

Juniper Advanced Threat Prevention Appliance

Manager of Central Managers User's Guide

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.

Juniper Advanced Threat Prevention 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 document 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 <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

About the Documentation

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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://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 <http://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 <http://www.juniper.net/support/requesting-support.html>

Inside This Guide

- MCM CONFIGURATION
- TO CONVERT A CM TO AN MCM
- SAMPLE MCM CLI CONFIGURATION SEQUENCE
- TO REGISTER AND SYNC INCIDENTS FROM DISTRIBUTED CMs TO AN MCM
- SAMPLE CLI SEQUENCE FOR CM REGISTERING AND SYNCING TO AN MCM
- USING THE MCM WEB UI
- WHAT TO DO NEXT

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

Status	Incident ID	Risk	Threat	Progression	Collector Type	Threat Source	Threat Target	Zone	Target OS	Collector	Date & Time
New	648230	High	TROJAN_DROPPER	DL	test_189	greaflesrey.asi	test_189	Default Zone	unknown	PartnerDemo-He-w-Collector	Jan 18 9:45:00 am
New	648238	High	TROJAN_DROPPER	DL	test_208	greaflesrey.asi	test_208	Default Zone	unknown	PartnerDemo-He-w-Collector	Jan 18 9:45:00 am
New	648229	High	WORM_DORNBOT	DL	test_14	greaflesrey.asi	test_14	Default Zone	unknown	PartnerDemo-He-w-Collector	Jan 18 9:45:00 am
New	648227	High	WORM_CONFICKER	DL	test_62	greaflesrey.asi	test_62	Default Zone	unknown	PartnerDemo-He-w-Collector	Jan 18 9:45:00 am

Progression
DELIVERY
EXPLOITATION & INSTALLATION
COMMAND & CONTROL

Triggers
Phishing: 0
Exploits: 0
Downloads: 1
Executions: 0
Infections: 0
Custom Rules: 0

Incident Details
Zone: Default Zone
Incident ID: 648230
Hostname: test_189
Username: test_user_189
IP Address: 10.1.1.189
FQDN: 10.1.1.189
Source Email ID: -

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.

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.

To convert a CM to an MCM

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

- Step 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.
- Step 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.

- Step 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 syn incidents on distributed CMs to a configured MCM. A sample CLI sequence follows.

- Step 1 Set the MCM IP on a distributed CM.
- Step 2 Set the passphrase; this must be same passphrase configured on the MCM.
- Step 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

CSV

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

SUMMARYEXPLOITSDOWNLOADSEXTERNAL 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.

