



Manager of Central Managers User's Guide



Modified: 2018-07-30

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Manager of Central Managers User's Guide
Copyright © 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	ix
	Documentation and Release Notes	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xiii
Chapter 1	Manager of Central Managers User's Guide	15
	Overview	15
	MCM Configuration	16
	To convert a CM to an MCM	17
	Sample MCM CLI Configuration Sequence	17
	To Register and Sync Incidents from Distributed CMs to an MCM	18
	Sample CLI Sequence for CM Registering and Syncing to an MCM	18
	Using the MCM Web UI	19
	What To Do Next	20

List of Figures

Chapter 1	Manager of Central Managers User's Guide	15
	Figure 1: Manager of CMs (MCM) Web UI	15
	Figure 2: Incidents Tab	19

List of Tables

About the Documentation	ix
Table 1: Notice Icons	x
Table 2: Text and Syntax Conventions	x

About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

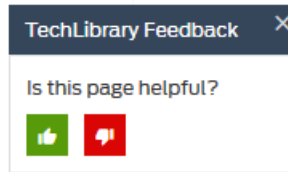
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://www.juniper.net/support/requesting-support.html>.

CHAPTER 1

Manager of Central Managers User's Guide

- Overview on page 15
- MCM Configuration on page 16
- What To Do Next on page 20

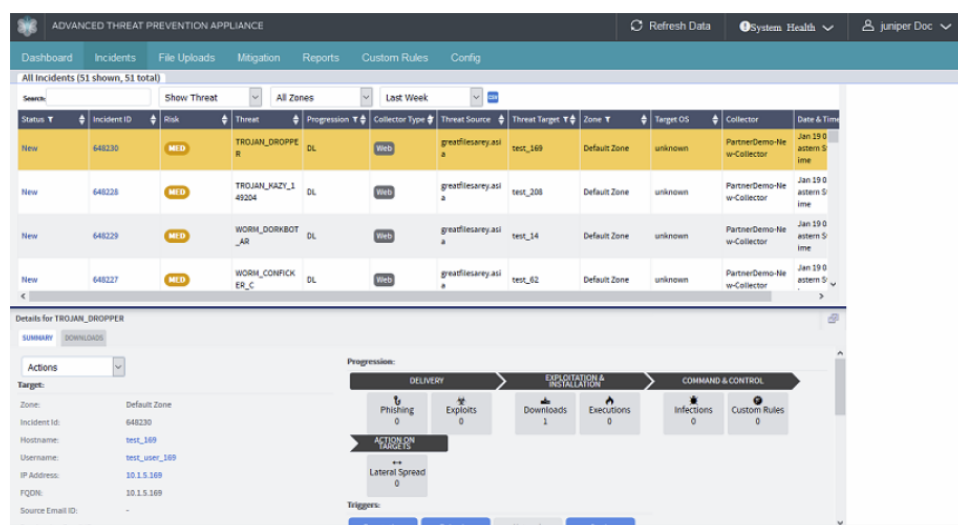
Overview

The Juniper ATP Appliance Manager of Central Managers (MCM) is a device that provides a centralized Web UI for users that deploy multiple Core/Central Managers (CMs) in various geographic locations. The MCM allows customers with distributed enterprises to consolidate viewing of detected malware incidents occurring on multiple CMs registered to the central MCM.

The MCM Platform device type is represented as “mcm” in the Juniper ATP Appliance CLI. The MCM receives incident data from multiple secondary Central Manager (CM) appliances and displays that data in the primary MCM Web UI.

The MCM Web UI is a subset of the larger Juniper ATP Appliance Central Manager Web UI and includes only the Incidents tab and the Config tab for System Profile configurations, in addition to a device Refresh and Logout tab options.

Figure 1: Manager of CMs (MCM) Web UI



Note that the CM Name column details the name of each incident's originating Central Manager.

When an admin interacts with an incident in any way from the MCM Web UI (for example, by clicking on an incident to view its details, selecting a mitigation option, downloading IVP, viewing screenshots or traces, and so on) the MCM automatically connects directly to the originating Core/CM containing the incident. In this way, the MCM maintains only incident table data.

The MCM manages a list of its users with admin privileges for viewing Incident details and performing mitigation and whitelist actions, which will be applied only to the CM that generated the incident. SAML and RADIUS is supported for login to the MCM.



NOTE: The MCM must be provisioned with an MCM license in order to be upgraded via the Juniper ATP Appliance GSS, in the same manner as all other Juniper ATP Appliance device types.

Related Documentation

- [MCM Configuration on page 16](#)

MCM Configuration

Use the CLI command line in “cm” mode, available for MCM device types, to configure a manager of distributed central managers (MCM). It is recommended that an admin begin by converting a CM to an MCM via the CLI, and then set up each individual, distributed CMs to register to the configured MCM in order to sync incidents.



TIP: Communication between the MCM and the secondary CMs takes place on port 443 which must be set bidirectionally if the CMs and MCM communicate across a firewall boundary.

From the CLI “cm” mode, configure an MCM IP address and a shared secret/passphrase. When the MCM CLI is used, a Web UI MCM account is created via this passphrase which is used as the API key, which means that client CMs connected to the MCM can use this passphrase to perform a “login” API call to the management CM (MCM).



NOTE: The secret passphrase must be configured on all distributed CM and MCM devices to allow communications.



NOTE: In MCM configurations, all systems must be either in FIPS mode or not in FIPS mode. This is due to differences in how the device keys are calculated between modes.

- [To convert a CM to an MCM on page 17](#)
- [Sample MCM CLI Configuration Sequence on page 17](#)
- [To Register and Sync Incidents from Distributed CMs to an MCM on page 18](#)
- [Sample CLI Sequence for CM Registering and Syncing to an MCM on page 18](#)
- [Using the MCM Web UI on page 19](#)

To convert a CM to an MCM

Use the following procedure to convert a CM to an MCM. A sample CLI sequence follows.

1. Set the IP of the CM device that is to become an MCM to point to loopback IP address 127.0.0.1 to indicate that this is now the MCM.
2. Set a passphrase that is used for secure sync of incidents from each CM to the MCM. Set this same passphrase on the individual CMs that are to point and report to the MCM.



NOTE: The “remove” command converts an MCM back to a CM by removing all the MCM configuration. This will also delete all incidents from the MCM and deregisters all connected CMs that were registered to the MCM, so use this command with caution.

3. Verify MCM configuration by logging into the Web UI on the and noting that there are just two tabs - Incidents and Config, instead of the full Central Manager Web UI seen on a CM.



NOTE: The “resync” command is specific to connected CMs only. This command has no effect when executed on an MCM.

Sample MCM CLI Configuration Sequence

```
MCM-VM# cm
```

```
Entering the Central Manager configuration mode...
```

```
MCM-VM(cm)# set mcm
```

```
ip Set the IP address of the Manager of Central Managers
```

```
resync Resync with MCM
```

```
remove Remove entire MCM config
```

```
MCM-VM(cm)# set mcm ip 127.0.0.1
```

```
passphrase Set the device key passphrase for MCM
```

```
MCM-VM(cm)# set mcm ip 127.0.0.1 passphrase password123
```

To Register and Sync Incidents from Distributed CMs to an MCM

Use this procedure to register and sync incidents on distributed CMs to a configured MCM. A sample CLI sequence follows.

1. Set the MCM IP on a distributed CM.
2. Set the passphrase; this must be same passphrase configured on the MCM.
3. Set the username with the API key already configured to be used for communication between each CM and the MCM.



NOTE: The “remove” command deletes the MCM configuration entirely. However, this command when executed on a CM does not remove any incidents unlike when executed on an MCM.

Use the “resync” command on a CM to force a resync of all incidents from this CM to the MCM.

After configuring the parameters described above, incidents are immediately synced to the configured MCM.

Sample CLI Sequence for CM Registering and Syncing to an MCM

```
CM-VM6-LosAngeles(cm)# set mcm ip 1.2.3.4
```

```
passphrase Set the device key passphrase for MCM
```

```
CM-VM6-LosAngeles(cm)# set mcm ip 1.2.3.4 passphrase password123
```

```
username Enter a username to use for communication with MCM
```

```
<cr>
```

```
CM-VM6-LosAngeles(cm)# set mcm ip 1.2.3.4 passphrase password123
```

```
username Enter a username to use for communication with MCM
```

```
<cr>
```

```
CM-VM6-LosAngeles(cm)# set mcm ip 1.2.3.4 passphrase password123
```

```
username admin
```

```
CM-VM6-LosAngeles(cm)# show mcm
```

```
MCM IP Address: 1.2.3.4, username: admin
```

```
CM-VM6-LosAngeles(cm)#
```

Using the MCM Web UI

As mentioned in the introduction, the MCM Web UI management view displays two tabs: the Incidents and Config Tabs.

Use the Incidents tab to view all incidents reported from distributed CMs.

Figure 2: Incidents Tab

All Incidents (5 shown, 5 total)										
Search:		Show Threat		Last Month		All Zones				
Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector
New	8	HIGH	TROJAN_AGENT.DC	UP		User Uploaded	switch-56.corp.cyphort.com	Default Zone		Core File Upload Collector
New	7	HIGH	TROJAN_GENOME.DC	UP		User Uploaded	switch-54.corp.cyphort.com	Default Zone		Core File Upload Collector
New	9	HIGH	TROJAN_VAWTRAK.DC	UP		User				Core File Jun 24

Details for TROJAN_GENOME.DC

SUMMARY
EXPLOITS
DOWNLOADS
EXTERNAL SOURCES

Target:

Hostname: -

Username: -

IP Address: -

FQDN: -

Source Email ID: -

Destination Email ID: -

Risk: High

Threat Category: Trojan_Generic

Asset Value: Medium

Triggers:

Reputation Behavior

Network Static



NOTE: The Uploads button is not available from the MCM Web UI. Be aware also that there is a new column in MCM for the originating CM per incident, and that the Core/CM IP and hostname are displayed in the Summary section. Also: no benign incidents are communicate to the MCM. Lastly, CMs cannot be deleted from the MCM.



NOTE: Refer to the Juniper ATP Appliance Operator's Guide for more information about use of the Incidents tab.

On an MCM, the Details section for a selected incident displays the mitigation options as in a CM, and all options are available from the MCM.

Use the Config tab to add or modify MCM settings.

The Config Tab options on an MCM are reduced to System Profiles settings only, as follows:

- Password Reset
- Roles
- Users
- SAML Settings
- RADIUS Settings
- System Settings
- Certificate Management
- GSS Settings
- Secondary CMs
- Licensing
- Backup/Restore



NOTE: Refer to the Juniper ATP Appliance Operator's Guide for more information about use of the Config tab System Profiles configuration options.

What To Do Next

Refer to Juniper ATP Appliance documentation for more information:

- Juniper ATP Appliance Quick Start Guides— Quick Starts describe how to install and initially configure a Juniper ATP Appliance device; refer to the Quick Start for your device, feature or model:
 - Juniper ATP Appliance Core/CM Quick Start Guide
 - Juniper ATP Appliance All-in-One Quick Start Guide
 - Juniper ATP Appliance Email Traffic Collector Quick Start Guide
 - Juniper ATP Appliance Web Traffic Collector Quick Start Guide
 - Juniper ATP Appliance Mac OSX Quick Start Guide
 - Juniper ATP Appliance Virtual Core for AWS
- Juniper ATP Appliance CLI Command Reference Guide—Describes all the commands that are available in the command-line interface (CLI) for Juniper ATP Appliance devices.

- Juniper ATP Appliance Safety and Regulatory Guide—Contains conformance and safety information for Juniper ATP Appliance devices.
- Juniper ATP Appliance API Reference Guide— Provides Juniper ATP Appliance HTTP API functions and information about usage.
- Juniper ATP Appliance CEF & Syslog Support for SIEM Guide— Provides Juniper ATP Appliance CEF and Syslog format and field information with usage guidelines for SIEM support.
- Juniper ATP Appliance Operator's Guide— Provides usage and procedural information for all Juniper ATP Appliance products.

**Related
Documentation**

- [Overview on page 15](#)

