `err` - Error conditions
- `warning` - Warning conditions

- `notice` - Normal but significant conditions
- `info` - Informational messages
- `debug` - Debug-level messages
- `override class <class> priority` - Override log levels on a per-class basis

To allow syslog messages to be received from remote hosts:

```
logging receive
```

To include the number of seconds since the epoch in the logs:

```
logging fields seconds {enable|fractional-digits|whole-digits}
```

- `seconds enable` - Enable the seconds field
- `seconds fractional-digits {1|2|3|6}` - Specify the number of digits to the right of the decimal point (truncation is from the right)
- `seconds whole-digits {1|6|all}` - Specify the number of digits the left of the decimal point (truncation is from the left)
  - `all` - Do not limit the number of digits.

To set the format of the log files:

```
logging format {standard|welf}
```

- `format standard` - Use the standard format for log messages
- `welf` - Use WELF format for log messages

To set the severity of log entries recorded for select CLI commands:

```
logging level cli commands {none|emerg|alert|crit|err|warning|notice|info|debug}
```

- `none` - Disable logging
- `emerg` - Emergency: system is unstable
- `alert` - Action must be taken immediately
- `crit` - Critical conditions
- `err` - Error conditions
- `warning` - Warning conditions
- `notice` - Normal but significant conditions
- `info` - Informational messages
- `debug` - Debug-level messages

To send event logs to a specified server using the syslog protocol:

```
logging <hostname or IPv4 address>
```

Set the minimum severity of log messages sent to syslog servers:

```
logging trap {none|emerg|alert|crit|err|warning|notice|info|debug}
```

- `none` - Disable logging
- `emerg` - Emergency: system is unstable

- `alert` - Action must be taken immediately
- `crit` - Critical conditions
- `err` - Error conditions
- `warning` - Warning conditions
- `notice` - Normal but significant conditions
- `info` - Informational messages
- `debug` - Debug-level messages

Viewing log files

To view the log file:

```
show log [continuous] {matching|not matchin} <regex>
```

- `show log` - Show entire log file
- `continuous` - Show the log file as it gets updated
- `matching <regex>` - Show event logs that match a given regular expression
- `not matching <regex>` - Show event logs that do not match a given regular expression

To view a listing of archived files:

```
show log files
```

To view the contents of a log file:

```
show log files <file number> [{matching| not matching} <regex>]
```

- `<file number>` - The number that identifies the log file
- `matching <regex>` - View entries from the selected log file that matches a given regular expression
- `not matching <regex>` - View entries from the selected log file that does not match a given regular expression

MAPI

You can use the **`acceleration mapi`** command to accelerate e-mail traffic being sent to and from a Microsoft Exchange server.

Configuring MAPI acceleration

```
[no] acceleration mapi {enable|basic-header-marking-only}
```

To enable or disable MAPI acceleration:

```
[no] acceleration mapi enable
```

To accelerate or disable acceleration of MAPI traffic using only basic header marking:

```
[no] acceleration mapi basic-header-marking-only
```

- With basic header marking, only the top level RPC header of each message is ignored when the traffic is accelerated. When basic header marking is enabled, performance is good, but there is less reduction in MAPI traffic.When basic header marking is disabled, performance is slower, but provides better reduction by decoding lower levels of the protocol. The default setting is disabled.

Viewing MAPI acceleration configuration & status

To display MAPI acceleration configuration:

```
show acceleration mapi config
```

To display the state of MAPI acceleration:

```
show acceleration mapi
```

Mirror

You can use the **`mirror`** command to assign an interface to act as a mirror port. Mirror ports are typically used in clustered environments.

More information can be found in the Topologies Guide.

Configuring alarms

To assign the specified interface to act as a mirror port:

```
[no] mirror interface <inf>
```

Monitor

You can use the **`monitor`** command to configure details relevant to monitoring charts and the monitoring data that is collected.You can configure how the data is displayed, how the traffic is analyzed for monitoring purposes, which order of resolution methods are tried when resolving IP addresses to hostnames, whether data is collected, and whether collected data is deleted.

Configuring APM

```
monitor apm
```

To set the normalization size for APM calculation:

```
monitor apm transaction normalize <value>
```

- `<value>` - When calculating the network delay experienced during a transaction, the packet size can be normalized to reflect a consistent packet size allowing you to more easily compare delays when the packets are variable in size. Specify the number of bytes used to normalize the calculation of the network delay during a transaction. The default value is 1024, and the maximum value is 1048576.

Configuring monitoring sensitivity

```
monitor {bit-torrent|edonkey|openvpn|sensitivity|skype}
```

To set bit-torrent monitoring sensitivity:

```
monitor bit-torrent sensitivity {high|med|low}
```

- `{high|med|low}` - Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.

To set eDonkey monitoring sensitivity:

```
monitor edonkey sensitivity {high|med|low}
```

- `{high|med|low}` - Setting this to 'high' is recommended for most service provider environments. Setting it to 'low' is recommended in cases of high false positives.

To specify the sensitivity of the openvpn traffic monitoring:

```
monitor openvpn sensitivity {aggressive|safe}
```

To set the minimum number of packets needed before it is monitored:

```
monitor sensitivity <sensitivity>
```

- `<sensitivity>` - Acceptable values are between 1 and 10, with 10 being the lowest sensitivity. Setting this to a low value is not recommended in high load environments. When the sensitivity is set to a low value such as 9, flows that contain less than nine packets over a five minute period are not stored in the database. This prevents port scans from loading hundreds of unnecessary rows of data into the database.

To set Skype monitoring sensitivity:

```
monitor skype {high|med}
```

- `{high|med}` - Setting this to 'high' is recommended for most service provider environments.

Configuring displays

```
monitor display {chart-size|graphing|real-time|table-size|url-size}
```

To modify how monitoring screens are displayed:

```
monitor display {chart-size|graphing|real-time|table-size|url-size}
```

- `chart-size <size>`: Number of chart items to display. Acceptable values are 1-10.
- `graphing {flash|non-flash}`: Display the charts using Adobe Flash or non-Flash.

- `real-time update <time in seconds>`: Frequency that real-time charts are refreshed. Available values are 10, 20, 30, 40, 50, 60 seconds. Note that the real-time display shows 10 seconds of data regardless of the refresh frequency.
- `table-size <size>`: Number of lines of data displayed in report tables. Acceptable values are 1-1000.
- `url-size <size>`: Limit the number of characters used when displaying a URL. Acceptable values are 0 - 255.

Controlling order of hostname resolution methods

```
monitor host-resolution
```

To control the order of resolution methods tried when resolving IP addresses to hostnames:

```
monitor host-resolution {DNS|IP|Netbios|Network_Object} rank <ranking order>
```

- There are multiple host resolution methods that can be used to resolve IP addresses to hostnames. The system will attempt to resolve the hostname using one of the methods. If that method fails it will try another method. You can determine the order of host resolution methods that the system will use by ranking the first method as 1, the next as 2, and so on.
- `DNS` - The IP addresses will be resolved according to the DNS mappings.
- `IP` - The IP addresses will NOT be resolved to hostnames.
- `Netbios` - The IP addresses will be resolved to NetBIOS names.
- `Network_Object` - The IP addresses will be resolved according to the configured network objects.
- `<ranking order>` - Rank the method 1 - 4.

EXAMPLE

```
monitor host-resolution Network_Object rank 1
monitor host-resolution Netbios rank 2
monitor host-resolution DNS rank 3
monitor host-resolution IP rank 4
```

Configuring traffic analysis & monitoring

```
[no] monitor {dual-bridge-bypass|layer7|linklocal|asam}
```

To enable viewing flow data in the real-time monitor per bridge or merged into a single flow:

```
[no] monitor dual-bridge-bypass
```

- When enabled, a flow that traverses more than one bridge will be shown multiple times, once per bridge, in the real-time monitor.

- When disabled, a flow that traverses more than one bridge will be merged into a single flow in the real-time monitor.

To enable layer7 monitoring:

```
[no] monitor layer7
```

- Controls whether to analyze the application signatures within a packet to further classify the traffic within the reports. For example, when analyzing HTTP and FTP traffic and an MPEG file is detected within the packets, the application associated with the connection is changed to MPEG.

  When disabled, the Layer 7 signatures within packets are not analyzed and any application detection objects with Layer 7 rules are ignored.

To enable IPv6 link local traffic monitoring:

```
[no] monitor linklocal
```

To configure Application Specific Analysis Modules (ASAM) settings, which enables/disables drill-down monitoring capabilities for the specified application:

```
[no] monitor asam {anonymousproxy|apm|asymm-route|citrix|dcerpc|http|ssl|urllog|voip} enable
```

- `anonymousproxy` - When enabled, the system attempts to match the HTTP hostname and SSL common name against the list of anonymous proxy URLs downloaded by the appliance daily.

  Disable this module if it appears that an applications is being misclassified as anonymous proxy.
- `apm` - When enabled, this module calculates the network delay, server delay, round trip time (RTT), loss, efficiency, and TCP health for TCP connections.

  Disable this module if the RAM or CPU usage is increasing and affecting the performance of the appliance.
- `asymm-route` - When enabled, this module collects connection symmetry information.
- `citrix` - When enabled, the appliance attempts to extract user names and applications names from Citrix connections.

  Disable this module to stop the appliance in locations where privacy policy does not permit this type of user identification.
- `dcerpc` - When enabled, this module watches for client requests for Microsoft services such as MAPI and SMB.
- `http` - When enabled, this module attempts to further analyze connections identified as HTTP and attempts to extract information such as the host, URL, request type, and content type.
- `ssl` - When enabled, this module extracts public certificates from connections identified as SSL and decodes the information from those certificates (such as common name and organization unit).
- `urllog` - When enabled, *every* URL seen by the appliance is logged to the database. Specify how long (in days) the data will be saved.

- `voip` - When enabled, this module extracts VoIP related information such as code type and call quality information (MoS and rFactor scoring) from connections identified as RTP.

Configuring statistics collection

```
[no] monitor {ignore-internal|statistics}
```

To enable ignore internal to internal traffic:

```
[no] monitor ignore-internal
```

- Your network may have network objects on the WAN side of the appliance that have been configured as Internal objects, for example a router or firewall. Enabling the Ignore Internal-to-Internal option prevents traffic between network objects being included in the reports.

To enable collecting statistics:

```
[no] monitor statistics {subnet|subnet-application|virtual-circuit} enable
```

- `subnet` - Enable or disable collection of subnet data. This setting applies to all subnets on the appliance.
- `virtual-circuit` - Enable or disable collection of virtual circuit data and application data summarized across the appliance. If disabled, there will be no data shown in the virtual circuit chart or in the application chart. Data collection for applications within a subnet is enabled and disabled independent of this setting. This setting applies to all virtual circuits on the appliance.

Deleting stored monitoring data

```
monitor clear
```

To clear stored monitoring data:

```
monitor clear
{all|apm|appliance|subnet|aps|interface|monitor|network|optimizer|reduction|sla}
```

- `all` - Deletes all data associated with the all of the clear parameters below.
- `apm` - Deletes all data associated with Application Performance Metric (APM) charts, which are the detailed metric charts for the APS monitor.
- `appliance` - Deletes all data associated with the system charts - Connections, Accelerated Connections, CPU Usage, CPU Temperature, RAM Usage, Disk IO, and Swap Usage charts.
- `subnet` - Deletes all subnet data associated with the subnets charts.
- `aps` - Deletes all data associated with Application Performance Score (APS) summary chart.
- `interface` - Deletes all data associated with the Interfaces charts - Interface Throughput and Interface Packets Per Second charts.
- `monitor` - Deletes all detailed data, that is, deletes all the drill down data for applications, hosts, URLs, users, conversations. Summary information, that is, the totals for the entire appliance will still be available.

- `network` - Deletes all data associated with the Network Summary charts.
- `optimizer` - Deletes all data associated with the Control charts - Policies, Discard, and Prioritization Ratio charts.
- `reduction` - Deletes all data associated with the Optimization charts - Reduction and Edge Cache charts.
- `sla` - Deletes all data associated with Network Response (SLA) chart.

Viewing the configuration

```
show monitor {diagnostics|setup}
```

To display the diagnostic configuration, such as graphing format, Layer 7 monitoring, host resolution, and monitoring database status:

```
show monitor diagnostics
```

To display the monitoring configuration:

```
show monitor setup
```

Netflow

You can use the **`ip flow-export`** command to configure netflow export. Netflow records can be exported and sent to 3rd party applications.

Configuring NetFlow

```
ip flow-export {destination|export|options|template|timeout}
```

To set the destination address and port (UDP) of the device that will receive netflow records:

```
ip flow-export destination <IPv4 address> <udp-port>
```

To configure which information is sent:

```
[no] ip flow-export export {application|aps|bytes-long|direction|extra-info|

 interfaces|lost-bytes|network-delay|network-jitter|output-counts|

 packets-long|packets-size|payload-size|policy|rtt|server-delay|tos|

 traffic-class|ttl|usernames|vlan|voip}
```

- `application` - Export application identification information
- `aps` - Export the Appliation Performance Score (APS)
- `bytes-long` - Export byte counters as 64bit values instead of 32bit
- `direction` - Export flow direction (i.e. inbound|outbound)
- `extra-info` - Export extra information details (e.g. hostnames, codec names)

- `interfaces` - Export SNMP input and output interfaces
- `lost-bytes` - Export lost bytes count
- `network-delay` - Export network delay
- `network-jitter` - Export network jitter
- `output-counts` - Export output packet and byte counts
- `packets-long` - Export packet counters as 64bit values instead of 32bit values
- `packets-size` - Export minimum and maximum packet sizes
- `payload-size` - Set maximum netflow packet payload size
- `policy` - Export policy identification information
- `rtt` - Export round trip time (RTT)
- `server-delay` - Export server delay
- `tos` - Export minimum and maximum TOS
- `traffic-class` - Export traffic class id
- `ttl` - Export minimum and maximum TTL
- `usernames` - Export username details (see Active Directory and Static Users)
- `vlan` - Export VLAN identifier
- `voip` - Export R-Factor

To control refresh settings for export of options:

```
ip flow-export options {refresh-rate|timeout-rate|usernames}
```

- `options refresh-rate <packet_count>` - Sets the maximum number of packets allowed between options export
- `options timeout-rate <duration_sec>` - Sets the maximum number of seconds between options export
- `options usernames expiry-rate <duration_hours>` - Set the maximum number of hours to remember inactive usernames
- `options usernames timeout-rate <duration_min>` - Set the maximum number of minutes between export of username options

To control refresh settings for export of templates:

```
ip flow-export template {refresh-rate|timeout-rate}
```

- `template refresh-rate <packet_count>` - Set the maximum number of packets before template export
- `template timeout-rate <duration_sec>` - Set the maximum number of seconds before template export

To control how often netflow records are exported:

```
ip flow-export timeout active
```

- `timeout active <duration_min>` - How often to export active flow information

Viewing NetFlow Settings

To show the current flow-export settings:

```
show ip flow-export config
```

To show currently configured netflow destinations:

```
show ip flow-export collectors
```

To show netflow template details:

```
show ip flow-export templates {appid|appgroupid|appgroups|ipv4|ipv4voip|ipv4aps}
```

Network Object

You can use the **`network-object`** command to create a new network object or modify the properties of an existing network object.

Configuring network objects

```
network-object <name> {subnet|location|subnet-report}
```

To create a new network object:

```
[no] network-object <name>
```

- This creates a network object if it does not already exist.

To add a subnet to a network object:

```
network-object <name> subnet <ip-address> <netmask or mask length>
```

- <name> - The name of the network object
- <ip-address> - The IPv4 or IPv6 address
- <netmask or mask length> - The IPv4 netmask or mask length. E.g. 255.255.255.0 or /24

To set the location of the network object with respect to the appliance:

```
network-object <name> location {internal, external, inherit}
```

- location internal - Specify that IP addresses in this network object are on the internal (LAN) side of the appliance
- location external - Specify that IP addresses in this network object are on the external (WAN) side of the appliance.
- location inherit - Specify that the location is automatically inherited from parent network objects. For, if all subnets in this network object fall within an existing network object that is has a location of internal, this network object will also be internal.

To include this network object in the subnet report:

```
network-object <name> subnet-report
```

EXAMPLE

Create a network object called 'localServer' that is an internal host on 192.168.1.1/255.255.255.255, and enable subnet reporting:

```
network-object localServer subnet 192.168.1.1 /32

network-object localServer location internal

network-object localServer subnet-report
```

EXAMPLE

Create an network object called 'IPv6 Server' that is an external host on 2001:db8::1234:5678/128

```
network-object "IPv6 Server" subnet 2001:db8::1234:5678 /128

network-object "IPv6 Server" location external
```

To see whether inherit resolved to internal or external:

```
show network-object <name>
```

NTP

You can use the **`ntp`** command to configure an NTP server to set the time on the appliance. If you want to manually set the date and time, use the time command.

Configuring Date & Time via NTP

```
ntp {server|peer|enable|disable}
```

To configure an NTP server:

```
ntp server <hostname or IPv4 address> [version <ntp-version>]
```

To configure an NTP peer node:

```
ntp peer <hostname or IPv4 address> [version <ntp-version>]
```

- `peer <hostname or IPv4 address>` - Specify an NTP peer. NTP peers will negotiate to synchronize their times. Neither is the master.

To enable or disable NTP time synchronization:

```
ntp {enable|disable}
```

© 2016 Exinda Networks Inc.

Optimizer

You can use the **optimizer** command to manage the running state of the optimizer engine.

Manage the operational state of the optimizer

To enable the optimizer:

```
optimizer enable
```

To stop the optimizer:

```
no optimizer enable
```

To restart the optimizer:

```
optimizer restart
```

Configuring the optimizer

```
optimizer {default|enable|global-qos|restart}

show optimizer
```

To install pre-configured default policies based on the policy wizard:

```
optimizer default {accelerate|accelerateqos|qos}
```

- `default accelerate` - Install the default acceleration policy set
- `default accelerateqos {dualvc|singlevc}` - Install one of the default QoS with acceleration policy sets
  - `dualvc` - Install the default enterprise QoS with acceleration policy set with two virtual circuits
  - `singlevc` - Install the default enterprise QoS with acceleration policy set with a single virtual circuit
- `default qos {enterprise {dualvc|singlevc} | serviceprovider} inbound <bandwidth (kbps)> outbound <bandwidth <kbps>` - Install one of the default QoS policy sets
  - `enterprise dualvc` - Install the default enterprise QoS policy set with two virtual circuits
  - `enterprise singlevc` - Install the default enterprise QoS policy set with a single virtual circuit
  - `serviceprovider` - Install the default serviceprovider QoS policy set (with a single virtual circuit)

To specify how policies are applied in multi-bridge deployments (Global QoS):

```
optimizer global-qos {enable|mq {mode|switch-bandwidth}}
```

- `optimizer global-qos enable` - Enable global QoS. Optimizer policies are applied globally, to the entire system. For example, if there were a single policy to restrict all traffic to 1Mbps, this would be applied across all bridges. So, the sum of all traffic through all the bridges would not exceed 1Mbps. This is typically used when you are using multiple bridges and wish to QoS everything as one link.
- `no optimizer global-qos enable` - Disable global Qos. Optimizer policies are applied to each bridge (LAN and WAN pair) independently. For example, if there ware a single policy to restrict all traffic to 1Mbps, this would be applied independently to all bridges. So, the traffic through each bridge would not exceed 1Mbps.
- `optimizer global-qos mq mode {auto-license|single|multi|multi-per-vc}` - Specify how policy queues will be handled across CPUs.
  - `mq mode auto-license` - Let the appliance automatically select single or multi-queue configuration based on license
  - `mq mode single` - Use a single global policy queue in memory to handle the traffic shaping of all virtual circuits
  - `mq mode multi` - Use one policy queue per CPU where the flows of a given virtual circuit are divided evenly amongst the policy queues.
  - `mq mode multi-per-vc` - Use one policy queue per CPU where each virtual circuit is assigned to a single policy queue.
- `optimizer global-qos mq switch-bandwidth <bandwidth [G|M|k]>` - This command should not be used. This indicates when the auto-license mode switches between single or multi-queue mode. However, this is based on license level so it should not be overwritten and may not work as expected if modified.

Circuits

You can use the **`circuit`** command to create a new optimizer circuit.

Configuring Circuits

```
circuit <circuit name> {bandwidth|bridge|order}
no circuit <circuit name> [bridge]
```

To set inbound and outbound bandwidth in kbps:

```
circuit <circuit name> bandwidth {inbound|outbound} <bandwidth_kbps>
```

To set which bridge to attach this circuit to:

```
circuit <circuit name> bridge {ALL|<name>}
```

To set the circuit ordering number:

```
circuit <circuit name> order <order_number>
```

To delete a circuit:

```
no circuit <circuit name>
```

To unbind the bridge from a circuit:

```
no circuit <circuit name> bridge
```

EXAMPLE

Create a new circuit with 200kbps bandwidth in both directions.

```
circuit circuit_1 order 1
circuit circuit_1 bandwidth inbound 200
circuit circuit_1 bandwidth outbound 200
circuit circuit_1 bridge ALL
```

Virtual Circuits

You can use the **`circuit ... vcircuit`** command to configure virtual circuits within an existing circuit.

Configuring virtual circuits

```
circuit <circuit_name> vcircuit <vcircuit_name> {app-group|app-name|bandwidth|connection-
limit|direction|dynamic|network-object|order|schedule|vlan}
no circuit <circuit_name> vcircuit <vcircuit_name>
```

To set the virtual circuit ordering number:

```
circuit <circuit-name> vcircuit <name> order <num>
```

- `order <num>` - Set the order of the virtual circuit within the circuit.

To set the bandwidth for this virtual circuit:

```
circuit <circuit-name> vcircuit <name> bandwidth <amount> {kbps|%}
```

- `<amount> {kbps|%}` - Set the amount of bandwidth as kbps or as a percentage. If `kbps` or `%` are not specified, `kbps` is used.

To set the filter settings for matching traffic:

```
circuit <circuit-name> vcircuit <name> {{app-group|app-name}|connection-limit|network-
object|schedule|vlan}
```

- `schedule` - Set the schedule for matching traffic.
- `app-group` - Set the application group for matching traffic.
- `app-name` - Set the application for matching traffic. Only an application group or application can be specified.
- `vlan` - Set the VLAN for matching traffic.
- `network-object <name>` - Set the Network Object to match.

© 2016 Exinda Networks Inc.

- `connection-limit <num>` - Limit the number of connections that can be handled by this virtual circuit. Connections exceeding this limit will be passed on for evaluation by the next virtual circuit. "0" mean no connection limit.
- `direction {inbound|outbound|both}` - Set the direction of the traffic for matching traffic. Values can be inbound, outbound, or both (bi-directional).

To set dynamic virtual circuit settings:

```
circuit <circuit-name> vcircuit <name> dynamic {bandwidth|enable|external|host-
limit|internal}
```

- `bandwidth {burst|guaranteed }` - Specify the Dynamic Virtual Circuit bandwidth values. If `kbps` or `%` are not specified, `kbps` is used.
  - `bandwidth burst {auto|<amount> {kbps|%}` - Configure the burst per-host bandwidth for the dynamic virtual circuit. This can be specified as auto configured or as an amount specified as kbps or as a percentage of the virtual circuit.
  - `bandwidth guaranteed <amount> {kbps|%}` - Configure the guaranteed per-host bandwidth for the dynamic virtual circuit specified as kbps or as a percentage of the virtual circuit.
- `enable` - Enable/disable Dynamic Virtual Circuit.
- `external` - Specify that the bandwidth is shared amongst hosts that are on the external side of the appliance
- `internal` - Specify that the bandwidth is shared amongst hosts are on the internal side of the appliance.
- `host-limit <num>` - Specify the number of unique hosts that will be managed by this virtual circuit.

EXAMPLE

Create a virtual circuit that captures all traffic in both directions and assign it 200kbps.

```
circuit circuit_1 vcircuit VC1 order 1
circuit circuit_1 vcircuit VC1 bandwidth 200 kbps
circuit circuit_1 vcircuit VC1 direction both
circuit circuit_1 vcircuit VC1 network-object ALL
```

To delete a virtual circuit:

```
no circuit <circuit_name> vcircuit <vcircuit_name>
```

Policies

You can use the **`policy`** command to create a new Optimizer policy. Policies can then be used in Optimizer virtual circuits.

Configuring policy

```
policy <policy-name> {action|enable|filter|schedule}

■ action {discard|ignore|optimize|redirect type {http_redirect|html_response}}
```

To configure the policy's action to discard (block):

```
policy <policy-name> action discard {first-packet}
```

- `action discard first-packet` - Discard only the first packet in a connection

To configure the policy's action to ignore (monitor):

```
policy <policy-name> action ignore
```

- This allows the packets to pass through the appliance unaffected, which monitors the traffic.

To configure the policy's action to optimize by shaping the bandwidth:

```
policy <policy-name> action optimize qos {bandwidth|enable|priority}
```

- `qos bandwidth guaranteed <num> {kbps|%}` - Configure the policy's guaranteed bandwidth either as kbps or as a percentage of the parent's virtual circuit's bandwidth
- `qos bandwidth burst <num> {kbps|%}` - Configure the policy's burst bandwidth either as kbps or as a percentage of the parent's virtual circuit's bandwidth
- `qos enable` - Enable the QoS action for the policy
- `qos priority <priority (1-10)>` - Set the burst priority ranging from 1 (high) to 5 (normal) to 10 (low). If excess bandwidth is available, the burst priority is used to decide how excess bandwidth is distributed. Policies with a higher burst priority will be preferred when allocating excess bandwidth.

EXAMPLE

Create an Optimizer Policy that matches all traffic belonging to the 'Web' Application Group and guarantees 20% of the bandwidth to that traffic, allowing it to burst to 100%.

```
policy Policy_1
policy Policy_1 schedule ALWAYS
policy Policy_1 action optimize
 policy Policy_1 action optimize qos bandwidth burst 100 %
policy Policy_1 action optimize qos bandwidth guaranteed 20 %
policy Policy_1 action optimize qos priority 2
policy Policy_1 action optimize qos enable
policy Policy_1 filter 1
policy Policy_1 filter 1 app-group Web
policy Policy_1 filter 1 network-object destination ALL
policy Policy_1 filter 1 direction both
policy Policy_1 filter 1 network-object source ALL
```

To configure the policy's action to optimize by accelerating:

```
policy <policy-name> action optimize aa {enable|reduction-type|type}
```

- `aa enable` - Enable application acceleration for this policy.
- `aa reduction-type {disk|lz|none}` - Specify the reduction technique
  - `disk` - De-duplicate the traffic. The appliance's hard disk drive is used to store the de-duplication patterns.
  - `lz` - Crompress the traffic using a network optimized LZ compression algorithm.
  - `none` - Do not attempt to reduce the traffic. The traffic will still be acclerated.
- `aa type {acceleration|compression|edge-cache}` - Specify the type of acceleration
  - `acceleration` - Enable full application acceleration
  - `compression` - Enable legacy compression
  - `edge-cache` - Enable Edge Cache

To configure the policy's action to optimize by marking packets:

```
policy <policy-name> action optimize mark {dscp|tos|vlan}
```

- `mark dscp <DSCP mark (0-63)>` - Specify which DSCP mark to put in the IP header of each packet
- `mark tos {normal|min-cost|max-reliability|max-throughput|min-delay}` - Set the ToS mark to put in the IP header of each packet
- `mark vlan {id <VLAN id (0-4094)>} {priority <VLAN priority (0-7)>}` - Specify which VLAN ID and priority to rewrite for each packet. Rewrite the 802.1Q VLAN ID and/or Priority only if an existing VLAN header is present. This is a packet based VLAN rewrite feature. Only packets matching this policy will be rewritten. Other packets that do not match this policy may be required to be rewritten in order for this feature to work (including non-IP packets such as ARP, which are not even processed by the Optimizer). Ensure that your topology supports this method of rewriting VLAN IDs before using this feature.

To configure the policy's action to redirect to a webpage (HTTP Redirect):

```
policy <policy-name> action redirect type http_redirect
```

```
policy <policy-name> action redirect value <url>
```

- `value <url>` - Specify the URL that you want to redirect the traffic to

EXAMPLE

Redirect traffic to http://mysystem.mycompany.com/login

policy myPolicy
policy myPolicy action redirect
policy myPolicy action redirect type http_redirect
 policy myPolicy action redirect value "http://mysystem.mycompany.com/login"
policy myPolicy filter 3
policy myPolicy filter 3 app-name HTTP
policy myPolicy filter 3 app-name HTTP-ALT
policy myPolicy filter 3 app-name HTTPS

To configure the policy's action to return a HTML response:

```
policy <policy-name> action redirect type html_response
```

```
policy <policy-name> action redirect value <url>
```

- `value <url>` - Specify the html to send back to the client

EXAMPLE

Redirect traffic to http://mysystem.mycompany.com/login

policy myPolicy
policy myPolicy action redirect
policy myPolicy action redirect type html_response
policy myPolicy action redirect value "Two Hours Exceeded"
policy myPolicy filter 3
policy myPolicy filter 3 app-name HTTP
policy myPolicy filter 3 app-name HTTP-ALT
policy myPolicy filter 3 app-name HTTPS

Note that "Two Hours Exceeded" is the name of a pre-defined HTML Response object.

To configure the policy to only be active for a particular schedule:

```
policy <policy-name> schedule <schedule-name>
```

- `schedule <schedule-name>` - Specify the schedule by name for when this policy will be active. Note the default is 'ALWAYS'.

To configure the rules that will be used to filter the traffic to determine if this policy will apply to the traffic:

```
policy <policy-name> filter <filter-num>
```

- `filter <filter-num>` - Specify the order number of the filter. The numbered filter allows you to tie together several CLI commands into a single filter.

```
policy <policy-name> filter <filter-num> {app-group|app-name|direction|dscp|network-
object|tos|vlan}
```

- `app-group <name>` - Specify an application group to match against the traffic
- `app-name <name>` - Specify a single application to match against the traffic
- `direction {inbound|outbound|both}` - Specify the traffic direction relative to the appliance. Options are inbound, outbound, or bi-directional.
- `dscp <num>` - Specify a DSCP value to match against the traffic
- `network-object {destination|source} <name>` - Specify the source or destination network object to match against the traffic
- `tos {normal|min-cost|max-reliability|max-throughput|min-delay}` - Specify a ToS name to match against the traffic
- `vlan <name>` - Specify a VLAN object to match against the traffic

To enable the policy:

```
policy <policy-name> enable
```

PBR

You can use the **pbr** command to configure the appliance with Policy Based Routing (PBR) so an Exinda appliance can be inserted in the network out-of-path, but retain in-path optimization capabilities.

Configuring policy based routing

```
pbr interface <interface-name> {ip|ipv6|mq}
```

To specify the IP address to route traffic to after it arrives at the interface:

```
pbr interface <interface-name> {ip|ipv6} next-hop <ip-address>
```

- `<interface-name>` - Name of the interface. E.g. eth1, eth2, eth3, eth4.

To specify the multi-queue NIC operation mode for this PBR interface:

```
pbr interface <interface-name> mq mode {auto-license|single|multi|multi-per-vc}
```

- `interface <interface-name>` - Name of the interface. E.g. eth1, eth2, eth3, eth4.
- `mq mode auto-license` - QoS automatically selects single or multi-queue configuration based on license.
- `mq mode single` - Force QoS to use a single queue network interface configuration.
- `mq mode multi` - Force QoS to use a multi-queue network interface configuration.
- `mq mode multi-per-vc` - Force QoS to use a multi-queue network interface configuration with virtual circuits allocated per queue.

To specify the bandwidth at which the PBR interface auto-license mode switches from single-queue to multi-queue:

```
pbr interface <interface-name> mq switch-bandwidth <bandwidth [G|M|k]>
```

- `<bandwidth [G|M|k]>` - Specify the bandwidth at which to switch to a multi-queue configuration.

Viewing policy based routing configurations

To display the parameters of the PBR interface configurations:

```
show pbr
```

PDF Reports

You can use the **`report pdf`** command to create a new pdf report.

Configure pdf reports

```
report pdf <name> {basic|custom|detailed|email|email-
report|frequency|netpercentile|password|vc-axis-unit}
```

To create a basic pdf report:

```
(config)# no report pdf <name>
```

```
report pdf <name> basic {aps|network|tcp|health|sla|subnets|edge-
cache|voip|prioritization|flows}
```

- `aps` — Include APS reports.
- `network` — Include Network reports.
  - To set the percentile line in the network report:
    - report pdf <report-name> netpercentile {none|70|75|80|85|90|95}
- `tcp` — Include TCP efficiency reports.
- `health` — Include TCP health reports.
- `sla` — Include SLA reports.
- `subnets` — Include Subnets reports.
- `edge-cache` — Include Edge Cache reports.
- `prioritization` — Include Prioritization Ratio reports.
- `flows` — Include Flow reports.

To create a detailed pdf report:

```
report pdf <name> detailed {appliance|interface|peer|pps|subnet|vcircuit}
```

- detailed appliance {aa_connection|connection|cpu_usage|cpu_temperature|memory_usage|swap_usage|diskio} - Include the appliance statistic reports.
- detailed interface {ALL|<interface|WCCP>} - Include the interface report.
- peer {all|<peer name>} - Include the WAN Memory report.
- pps {ALL|<interface|WCCP>} - Include the packets per second report.
- subnet <subnet name> {application|host|conversation|url|user} - Include the subnet report.
- vcircuit <vc name> {discard|optimizer} - Include the virtual circuit report.
  - To set the y-axis to either bytes or percentage on the virtual circuit report:
    - report pdf <report-name> vc-axis-unit {Bytes|Percent}

To specify the time range for a report that will be available for on-demand generation:

```
report pdf <name> frequency on-demand {last_60_minutes|last_24_hours|last_7_days|last_30_
days|last_12_months|current_hour|today|this_week|this_month|this_year|last_
hour|yesterday|last_week|last_month|last_year|custom}
```

- If custom, specify a start and end date/time for the custom, on-demand report. Time format is "YYYY/MM/DD HH".
  - report pdf <name> custom {start <time>|end <time>}

> **EXAMPLE**
>
> Custom pdf on-demand time range
>
> report pdf myreport frequency on-demand custom
>
> report pdf myreport custom start "2014/05/12 16"
>
> report pdf myreport custom end "2014/05/23 16"

To specify the time range for a report that will be scheduled for emailing:

```
report pdf <name> frequency scheduled {hourly|daily|weekly|monthly|custom_daily|custom_
weekly|custom_monthly}
```

- hourly - The report will be emailed hourly.
- daily - The report will be emailed daily.
- weekly - The report will be emailed weekly.
- monthly - The report will be emailed monthly.
- custom_daily - The report will be emailed daily. Additionally, you need to specify the custom time range:
  - report pdf <name> custom-daily {start <time>|end <time>}
    - <time> - Military time. E.g. 4:00pm is specified as 16:00

EXAMPLE

Scheduled daily report with custom time range of 9:00am-6:00pm

report pdf myreport frequency scheduled custom_daily

report pdf myreport custom-daily start 9:00

report pdf myreport custom-daily end 18:00

- custom_weekly - The report will be emailed weekly. Additionally, you need to specify the custom date range:
  - report pdf <name> custom-weekly {start {Sun|Mon|Tue|Wed|Thu|Fri|Sat}|end {Sun|Mon|Tue|Wed|Thu|Fri|Sat}}

EXAMPLE

Scheduled weekly report with custom time range of Monday - Friday

report pdf myreport frequency scheduled custom_weekly

report pdf myreport custom-weekly start Mon

report pdf myreport custom-weekly end Fri

- custom-monthly - The report will be emailed monthly. Additionally, you need to specify the custom date range:
  - report pdf <name> custom-monthly {start <1-31>|end <1-31>}

EXAMPLE

Scheduled monthly report with custom time range of 1st-15th of the month

report pdf myreport frequency scheduled custom_monthly

report pdf myreport custom-monthly start 1

report pdf myreport custom-monthly end 15

To specify email recipients (optional for on-demand reports):

```
report pdf <name> email <email address>
```

NOTE

Reports scheduled to be generated hourly or for the last hour cannot be emailed on-demand.

To password protect the pdf file:

```
report pdf <name> password <password>
```

To force a report to be emailed immediately:

```
report pdf <name> email-report
```

EXAMPLE

Create a custom time-range PDF report that is emailed to a recipient

```
report pdf MyFullReport
report pdf MyFullReport basic aps
report pdf MyFullReport basic network
report pdf MyFullReport basic sla
report pdf MyFullReport basic subnets
report pdf MyFullReport detailed appliance connection
report pdf MyFullReport detailed appliance cpu_temperature
report pdf MyFullReport detailed appliance cpu_usage
report pdf MyFullReport detailed appliance memory_usage
report pdf MyFullReport detailed appliance swap_usage
report pdf MyFullReport detailed interface ALL
report pdf MyFullReport detailed interface eth11
report pdf MyFullReport detailed pps ALL
report pdf MyFullReport detailed pps br10
report pdf MyFullReport detailed subnet ALL application
report pdf MyFullReport detailed subnet ALL conversation
report pdf MyFullReport detailed subnet ALL host
report pdf MyFullReport detailed subnet ALL url
report pdf MyFullReport detailed subnet ALL user
report pdf MyFullReport detailed vcircuit ALL discard
report pdf MyFullReport detailed vcircuit ALL optimizer
report pdf MyFullReport frequency on-demand custom
report pdf MyFullReport custom end "2014/02/13 09"
report pdf MyFullReport custom start "2014/02/14 16"
```

Processes

You can use the **show pm process** command to view information on a running process or service.

```
show pm process

show processes [{limit <num>|sort|threads}]
```

To show the information on a running process or service:

```
show pm process <process-name>
```

EXAMPLE

Show the status of the collectord service

```
# show pm process collectord
Process collectord
Configuration:
Launchable:  yes
Auto-launch:  yes
Auto-relaunch:  yes
Launch path:  /opt/tms/bin/collectord
Re-exec path:  (none)
Argv:  /opt/tms/bin/collectord
      Max snapshots:   10
      Launch order:    0
Launch timeout:  0
Shutdown order:  0
CPU Affinity:  (not set)
Test liveness:  no
Hung count:  4

State:
Current status:  running
PID:  3489
Num. failures:  0
Last launched:  2011/04/04 10:40:20.949 (1 day 0 hr 26 min 28.079 sec ago)
Last terminated:
Next launch:
```

To view CPU and memory use of all processes:

```
show processes [{limit <num>|sort|threads}]
```

- `limit <num>` - Show processes, limiting the number of lines displayed. Use this to generate a "top N" style display. The default sort order is CPU usage.
- `sort {cpu|memory|time}` - Sort processes by CPU usage, memory (RSS as a percentage of total) or process time.
- `threads` - Show process threads

EXAMPLE

Show the top 5 processes by CPU usage

```
# show processes sort cpu limit 5
User        Memory Usage (kB)    %CPU %Memory S  Time     Process
         Virtual Resident Shared
-------- ------- -------- ------ ---- ------- - --------- --------------
   admin    616m     341m   110m  4.0     8.8 S   7:25.02 collectord
   admin       0        0      0  2.0     0.0 S   6:33.50 kipmi0
   admin   73996      10m   8564  2.0     0.3 S   7:28.65 communityd
   admin   61192     9496   6884  2.0     0.2 S   0:19.68 slad
   admin       0        0      0  2.0     0.0 S   0:14.80 kworker/u:1
```

Protocols

You can use the **`protocol`** command to create a new protocol.

Configuring alarms

To create a new protocol:

```
protocol <protocol name> number <protocol number>
no protocol <protocol name>
```

EXAMPLE

Create a protocol for ICMP with protocol number 1

```
protocol icmp number 1
```

Radius

You can use the **`radius-server`** command to configure the Exinda appliance to authenticate user login attempts with a remote Radius server.

Configuring Radius

```
radius-server {host|key|retransmit|timeout}
```

To specify the hostname or IP address of the Radius server.

```
radius-server host <hostname or IP address>
```

- `host <hostname or IP address>` - IPv4 addresses can be used.

To specify the key for accessing the Radius server:

```
radius-server key <key string>
```

To specify how often authentication requests should be retransmitted to the Radius server:

```
radius-server retransmit <retries>
```

- `retransmit <retries>` - Specify how many retries should be attempted

To specify how many seconds before the connection to the Radius server times out:

```
radius-server timeout <seconds>
```

Real Time

You can use the **`realtime`** command to display real-time traffic information for applications, hosts, and conversations, as well as a list of asymmetric connections.

Displaying realtime

```
show realtime {apm|applications|conversations|hosts}

show monitor asymmetric-route
```

To display real-time performance values of applications:

```
show realtime apm applications
```

- The output includes application name, RTT (ms), network delay (ms), server delay (ms), transaction delay (ms), and number of transaction flows.

To display real-time TCP connection health details for hosts:

```
show realtime apm hosts
```

© 2016 Exinda Networks Inc.

- The output includes host, retransmitted bytes, aborted connections, refused connections, ignored connections, and number of flows.

To display real-time traffic rate for applications:

```
show realtime applications direction {inbound|outbound|both} [limit <number-of-
applications>]
```

- `direction {inbound|outbound|both}` - Show applications for only inbound traffic, only outbound traffic, or both
- `limit <number-of-applications>` - Limit the number of applications to show in the output. Note that the rest of the traffic is merged into a single 'Other' category.

To display real-time traffic rate for hosts:

```
show realtime hosts direction {inbound|outbound|both} [limit <number-of-hosts>]
```

- `direction {inbound|outbound|both}` - Show host for only inbound traffic, only outbound traffic, or both
- `limit <number-of-applications>` - Limit the number of hosts to show in the output. Note that the rest of the traffic is merged into a single 'Other' category.

To display real-time traffic rate for conversations:

```
show realtime conversations {aatype|direction|group|limit|show-policies|users}
```

- `aatype` - Include details indicating if the connection was processed by TCP Acceleration, Edge Cache or was not accelerated.
- `direction [inbound|outbound|both]` - Indicate which direction to show
- `group` - Group multiple flows into one conversation
- `limit <number>` - Limit output to the top <number> of conversations
- `show-policies` - Group conversations by policy
- `users` - Include user names in the conversations, if available

To display a list of all asymmetrical connections:

```
show monitor asymmetric-route
```

Reboot and Shutdown

You can use the **`reload`** command to reboot and shutdown the appliance.

Setting commands

```
stats {alarm|chd|clear-all|export|sample}
```

To reboot the appliance use the reload command.

```
reload {force|halt|mode|noconfirm}
```

- `force` - Force an immediate reboot of the system even if it's busy.
- `halt` - Shut down (power off) the system.
- `mode kexec` - Fast reboot with kexec (skips the BIOS).
- `mode bios` - Slow reboot via the BIOS (traditional reboot).
- `mode biosnext` - Slow reboot via the BIOS (for the next boot only).
- `noconfirm` - Reboot the system without asking about unsaved changes.

Schedules

You can use the **`schedule`** command to configure schedules. Schedule objects define a time range. They can be used to enable Optimizer policies at different times e.g. Work Hours/After Hours.

Configuring schedules

```
schedule <name> days <start-day> <end-day> times <start-time> <end-time>
```

```
schedule <name> days <start-day> <end-day> times <start-time> <end-time>
no schedule <name>
```

- `days <start-day> <end-day>` - The date range for this time period in the schedule. The day is specified as monday|tuesday|wednesday|thursday|friday|saturday|sunday.
- `times <start-time> <end-time>` - The time range for the days in this time period.The time is specified in military time - i.e. 1803 for 6:03pm
- This command can be called multiple times for a given schedule name so that there are several time periods associated with the schedule.

EXAMPLE

Create an 'After Hours' schedule that includes 6pm to 8am, Monday to Friday and all day Saturday and Sunday.

```
schedule "After Hours" days Monday Friday times 1800 2400
schedule "After Hours" days Monday Friday times 0000 0800
schedule "After Hours" days Saturday Saturday times 0000 2400
```

SDP

You can use the **`sdp`** command to enable using SDP (Service Delivery Point) to manage your Exinda.

Configuring SDP

```
sdp {address|enable|verify}

service sdp restart
```

To set the SDP server address:

```
sdp {address|enable|verify}
```

- sdp address <sdp ip or fqdn> - Address of your SDP

To enable the SDP service:

```
sdp enable
```

To enable SDP verify certificate:

```
sdp verify
```

To restart the SDP service:

```
service sdp restart
```

Viewing SDP status

To show the SDP service running status:

```
show service sdp
```

Serial Console Speed

The following table details the effect of the serial speed on the parts of the system that use the serial console. The speed in the table is the configured speed, or the default speed if it has never been configured. The 6062, 8062, and 10062 appliances have a default serial console speed of 115200. All other hardware has a default serial speed of 9600.

Item	Speed	Notes
BIOS	n/a	If a serial console is connected at boot time the BIOS output will adjust to match the serial speed. If no serial port is connected at boot time it will use the default speed for the model.
Boot menu	9600 or 115200	The boot menu will operate at the configured baud rate.

© 2016 Exinda Networks Inc.

Item	Speed	Notes
Kernel log messages	9600 or 115200	The kernel log messages will operate at the configured baud rate.
Login	9600	The serial port will operate at 9600 baud.
Login	115200	The serial port will operate at 115200 baud. However if a serial console at 9600 baud is connected while at the login prompt, and any key pressed, the serial login prompt will switch to 9600 baud. It will remain at 9600 baud until the user logs out and the login prompt is presented once again.

⚠ **CAUTION**

The Console speed must be set to 9600 baud before downgrading to a version of firmware prior to version 6.3.8 as those versions do not fully support the serial console speed of 115200.

To view the currently configured serial console speed, and the default speed for that model of Exinda appliance:

```
show serial
```

To change the serial console speed:

```
serial speed [9600|115200]
```

After changing the serial console speed, you must reboot the appliance to ensure that all areas of the system recognize the new speed.

Service Level Agreements

You can use the **`sla`** command to configure a site service level agreement object. A SLA object will ping the specified site every 10 seconds to report on the site's availability.

Configuring SLA

```
sla <name> {destinationip|duration|enable|pingsize}
```

```
sla <sla-name> {destinationip|duration|enable|pingsize}

no sla <sla-name>
```

- `destinationip <address>` - Specify the IP address to ping.
- `threshold <duration>` - Threshold limit (msec). This is the ping response time that will cause an alert to be triggered.
- `duration <duration>` - Set the duration (seconds) before an alert is raised. Available settings are 0, 30, 60, 300, 1800 and 3600. The ping response time must be above the threshold for the specified duration before an alert is triggered.
- `pingsize <size>` - Specify the ping packet size (in bytes). Default is 64.
- `enable` - Enable monitoring of the SLA object.

SMB Acceleration

You can use the **`acceleration smb`** command to configure SMB acceleration settings.

Configuring adaptive response settings

```
acceleration smb {application|cache|enable|v1|v2}
```

To enable or disable SMB acceleration.

```
[no] acceleration smb enable
```

To add applications supported by the SMB module:

```
[no] acceleration smb application <application>
```

To clear the SMB disk cache:

```
acceleration smb cache clear
```

SMB1 commands

```
acceleration smb v1 {enable|meta-cache|prefetch|read-ahead|write-behind}
```

To enable or disable SMB1 acceleration:

```
[no] acceleration smb v1 enable
```

To enable or disable SMB1 meta-caching:

```
[no] acceleration smb v1 meta-cache
```

To set the amount to pre-fetch:

```
acceleration smb v1 prefetch <prefetch-kbytes>
```

- `prefetch <prefetch-kbytes>` - Value in kbytes must be between 0 and 8192.

To enable or disable SMB1 read-ahead :

```
[no] acceleration smb v1 read-ahead
```

© 2016 Exinda Networks Inc.

To enable or disable SMB1 write-behind :

```
[no] acceleration smb v1 write-behind
```

To enable or disable SMB1 signing :

```
[no] acceleration smb v1 signing enable
```

SMB2 commands

```
acceleration smb v2 {enable|signing enable}
```

To enable or disable SMB2 acceleration:

```
[no] acceleration smb v2 enable
```

To enable or disable SMB2 signing :

```
[no] acceleration smb v2 signing enable
```

Viewing acceleration settings

```
show acceleration smb {applications|signed-servers|v1|v2}
```

To list the applications that support SMB:

```
show acceleration smb applications
```

To list the SMB signed servers:

```
show acceleration smb signed-servers
```

To display the configuration for SMB1:

```
show acceleration smb v1 config
```

To display the SMB1 connections:

```
show acceleration smb v1 connections [list [detailed]]
```

- `smb v1 connections` - Display the connections.
- `smb v1 connections list` - Display the connections with sources and destinations of the connections.
- `smb v1 connections list detailed` - Display the connections, the sources and destinations of the connection, and the client/server operating systems and shared file directories.

To display the configuration for SMB2:

```
show acceleration smb v2 config
```

To display the SMB2 connections:

```
show acceleration smb v2 connections [list]
```

- `smb v2 connections` - Display the connections.
- `smb v2 connections list` - Display the connections with sources and destinations of the connections.

SNMP

You can use the **`snmp-server`** command to configure SNMP.

Configuring SNMP

```
snmp-server {community|contact|enable|host|listen|location|port|restrict|user}
```

To add a new SNMP community:

```
snmp-server community <community>
```

To set a value for the syscontact variable in MIB-II:

```
snmp-server contact <contact>
```

Set a value for the syslocation variable in MIB-II:

```
snmp-server location <location>
```

To enable SNMP-related functionality:

```
snmp-server enable
```

To enable community-based authentication:

```
snmp-server enable communities
```

To enable sending of SNMP traps and informs from this system:

```
snmp-server enable notify
```

To specify the hostname or IP address to send SNMP traps to:

```
snmp-server host <host>
```

- `host <host>` - Hostname or IP address. IPv4 or IPv6 addresses can be used.

To specify the port for sending the SNMP trap:

```
snmp-server port <port>
```

- `port <port>` - UDP port for the SNMP agent.

To configure SNMP server interface access restrictions:

```
snmp-server listen {enable|interface <interface>}
```

- `listen interface <interface>` - Add the named interface to the SNMP server access restriction list

To configure SNMP access on a per-user basis:

```
snmp-server user <username> v3 {auth|enable|encrypted|prompt}
```

- `v3` - Configure SNMP v3 users
- `auth {md5|sha} <password> [priv <privacy-type>]` - Configure SNMP v3 security parameters

To restrict a network object from accessing the SNMP server:

```
snmp-server restrict <network-object>
```

SSH

You can use the **`ssh`** command to enable SSH access the system

Configuring SSH Servers

```
ssh server {restrict|enable|host-key|listen|min-version|ports|x11-forwarding}
```

To restrict a network object from accessing the SSH server:

```
ssh server restrict <network-object>
```

To enable SSH access to the system:

```
ssh server enable <server-name>
```

To set a new RSA or DSA host key:

```
ssh server host-key <key> {private-key|public-key}
```

- `private-key` - Set the new private key for host keys of the specified type
- `public-key` - Set the new public key for host keys of the specified type

To generate a new RSA or DSA host key:

```
ssh server host-key generate
```

To enable SSH interface restrictions on access to the system:

```
ssh server listen enable
```

To add an interface to the SSH server access restriction list:

```
ssh server listen interface <interface-name>
```

To specify the minimum version of the SSH protocol that is supported:

```
ssh server min-version <version-number>
```

To set the ports the SSH server listens on:

```
ssh server ports <port-number>
```

To enable x11 forwarding on the SSH server:

```
ssh server x11-forwarding enable
```

Configuring SSH clients

```
ssh client {global|user}
```

To configure whether the SSH client checks for a host key from the list of known host keys:

```
ssh client global host-key-check [yes|no|ask]
```

To add a global SSH client known host entry:

```
ssh client global known-host <known host entry>
```

To configure the authorized key for the specified SSH user:

```
ssh client user <user name> authorized-key sshv2
```

To identify the type of key used by the SSH user:

```
ssh client user <user name> identity <key type>
```

To set the known host for the SSH user:

```
ssh client user <user name> known-host <known host>
```

Viewing SSH configurations

```
show ssh {client|server}
```

To display the parameters of the SSH client:

```
show ssh client <client-name>
```

To display the parameters of the SSH server:

```
show ssh server <server-name>
```

To display the settings of the SSH server with full host keys:

```
show ssh server host-keys <server-name>
```

Network User

You can use the **`network-user`** command to manually create network objects based on an IP address or to dynamically create a network object based on an Active Directory group or user.

Configuring network user object

```
network-user {static-user|network-object}
```

To manually configure a network object for a user:

```
[no] network-user static-user <user-name> address <IP-address> [group]
```

© 2016 Exinda Networks Inc.

- `static-user <user-name>` - The name of the user.
- `address <IP-address>` - The corresponding static IPv4 or IPv6 address of the user. Multiple addresses may be specified.
- `group` - The group that the user belongs to (optional)

To create a dynamic Network Object based on a user or group:

```
[no] network-user network-object <network-object> {group | user} <user or group>
```

- `network-object <network-object>` - The name of the dynamic network object that will be created.
- `group <ad-group>` - The Active Directory group name that the dynamic network object will be mapped to.
- `user <ad-user>` - The Active Directory user name that the dynamic network object will be mapped to.

EXAMPLE

Create a dynamic Network Object called 'Students Network Object' from the Active Directory 'Students' group

```
network-user network-object "Students Network Object" group Students
```

Storage

You can use the **`storage`** command to manage the disk storage used by system services.

CAUTION

Put the Exinda appliance into bypass before changing the partition size of wan-memory. See "Bypass" on page 141 for more information.

Configuring storage

```
storage {service|tasks}

show storage
```

To manage the disk storage for specified services:

```
storage service {edge-cache|cifs|monitor|users|wan-memory|virt} {format|size}
```

- `format` - Format the volume being used by the specified service
- `size` - Resize the volume being used by the specified service

To clear the current storage tasks list:

© 2016 Exinda Networks Inc.

```
storage tasks clear
```

Viewing storage configuration

To show the current storage configuration:

```
show storage [{disk|raid|service|smart|tasks}]
```

- `show storage` - Show summary storage details
- `show storage disk [<disk>]` - Show storage disk details for all or a specified disk
- `show storage service {cifs|edge-cache|monitor|users|virt|wan-memory}` - Show the current storage running state for the specified service.
- `show storage tasks` - Show currently running storage tasks (e.g. size or format operations)
- `show storage raid adapter [<A>]` - Show all information about RAID adapters.
- `show storage raid adapter <A> logical` - Show information about logical drives on a specified adapter.
- `show storage raid adapter <A> drive` - Show information about physical drives on a specified adapter.
- `show storage raid adapter <A> eventlog {last <N>|all}` - Show the eventlog for a specified adapter. Use "last <N>" to show the last N events.
- `show storage smart device <device> attributes` - Show S.M.A.R.T. vendor attributes and values

TACACS+

You can use the **`tacacs-server`** command to configure the Exinda appliance to authenticate user login attempts with a remote TACACS+ server.

Configuring TACACS+ servers

```
tacacs-server {host|key|retransmit|timeout}
```

To specify the hostname or IP address of the TACACS+ server:

```
tacacs-server host <hostname or IP address>
```

- `host <hostname or IP address>` - IPv4 addresses can be used.

To specify the key for accessing the TACACS+ server:

```
tacacs-server key <key string>
```

To specify how often authentication requests should be retransmitted to the TACACS+ server:

```
tacacs-server retransmit <retries>
```

To specify how many seconds before the connection to the TACACS+ server times out:

```
tacacs-server timeout <seconds>
```

Telnet

You can use the **telnet-server** command to enable a telnet server and restrict access to it.

Configuring Telnet

```
[no] telnet-server {enable|restrict}
```

To enable the Telnet server:

```
[no] telnet-server enable
```

To restrict a network object from accessing the Telnet server:

```
[no] telnet-server restrict <network-object>
```

Time

You can use the **clock** command to manually configure the date, time, and timezone on the appliance. If you want the time to be set via NTP server, use the ntp command.

Note that using these commands will force the UI to restart without a prompt.

Manually configuring the date & time

```
clock {set|timezone}
```

To set the appliance's time and date:

```
clock set <hh>:<mm>:<ss> [<yyyy>/<mm>/<dd>]
```

- `<hh>:<mm>:<ss> [<yyyy>/<mm>/<dd>]` - If the date is not set, the time will change without affecting the date. Time adjustment is not allowed if NTP is enabled.

> **EXAMPLE**
>
> Set the time zone and adjust the system clock to 11:00pm.
>
> ```
> clock timezone Australia Melbourne
> clock set 23:00:00
> ```

To set the appliance's time zone:

```
clock timezone {<region>|UTC|UTC-offset <utc-offset>}
```

- `<region>` - Set the region. The region is specified by several keywords.
  E.g. America North United_States Pacific
  E.g. Australia Melbourne
  E.g. Europe Eastern Moscow
- `<utc-offset>` - Set the UTC offset. Options range from UTC-9 to UTC+0 to UTC+14.

Enabling Virtualization in the CLI

You can use the **`virt`** command to creat or edit virtual machines.

Configuring virtual machines

```
[no] virt {enable|interface|vm|vnet|volume}
```

To enable the virtualization feature:

```
virt enable
```

To assign an interface to use as a VM access port:

```
virt interface <interface>
```

To configure a virtual machine:

```
virt vm <name>
{arch|boot|comment|console|copy|feature|install|interface|memory|power|rename|storage|vcpus}
```

- `arch {i386|x86_64}` - Set CPU architecture.
- `boot {auto-power|device}` - Configure boot options.
  - `auto-power {on|off|last}` - Specify power state for VM to have after host boot.
    - `auto-power on` - Always power VM on. If VM was running at last shutdown, restore its state.
    - `auto-power off` - Always leave VM powered off. If VM was running at last shutdown, its state is lost.
    - `auto-power last` - Power VM on only if it was running at last shutdown. In this case, also restore its state.
  - `device order {cdrom|hd}` - Specify order to try devices during boot.
    - E.g. device order cdrom hd
    - E.g. device order hd cdrom
- `comment <comment>` - Set a comment describing this virtual machine.
- `console {connect|graphics|text}` - Configure or connect to the text or graphica
- `copy <new_name> [storage copy-type {shallow|none}]` - Make a duplicate copy of this virtual machine.

© 2016 Exinda Networks Inc.

  - `storage copy-type {shallow|none}` - Make a duplicate copy of this VM's storage.
    - `shallow` - Use the same volumes as the source VM.
    - `none` - New VM will have no attached storage
- `feature {pae|acpi|apic} enable` - Enable/disable certain virtualization features.
  - `pae` - Physical Address Extension
  - `acpi` - Advanced Configuration and Power Interface
  - `apic` - Advanced Programmable Interrupt Controller
- `install {cancel|cdrom}` - Install an operating system onto this virtual machine (temporarily attach a CD and boot from it).
  - `cancel` - Cancel an install already in progress
  - `cdrom file <volume-name> {connect-console|disk-overwrite|timeout|verify}` - Install an operation system from a CD-ROM (ISO) image
    - `connect-console` - Connect to the console during installation
    - `disk-overwrite` - Install even if primary target volume is not empty
    - `timeout {<minutes>|none}` - Specify a timeout for installation (default is no timeout)
    - `verify` - Options for verifying OS installation
- `interface <name> {bridge|macaddr|model|name|order|type|vnet}` - Configure virtual interfaces.
- `memory <MB>` - Set memory allowance.
- `power {cycle|off|on}` - Turn this virtual machine on or off, plus other related options.
- `rename <new_name>` - Rename this virtual machine.
- `storage {create|device}` - Configure storage for this virtual machine.
  - `create disk {bus|drive-number|file|mode|size-max}` - Create new storage device for the VM, with an automatically assigned name.
  - `device {bus|drive-number|move|swap}` - Modify existing storage device, or crate a new one with a specific name.
- `vcpus {count|vcpu}` - Specify number of virtual CPUs.
  - `vcpus count <count>` - Specify number of virtual CPUs
  - `vcpu <vcpu>` - Specify options for a particular virtual CPU

To configure or manage virtual networks:

```
virt vnet <name> {dhcp|forward|ip|vbridge}
```

- `dhcp range <low_ip> <high_ip>` - Configure a DHCP range to assign to this vnet.
- `forward {none|nat|route} interface <name>` - Configure the type of forwarding.
- `ip address <ip> <netmask>` - Configure the IP address of this vnet.
- `vbridge name <name>` - Create a virtual bridge.

To manage virtual storage volumes:

```
virt volume {create|fetch|file}
```

- `create disk file <name> size-max <MB>` - Create an empty virtual disk image.
- `fetch <url>` - Fetch a virtual disk image (*.img) or a CD ROM image (*.iso) from the URL.
- `file {create|copy|move|upload}` - Perform basic file operations.

VLANs

You can use the **`vlan vlan-id`** command to create a VLAN interface. VLAN interfaces are typically used in a trunk Topology to associate a VLAN ID to the interface that is used to manage the appliance.

Configuring VLANs

```
vlan vlan-id <id> interface <inf>

vlan object <name> {id|priority}
```

To associate a VLAN ID with an interface:

```
vlan vlan-id <id> interface <inf>
```

To create a VLAN object, which can be used in the Optimizer:

```
vlan object <name> {id|priority}
no vlan <name>
```

- `id <low (0-4094)> <high (0-4094)>` - Set the ID range. To match a single ID use the same number for low and high.
- `priority <low (0-7)> <high (0-7)>` - Set the priority range. To match a single priority, specify the same number for both low and high.

EXAMPLE

Create a VLAN Object that defines all tagged VLANs with a VLAN ID between 2 and 7 (inclusive).

```
vlan object VLAN1 id 2 7
```

EXAMPLE

Create a VLAN Object that defines all tagged VLANs with a VLAN priority of 2.

```
vlan object VLAN2 priority 2 2
```

Viewing VLANs

To show VLAN objects:

```
show vlan object <vlan>
```

EXAMPLE

Show VLAN object info

```
show vlan object VLAN1
```

Output:

```
Object: VLAN1

ID, Lower limit:             2

ID, Higher limit:            7

Priority, Lower Limit:       0

Priority, Higher Limit:      7

Type:                        802.1Q
```

WCCP

You can use the **wccp** command to configure WCCP on the appliance. WCCP allows for out-of-path application acceleration.

Configuring WCCP

```
[no] wccp {interface|service}
```

To assign an interface to use for WCCPv2 traffic:

```
wccp interface <interface>
```

To configure WCCP services:

```
wccp service <service group (1-99)> {assignment|group-address|password|router}
```

- `assignment {HASH|MASK}` - Set the assignment type of the service group
- `group-address <multicast-address>` - configure the multicast address for sending WCCPv2 messages to
- `password <password (1-8 characters)>` - Configure the password used by the service group
- `router <address>` - Configure the routers in the service group

See the WCCP HowTo Guide for more information.

Web UI and Web Proxy

You can use the **web** command to configure the web user interface (Web UI).

Configuring web UI

```
web {auto-logout|logout|console|http|httpd|https|proxy|enable}
```

To enable or disable the Web UI:

```
[no] web enable
```

To configure the length of user inactivity before auto-logout (in seconds):

```
web auto-logout <time>
```

To configure HTTP access to the Web UI:

```
web http {enable|port|redirect|restrict}
```

- enable - Enable http access to the web UI.
- port <port-number> - Set the port number for http access to the web UI.
- redirect - Enable redirection to https.
- restrict <network-object> - Restrict access to the web UI for a particular named network object.

To configure HTTPS access to the Web UI:

```
https {enable|certificate|customssl|port|restrict}
```

- enable - Enable https access to the web UI.
- port <port-number> - Set the port number for https access to the web UI.
- certificate regenerate - Configure a certificate for use for https connections.
- customssl - Configure a custom SSL certificate.
- restrict <network-object> - Restrict access to the web UI for a particular named network object.

To configure a custom SSL certificate:

```
https customssl {enable|certificate|generate csr country <country> state <state> location
<location> organization <org> hostname <hostname>|privatekey}
```

- certificate <certificate> – Specify the certificate to use.
- country <country> – Type your country code. E.g. US.
- state <state> – Type your state. E.g. California.
- location <location> – Type your location. E.g. "San Franscisco".
- organization <org> – Type your organization. E.g. "Exinda Networks".
- hostname <hostname> – Type your full hostname to access your appliance.
- privatekey <pkey> – Type a custom SSL private key that you have obtained or generated.

To configure renewal and timeout session settings:

© 2016 Exinda Networks Inc.

```
web session {renewal <number-of-minutes>|timeout <number-of-minutes>}
```

To enable or disable deflate compression encoding:

```
[no] web httpd compression
```

To enable or disable Web interface restrictions:

```
[no] web httpd listen {enable|interface <interface>}
```

To restrict the listen interface for the Web UI. The configured interface should be statically configured (DHCP disabled).

```
web httpd listen interface <interface>
```

Configuring web proxy

```
web proxy {host|proxy}
```

Configure the web proxy host address and port:

```
web proxy host <hostname or IP address> [port <port>]
```

- `host <hostname or IP address>` - IPv4 and IPv6 addresses can be used.

To configure the type of proxy authentication:

```
web proxy auth authtype {none|basic}
```

Configure the username and password for basic authentication:

```
web proxy auth basic {password|username}
```

Viewing web settings

To show Web UI configuration and running state:

```
show web
```

Other Commands

There are other commands that may be helpful.

To measure TCP/UDP bandwidth:

```
iperf [-s|-c host]
```

- This command requires 2 Exinda appliances. One needs to be run as an iperf server; see the -s option. The other needs to be run as an iperf client, which connects to the iperf server; see the -c option.

To send ICMP echo requests to a specified host:

```
ping <hostname or ip address of remote host>
```

© 2016 Exinda Networks Inc.

To trace the route that packets take to a destination:

```
traceroute <hostname or ip address of remote host>
```

© 2016 Exinda Networks Inc.