

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase sans-serif font.

TECHDOCS

WildFire Appliance Administration

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2021-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

August 23, 2023

Table of Contents

WildFire Appliance Overview.....	7
About the WildFire Appliance.....	8
WildFire Private Cloud.....	9
WildFire Hybrid Cloud.....	10
WildFire Appliance Interfaces.....	11
WildFire Appliance File Type Support.....	12
Set Up and Manage a WildFire Appliance.....	15
Configure the WildFire Appliance.....	16
Forward Files For WildFire Appliance Analysis.....	24
Submit Malware or Reports from the WildFire Appliance.....	30
Set Up Authentication Using a Custom Certificate on a Standalone WildFire Appliance.....	32
WildFire Appliance Mutual SSL Authentication.....	32
Configure Authentication with Custom Certificates on the WildFire Appliance.....	33
Set Up the WildFire Appliance VM Interface.....	36
Virtual Machine Interface Overview.....	36
Configure the VM Interface on the WildFire Appliance.....	38
Connect the Firewall to the WildFire Appliance VM Interface.....	40
Enable WildFire Appliance Analysis Features.....	42
Set Up WildFire Appliance Content Updates.....	42
Enable Local Signature and URL Category Generation.....	46
Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud.....	47
Upgrade a WildFire Appliance.....	49
Install WildFire Appliance Device Certificate With an Internet Connection.....	56
Monitor WildFire Appliance Activity.....	61
About WildFire Logs and Reporting.....	62
Use the WildFire Appliance to Monitor Sample Analysis Status.....	63
View WildFire Analysis Environment Utilization.....	63
View WildFire Sample Analysis Processing Details.....	64
Use the WildFire CLI to Monitor the WildFire Appliance.....	66
View the WildFire Appliance System Logs.....	66
Use the Firewall to Monitor WildFire Appliance Submissions.....	68
View WildFire Appliance Logs and Analysis Reports.....	69
WildFire Appliance Clusters.....	71
WildFire Appliance Cluster Resiliency and Scale.....	72

WildFire Cluster High Availability.....	74
Benefits of Managing WildFire Clusters Using Panorama.....	75
WildFire Appliance Cluster Management.....	77
Deploy a WildFire Cluster.....	81
Configure a Cluster Locally on WildFire Appliances.....	83
Configure a Cluster and Add Nodes Locally.....	83
Configure General Cluster Settings Locally.....	90
Remove a Node from a Cluster Locally.....	93
Configure WildFire Appliance-to-Appliance Encryption.....	97
Configure Appliance-to-Appliance Encryption Using Predefined Certificates Through the CLI.....	97
Configure Appliance-to-Appliance Encryption Using Custom Certificates Through the CLI.....	98
Monitor a WildFire Cluster.....	102
View WildFire Cluster Status Using the CLI.....	102
WildFire Application States.....	114
WildFire Service States.....	121
Upgrade WildFire Appliances in a Cluster.....	123
Upgrade a Cluster Locally with an Internet Connection.....	123
Upgrade a Cluster Locally without an Internet Connection.....	128
Troubleshoot a WildFire Cluster.....	134
Troubleshoot WildFire Split-Brain Conditions.....	134

Use the WildFire Appliance CLI..... 139

WildFire Appliance Software CLI Concepts.....	140
WildFire Appliance Software CLI Structure.....	140
WildFire Appliance Software CLI Command Conventions.....	140
WildFire Appliance CLI Command Messages.....	141
WildFire Appliance Command Option Symbols.....	142
WildFire Appliance Privilege Levels.....	143
WildFire CLI Command Modes.....	145
WildFire Appliance CLI Configuration Mode.....	145
WildFire Appliance CLI Operational Mode.....	148
Access the WildFire Appliance CLI.....	149
Establish a Direct Console Connection.....	149
Establish an SSH Connection.....	149
WildFire Appliance CLI Operations.....	150
Access WildFire Appliance Operational and Configuration Modes.....	150
Display WildFire Appliance Software CLI Command Options.....	150
Restrict WildFire Appliance CLI Command Output.....	151

Set the Output Format for WildFire Appliance Configuration Commands.....	152
WildFire Appliance Configuration Mode Command Reference.....	153
set deviceconfig cluster.....	153
set deviceconfig high-availability.....	154
set deviceconfig setting management.....	157
set deviceconfig setting wildfire.....	157
set deviceconfig system eth2.....	160
set deviceconfig system eth3.....	161
set deviceconfig system panorama local-panorama panorama-server.....	162
set deviceconfig system panorama local-panorama panorama-server-2.....	163
set deviceconfig system update-schedule.....	164
set deviceconfig system vm-interface.....	165
WildFire Appliance Operational Mode Command Reference.....	167
clear high-availability.....	168
create wildfire api-key.....	169
delete high-availability-key.....	170
delete wildfire api-key.....	171
delete wildfire-metadata.....	172
disable wildfire.....	173
edit wildfire api-key.....	174
load wildfire api-key.....	175
request cluster decommission.....	175
request cluster reboot-local-node.....	177
request high-availability state.....	178
request high-availability sync-to-remote.....	180
request system raid.....	181
request wildfire sample redistribution.....	182
request system wildfire-vm-image.....	184
request wf-content.....	185
save wildfire api-key.....	186
set wildfire portal-admin.....	187
show cluster all-peers.....	188
show cluster controller.....	189
show cluster data migration status.....	190
show cluster membership.....	190
show cluster task.....	193
show high-availability all.....	195
show high-availability control-link.....	196
show high-availability state.....	198
show high-availability transitions.....	199

show system raid.....	200
submit wildfire local-verdict-change.....	201
show wildfire.....	202
show wildfire global.....	204
show wildfire local.....	208
test wildfire registration.....	215

WildFire Appliance Overview

WildFire™ provides detection and prevention of zero-day malware using a combination of dynamic and static analysis to detect threats and create protections to block malware. WildFire extends the capabilities of Palo Alto Networks next-generation firewalls to identify and block targeted and unknown malware.

About the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The WildFire appliance provides an on-premises WildFire private cloud, enabling you to analyze suspicious files in a sandbox environment without requiring the firewall to send files out of network. To use the WildFire appliance to host a WildFire private cloud, configure the firewall to submit samples to the WildFire appliance for analysis. The WildFire appliance sandboxes all files locally and analyzes them for malicious behaviors using the same engine the WildFire public cloud uses. Within minutes, the private cloud returns analysis results to the firewall **WildFire Submissions** logs.



The WildFire Appliance Administration covers setting up and configuring the WildFire appliance, but shares much of the operational design and capabilities with the WildFire public cloud. For more information about the WildFire analysis capabilities, refer to the Advanced WildFire Administration.

You can enable a WildFire appliance to:

- Locally generate antivirus and DNS signatures for discovered malware, and to assign a [URL category](#) to malicious links. You can then enable connected firewalls to retrieve the latest signatures and URL categories every five minutes.
- Submit malware to the WildFire public cloud. The WildFire public cloud re-analyzes the sample and generates a signature to detect the malware—this signature can be made available within minutes to protect global users
- Submit locally-generated malware reports (without sending the raw sample content) to the WildFire public cloud, to contribute to malware statistics and threat intelligence.

You can configure up to 100 Palo Alto Networks firewalls, each with valid WildFire subscriptions, to forward to a single WildFire appliance. Beyond the WildFire firewall subscriptions, no additional WildFire subscription is required to enable a WildFire private cloud deployment.

You can manage WildFire appliances using the local appliance CLI, or you can centrally [Manage WildFire Appliances with Panorama](#). Starting with PAN-OS 8.0.1, you can also group WildFire appliances into [WildFire Appliance Clusters](#) and manage the clusters locally or from Panorama.

WildFire Private Cloud

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

In a Palo Alto Networks private cloud deployment, Palo Alto Networks firewalls forward files to a WildFire appliance on your corporate network that is being used to host a private cloud analysis location. A WildFire private cloud can receive and analyze files from up to 100 Palo Alto Networks firewalls.

Because the WildFire private cloud is a local sandbox, benign, grayware, and phishing samples that are analyzed never leave your network. By default, the private cloud also does not send discovered malware outside of your network; however, you can choose to automatically forward malware to the WildFire public cloud for signature generation and distribution. In this case, The WildFire public cloud re-analyzes the sample, generates a signature to identify the sample, and distributes the signature to all Palo Alto Networks firewalls with Threat Prevention and WildFire licenses.

If you do not want the WildFire private cloud to forward even malicious samples outside of your network, you can:

- Enable the WildFire appliance to forward the malware report (and not the sample itself) to the WildFire public cloud. WildFire reports provide statistical information that helps Palo Alto Networks assess the pervasiveness and propagation of the malware. For more details, see [Submit Malware or Reports from the WildFire Appliance](#).
- [Manually Upload Files to the WildFire Portal](#) instead of automatically forwarding all malware, or [Use the WildFire API](#) to submit files to the WildFire public cloud.

You can also [Enable Local Signature and URL Category Generation](#) on the WildFire appliance. Signatures the WildFire appliance generates are distributed to connected firewalls so that the firewalls can effectively block the malware the next time it is detected.

Android Application Package (APK) and MAC OSX files are not supported for WildFire private cloud analysis.

WildFire Hybrid Cloud

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

A firewall in a WildFire hybrid cloud deployment can forward certain samples to one of the Palo Alto Networks-hosted WildFire public clouds and other samples to a WildFire private cloud hosted by a WildFire appliance. A WildFire hybrid cloud deployment allows the flexibility to analyze private documents locally and inside your network, while the WildFire public cloud analyzes files from the Internet. For example, forward Payment Card Industry (PCI) and Protected Health Information (PHI) data exclusively to the WildFire private cloud for analysis, while forwarding Portable Executables (PEs) to the WildFire public cloud for analysis. In a WildFire hybrid cloud deployment, offloading files to the public cloud for analysis allows you benefit from a prompt verdict for files that have been previously processed in the WildFire public cloud, and also frees up the WildFire appliance capacity to process sensitive content. Additionally, you can forward certain file types to the WildFire public cloud that are not currently supported for WildFire appliance analysis, such as Android Application Package (APK) files.

In a WildFire hybrid cloud deployment, there might be some cases where a single file matches your criteria for both public cloud analysis and private cloud analysis; in these cases, the file is submitted only to the private cloud for analysis as a cautionary measure.

To set up hybrid cloud forwarding, see [Forward Files For WildFire Appliance Analysis](#).

WildFire Appliance Interfaces

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

The WF-500 appliances are equipped with four RJ-45 Ethernet ports located at the back of the appliance. These ports are labeled **MGT**, **1**, **2**, and **3** and correspond to specific interfaces.

The WildFire appliance has three interfaces:

- **MGT**—Receives all files forwarded from the firewalls and returns logs detailing the results back to the firewalls. See [Configure the WildFire Appliance](#).
- **Virtual Machine Interface (VM interface)**—Provides network access for the WildFire sandbox systems to enable sample files to communicate with the Internet, which allows WildFire to better analyze the behavior of the sample. When the VM interface is configured, WildFire can observe malicious behaviors that the malware would not normally perform without network access, such as phone-home activity. However, to prevent malware from entering your network from the sandbox, configure the VM interface on an isolated network with an Internet connection. You can also enable the Tor option to hide the public IP address used by your company from malicious sites that are accessed by the sample. For more information on the VM interface, see [Set Up the WildFire Appliance VM Interface](#).
- **Cluster Management Interface**—Provides cluster-wide communication among the WildFire appliance nodes that are members of a WildFire appliance cluster. This is a different interface than the MGT interface for firewall operations. You can configure the Ethernet2 interface or the Ethernet3 interface (labeled **2** and **3**, respectively) as the cluster management interface.

Obtain the information required to configure network connectivity on the MGT port, the VM interface, and the cluster management interface (**WildFire appliance clusters only**) from your network administrator (IP address, subnet mask, gateway, hostname, DNS server). All communication between the firewalls and the appliance occurs over the MGT port, including file submissions, WildFire log delivery, and appliance administration. Therefore, ensure that the firewalls have connectivity to the MGT port on the appliance. In addition, the appliance must be able to connect to updates.paloaltonetworks.com to retrieve its operating system software updates.

WildFire Appliance File Type Support

The following table lists the file types that are supported for analysis in the WildFire appliance private cloud and through WildFire portal direct uploads.

File Types Supported for Analysis	WildFire Private Cloud (WildFire appliance)	WildFire Portal API (direct upload; all regions)
Links contained in emails	✓	✓
Android application package (APK) files	✗	✓
Adobe Flash files	✓	✓
Java Archive (JAR) files	✓	✓
Microsoft Office files (includes SLK and IQY files**)	✓	✓
Portable executable files (includes MSI files**)	✓	✓
Portable document format (PDF) files	✓	✓
Mac OS X files	✗	✓
Linux (ELF files and Shell scripts) files	✗	✓
Archive (RAR, 7-Zip, ZIP) files*	✓	✓
Script (BAT, JS, VBS, PS1, and HTA) files	✓	✓
Script (Perl and Python) scripts	✗	✓
Archive (ZIP [direct upload] and ISO) files*	✗	✓

* ZIP files are not directly forwarded to the Wildfire cloud for analysis. Instead, they are first decoded by the firewall, and files that match the WildFire Analysis profile criteria are separately forwarded for analysis.

** The WildFire appliance does not support MSI, IQY, and SLK file analysis.

Set Up and Manage a WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

The WildFire™ appliance can be configured as a locally-hosted WildFire private cloud. The following topics describe readying the WildFire appliance to receive files for analysis, how to manage the appliance, and how to enable the appliance to locally generate threat signatures and URL categories.

- [About the WildFire Appliance](#)
- [Configure the WildFire Appliance](#)
- [Set Up Authentication Using a Custom Certificate on a Standalone WildFire Appliance](#)
- [Set Up the WildFire Appliance VM Interface](#)
- [Enable WildFire Appliance Analysis Features](#)
- [Install WildFire Appliance Device Certificate With an Internet Connection](#)

Configure the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

This section describes the steps required to integrate a WildFire appliance into a network and perform basic setup.

STEP 1 | Rack mount and cable the WildFire appliance.

Refer to the [WildFire Appliance Hardware Reference Guide](#) for instructions.

STEP 2 | Connect a computer to the appliance using the MGT or Console port and power on the appliance.

1. Connect to the console port or the MGT port. Both are located on the back of the appliance.
 - **Console Port**—This is a 9-pin male serial connector. Use the following settings on the console application: 9600-8-N-1. Connect the provided cable to the serial port on the management computer or USB-To-Serial converter.
 - **MGT Port**—This is an Ethernet RJ-45 port. By default, the MGT port IP address is 192.168.1.1. The interface on your management computer must be on the same subnet as the MGT port. For example, set the IP address on the management computer to 192.168.1.5.
2. Power on the appliance.



The appliance will power on as soon as you connect power to the first power supply and a warning beep will sound until you connect the second power supply. If the appliance is already plugged in and is in the shutdown state, use the power button on the front of the appliance to power on.

STEP 3 | Register the WildFire appliance.

1. Obtain the serial number from the S/N tag on the appliance, or run the following command and refer to the `serial` field:

```
admin@WF-500> show system info
```

2. From a browser, navigate to the [Palo Alto Networks Support Portal](#) and log in.
3. Register the device as follows:
 - If this is the first Palo Alto Networks device that you are registering and you do not have a login, click **Register** at the bottom of the page.

To register, provide an email address and the serial number of the device. When prompted, set up a username and password for access to the Palo Alto Networks support community.
 - For existing accounts, log in and then click **My Devices**. Scroll down to the **Register Device** section at the bottom of the screen and enter the serial number of the device, the city and postal code, and then click **Register Device**.
4. To confirm WildFire registration on the WildFire appliance, log in to the appliance with an SSH client or by using the Console port. Enter a username/password of admin/admin and enter the following command on the appliance:

```
admin@WF-500> test wildfire registration
```

The following output indicates that the appliance is registered with one of the Palo Alto Networks WildFire cloud servers.

```
Test wildfire
wildfire registration: successful
download server list: successful
select the best server:
cs-s1.wildfire.paloaltonetworks.com
```

STEP 4 | Reset the admin password.

1. Set a new password by running the command:

```
admin@WF-500> set password
```

2. Type the old password, press enter and then enter and confirm the new password. Commit the configuration to ensure that the new password is saved in the event of a restart.



Starting with PAN-OS 9.0.4, the predefined, default administrator password (admin/admin) must be changed on the first login on a device. The new password must be a minimum of eight characters and include a minimum of one lowercase and one uppercase character, as well as one number or special character.

Be sure to use the [best practices for password strength](#) to ensure a strict password.

3. Type **exit** to log out and then log back in to confirm that the new password is set.

STEP 5 | Configure the management interface settings.

This example uses the following IPv4 values, but the appliance also supports IPv6 addresses:

- IPv4 address - 10.10.0.5/22
- Subnet Mask - 255.255.252.0
- Default Gateway - 10.10.0.1
- Hostname - wildfire-corp1
- DNS Server - 10.0.0.246

1. Log in to the appliance with an SSH client or by using the Console port and enter configuration mode:

```
admin@WF-500> configure
```

2. Set the IP information:

```
admin@WF-500# set deviceconfig system ip-address 10.10.0.5  
netmask 255.255.252.0 default-gateway 10.10.0.1 dns-setting  
servers primary 10.0.0.246
```



Configure a secondary DNS server by replacing primary with secondary in the above command, excluding the other IP parameters. For example:

```
admin@WF-500# set deviceconfig system dns-setting servers  
secondary 10.0.0.247
```

3. Set the hostname (wildfire-corp1 in this example):


```
admin@WF-500# set deviceconfig system hostname wildfire-corp1
```

4. Commit the configuration to activate the new management (MGT) port configuration:

```
admin@WF-500# commit
```

5. Connect the MGT interface port to a network switch.
6. Put the management PC back on your corporate network, or whatever network is required to access the appliance on the management network.
7. From your management computer, use an SSH client to connect to the new IP address or hostname assigned to the MGT port on the appliance. In this example, the IP address is 10.10.0.5.

STEP 6 | Activate the appliance with the WildFire authorization code that you received from Palo Alto Networks.

 *Though it will function without an auth-code, the WildFire appliance cannot retrieve software or content updates without a valid auth-code.*

1. Change to operational mode:

```
admin@WF-500# exit
```

2. Fetch and install the WildFire license:

```
admin@WF-500> request license fetch auth-code <auth-code>
```

3. Verify the license:

```
admin@WF-500> request support check
```


Information about the support site and the support contract date is displayed. Confirm that the date displayed is valid.

STEP 7 | Set the WildFire appliance clock.

There are two ways to do this. You can either manually set the date, time, and timezone or you can configure the WildFire appliance to synchronize its local clock with a Network Time Protocol (NTP) server.


- To set the clock manually, enter the following commands:

```
admin@WF-500> set clock date <YYYY/MM/DD> time <hh:mm:ss>
admin@WF-500> configure
admin@WF-500# set deviceconfig system timezone <timezone>
```

 *The time stamp that will appear on the WildFire detailed report will use the time zone set on the appliance. If administrators in various regions will view reports, consider setting the time zone to UTC.*

- To configure the WildFire appliance to synchronize with an NTP server, enter the following commands:

```
admin@WF-500> configure
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server ntp-server-address <NTP primary server IP address>
admin@WF-500# set deviceconfig system ntp-servers secondary-ntp-
server ntp-server-address <NTP secondary server IP address>
```

 *The WildFire appliance does not prioritize the primary or secondary NTP server; it synchronizes with either server.*

STEP 8 | (Optional for NTP configuration) Set up NTP authentication.

- Disable NTP authentication:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server authentication-type none
```

- Enable symmetric key exchange (shared secrets) to authenticate the NTP server time updates:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server authentication-type symmetric-key
```

Continue to enter the **key-ID** (1 - 65534), choose the **algorithm** to use in NTP authentication (**MD5** or **SHA1**), and then enter and confirm the authentication algorithm **authentication-key**.

- Use autokey (public key cryptography) to authenticate the NTP server time updates:

```
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-server authentication-type autokey
```

STEP 9 | Choose the virtual machine image for the appliance to use to analyze files.

The image should be based on the attributes that most accurately represent the software installed on your end user computers. Each virtual image contains different versions of operating systems and software, such as Windows XP or Windows 7 32-bit or 64-bit and specific versions of Adobe Reader, and Flash. Although you configure the appliance to use one virtual machine image configuration, the appliance uses multiple instances of the image to improve performance.

- To view a list of available virtual machines to determine which one best represents your environment:

```
admin@WF-500> show wildfire vm-images
```

- View the current virtual machine image by running the following command and refer to the Selected VM field:

```
admin@WF-500> show wildfire status
```

- Select the image that the appliance will use for analysis:

```
admin@WF-500# set deviceconfig setting wildfire active-vm <vm-image-number>
```

For example, to use vm-5:

```
admin@WF-500# set deviceconfig setting wildfire active-vm vm-5
```

STEP 10 | Enable the WildFire appliance to observe malicious behaviors where the file being analyzed seeks network access.

[Set Up the WildFire Appliance VM Interface.](#)

STEP 11 | [#unique_16](#)

STEP 12 | (Optional) Enable the WildFire appliance to perform quick verdict lookups and synchronize verdicts with the WildFire public cloud.

The following CLI command enables the WildFire appliance to perform verdict lookups and synchronize verdicts with the WildFire public cloud. This feature is disabled by default; set the command to **yes** to enable the feature.

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence
cloud-query yes | no
```

STEP 13 | (Optional) Enable the WildFire appliance to get daily Palo Alto Networks content updates to facilitate and improve malware analysis.

[Enable WildFire Appliance Analysis Features](#)

STEP 14 | (Optional) Enable the WildFire appliance to generate DNS and antivirus signatures and URL categories, and to distribute new signatures and URL categorizations to connected firewalls.

[Enable Local Signature and URL Category Generation](#)

STEP 15 | (Optional) Automatically submit malware the WildFire private cloud discovers to the WildFire public cloud, to support global protection against the malware.

[Submit Malware to the WildFire Public Cloud..](#)

STEP 16 | (Optional) If you do not want to forward malware samples outside of the WildFire private cloud, instead submit WildFire analysis reports to the WildFire public cloud.



If you do not want to submit locally-discovered malware to the WildFire public cloud, it is a best practice to enable malware analysis report submissions to improve and refine WildFire threat intelligence.

[Submit Analysis Reports to the WildFire Public Cloud.](#)

STEP 17 | (Optional) Allow additional users to manage the WildFire appliance.

You can assign two role types: superuser and superreader. Superuser is equivalent to the admin account, and superreader only has read access.

In this example, you will create a superreader account for the user bsimpson:

1. Enter configuration mode:

```
admin@WF-500> configure
```

2. Create the user account:

```
admin@WF-500# set mgt-config users bsimpson <password>
```

3. Enter and confirm a new password.
4. Assign the superreader role:

```
admin@WF-500# set mgt-config users bsimpson permissions role-based superreader yes
```

STEP 18 | Configure RADIUS authentication for administrator access.

1. Create a RADIUS profile using the following options:

```
admin@WF-500# set shared server-profile radius <profile-name>
```

(Configure the RADIUS server and other attributes.)

2. Create an authentication profile:

```
admin@WF-500# set shared authentication-profile <profile-name>  
method radius server-profile <server-profile-name>
```

3. Assign the profile to a local admin account:

```
admin@WF-500# set mgt-config users username authentication-profile <authentication-profile-name>
```

Forward Files For WildFire Appliance Analysis

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Configure Palo Alto Networks firewalls to forward unknown files or email links and blocked files that match existing antivirus signatures for analysis. Use the **WildFire Analysis** profile to define files to forward to the WildFire private cloud (or additionally, the public cloud for hybrid cloud deployments), and then attach the profile to a security rule to trigger inspection for zero-day malware.

Specify traffic to be forwarded for analysis based on the application in use, the file type detected, links contained in email messages, or the transmission direction of the sample (upload, download, or both). For example, you can set up the firewall to forward Portable Executables (PEs) or any files that users attempt to download during a web-browsing session. In addition to unknown samples, the firewall forwards blocked files that match existing antivirus signatures. This provides Palo Alto Networks a valuable source of threat intelligence based on malware variants that signatures successfully prevented but neither WildFire nor the firewall has seen before.

You can extend WildFire analysis resources to a [WildFire Hybrid Cloud](#), by configuring the firewall to continue to forward sensitive files to your WildFire private cloud for local analysis, and forward less sensitive or unsupported file types to the WildFire public cloud.

Additionally, you can dedicate WildFire appliance resources to analyze specific file types: either documents (Microsoft Office files and PDFs) or PEs. For example, if you deploy a [WildFire Hybrid Cloud](#) to analyze documents locally and PEs in one of the WildFire public clouds, you can dedicate all analysis environments to documents. This allows you to offload analysis of PEs to the public cloud, allowing you to allocate additional WildFire appliance resources to process sensitive documents.

Before you begin:

- If another firewall resides between the firewall you are configuring to forward files and the WildFire cloud or WildFire appliance, make sure that the firewall in the middle allows the following ports:

Port	Usage
443	<ul style="list-style-type: none"> • Registration • PCAP Downloads • Sample Downloads • Report Retrieval • File Submission • PDF Report Downloads
10443	Dynamic Updates

STEP 1 | (PA-7000 Series Firewalls Only) To enable a PA-7000 Series firewall to forward samples for WildFire analysis, you must first [configure a data port on an NPC as a Log Card interface](#). If you have a PA-7000 series appliance equipped with an LFC ([log forwarding card](#)), you must [configure a port used by the LFC](#). When configured, the log card port or the LFC interface takes precedence over the management port when forwarding WildFire samples.

STEP 2 | Specify the WildFire private or hybrid cloud to which you want to forward samples.

Select **Device > Setup > WildFire** and edit the General Settings based on your WildFire cloud deployment (private or hybrid).

WildFire Private Cloud:

1. Enter the IP address or FQDN of the WildFire appliance in the **WildFire Private Cloud** field.

WildFire Hybrid Cloud:

1. Enter the **WildFire Public Cloud** URL:
 - United States: **wildfire.paloaltonetworks.com**
 - Europe: **eu.wildfire.paloaltonetworks.com**
 - Japan: **jp.wildfire.paloaltonetworks.com**
 - Singapore: **sg.wildfire.paloaltonetworks.com**
 - United Kingdom: **uk.wildfire.paloaltonetworks.com**
 - Canada: **ca.wildfire.paloaltonetworks.com**
 - Australia: **au.wildfire.paloaltonetworks.com**
 - Germany: **de.wildfire.paloaltonetworks.com**
 - India: **in.wildfire.paloaltonetworks.com**
 - Switzerland: **ch.wildfire.paloaltonetworks.com**
 - Poland: **pl.wildfire.paloaltonetworks.com**
 - Indonesia: **id.wildfire.paloaltonetworks.com**
 - Taiwan: **tw.wildfire.paloaltonetworks.com**
 - France: **fr.wildfire.paloaltonetworks.com**
 - Qatar: **qatar.wildfire.paloaltonetworks.com**
 - South Korea: **kr.wildfire.paloaltonetworks.com**
2. Enter the IP address or FQDN of the WildFire appliance in the **WildFire Private Cloud** field.

STEP 3 | Define the size limits for files the firewall forwards and configure WildFire logging and reporting settings.

Continue editing WildFire General Settings (**Device > Setup > WildFire**).

- Review the **File Size Limits** for files forwarded from the firewall.



*It is a **recommended WildFire best practice** to set the **File Size** for PEs to the maximum size limit of 10 MB, and to leave the **File Size** for all other file types set to the default value.*

- Select **Report Benign Files** to allow logging for files that receive a WildFire verdict of benign.
- Select **Report Grayware Files** to allow logging for files that receive a WildFire verdict of grayware.
- Define what session information is recorded in WildFire analysis reports by editing the Session Information Settings. By default, all session information is displayed in WildFire analysis reports. Clear the check boxes to remove the corresponding fields from WildFire analysis reports and click **OK** to save the settings.

STEP 4 | (**Panorama Only**) Configure Panorama to gather additional information about samples collected from firewalls running a PAN-OS version prior to PAN-OS 7.0.

Some WildFire Submissions log fields introduced in PAN-OS 7.0 are not populated for samples submitted by firewalls running earlier software versions. If you are using Panorama to manage firewalls running software versions earlier than PAN-OS 7.0, Panorama can communicate with WildFire to gather complete analysis information for samples submitted by those firewalls from the defined **WildFire Server** (the WildFire global cloud, by default) to complete the log details.

Select **Panorama > Setup > WildFire** and enter a **WildFire Server** if you'd like to modify the default setting to instead allow Panorama to gather details from the specified WildFire cloud or from a WildFire appliance.

STEP 5 | Define traffic to forward for WildFire analysis.

If you have a WildFire appliance set up, you can use both the private cloud and the public cloud in a hybrid cloud deployment. Analyze sensitive files locally on your network, while sending all other unknown files to the WildFire public cloud for comprehensive analysis and prompt verdict returns.

1. Select **Objects > Security Profiles > WildFire Analysis**, **Add** a new WildFire analysis profile, and give the profile a descriptive **Name**.
2. **Add** a profile rule to define traffic to be forwarded for analysis and give the rule a descriptive **Name**, such as local-PDF-analysis.
3. Define for the profile rule to match to unknown traffic and to forward samples for analysis based on:
 - **Applications**—Forward files for analysis based on the application in use.
 - **File Types**—Forward files for analysis based on file types, including links contained in email messages. For example, select **PDF** to forward unknown PDFs detected by the firewall for analysis.
 - **Direction**—Forward files for analysis based the transmission direction of the file (upload, download, or both). For example, select **both** to forward all unknown PDFs for analysis, regardless of the transmission direction.
4. Set the **Analysis** location to which the firewall forwards files matched to the rule.
 - Select **public-cloud** to forward matching samples to the WildFire public cloud for analysis.
 - Select **private-cloud** to forward matching samples to a WildFire private cloud for analysis.

For example, to analyze PDFs that could contain sensitive or proprietary information without sending these documents out of your network, set the **Analysis** location for the rule local-PDF-analysis to **private-cloud**.

<input type="checkbox"/>	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input checked="" type="checkbox"/>	local-PDF-analysis	any	pdf	both	public-cloud



Different rules can forward matched samples to different analysis locations, depending on your needs. The example above shows a rule that forwards sensitive file types for local analysis in a WildFire private cloud. You could create another rule to forward less sensitive file types, such as PEs, to the WildFire public cloud. This flexibility is supported with a [WildFire hybrid cloud deployment](#).



In a hybrid cloud deployment, files that match to both **private-cloud** and **public-cloud** rules are forwarded only to the private cloud as a cautionary measure.

5. (**Optional**) Continue to add rules to the WildFire analysis profile as needed. For example, you could add a second rule to the profile to forward Android application package (APK), Portable Executable (PE), and Flash files to the WildFire public cloud for analysis.
6. Click **OK** to save the WildFire analysis profile.

7. (Optional) Continue to add rules to the WildFire analysis profile as needed. For example, you could add a second rule to the profile to forward Android application package (APK), Portable Executable (PE), and Flash files to the WildFire public cloud for analysis.
8. Click **OK** to save the WildFire analysis profile.

STEP 6 | (Optional) Allocate WildFire appliance resources to analyze either documents or executables.



If you are deploying a hybrid cloud to analyze specific file types locally and in the WildFire public cloud, you can dedicate analysis environments to process a file type. This allows you to better allocate resources according to your analysis environment configuration. If you do not dedicate resources for an analysis environment, resources are allocated using default settings.

Use the following CLI command:

```
admin@WF-500# set
deviceconfig setting wildfire preferred-analysis-environment
documents
| executables | default
```

and choose from one of the following options:

- documents—Dedicate analysis resources to concurrently analyze 25 documents, 1 PE, and 2 email links.
- executables—Dedicate analysis resources to concurrently analyze 25 PEs, 1 documents, and 2 email links.
- default—The appliance concurrently analyzes 16 documents, 10 portable executables (PE), and 2 email links.

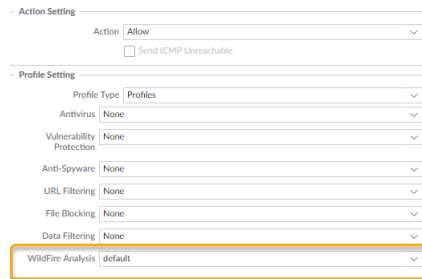
Confirm that all WildFire appliances processes are running by running the following command:

```
admin@WF-500> show system
software status
```

STEP 7 | Attach the WildFire Analysis profile to a security policy rule.

Traffic allowed by the security policy rule is evaluated against the attached WildFire analysis profile; the firewall forwards traffic matched to the profile for WildFire analysis.

1. Select **Policies > Security** and **Add** or modify a policy rule.
2. Click the **Actions** tab within the policy rule.
3. In the Profile Settings section, select **Profiles** as the **Profile Type** and select a **WildFire Analysis** profile to attach to the policy rule



STEP 8 | Make sure to enable the firewall to also [Forward Decrypted SSL Traffic for WildFire Analysis](#).



This is a [recommended WildFire best practice](#).

STEP 9 | Review and implement [WildFire Best Practices](#).

STEP 10 | Click **Commit** to apply the WildFire settings.

STEP 11 | (Optional) [Verify WildFire Submissions](#).

STEP 12 | Choose what to do next...

- [Verify WildFire Submissions](#) to confirm that the firewall is successfully forwarding files for WildFire analysis.
- [Submit Malware or Reports from the WildFire Appliance](#). Enable this feature to automatically forward malware identified in your WildFire private cloud to the WildFire public cloud. The WildFire public cloud re-analyzes the sample and generates a signature if the sample is malware. The signature is distributed to global users through Wildfire signature updates.
- [Monitor WildFire Appliance Activity](#) to assess alerts and details reported for malware.

Submit Malware or Reports from the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Enable the WildFire appliance cloud intelligence feature to automatically submit malware samples discovered in the WildFire private cloud to the WildFire public cloud. The WildFire public cloud further analyzes the malware and generates a signature to identify the sample. The signature is then added to WildFire signature updates, and distributed to global users to prevent future exposure to the threat. If you do not want to forward malware samples outside of your network, you can instead choose to submit only WildFire reports for the malware discovered on your network to contribute to WildFire statistics and threat intelligence.

- **Submit Malware to the WildFire Public Cloud**

Execute the following CLI command from the WildFire appliance to enable the appliance to automatically submit malware samples to the WildFire public cloud:

```
admin@WF-500admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
```



If the firewall that originally submitted the sample for WildFire private cloud analysis has packet captures (PCAPs) enabled, the PCAPs for the malware will also be forwarded to the WildFire public cloud.

- **Submit Malware Reports to the WildFire Public Cloud**



If the WildFire appliance is enabled to [Submit Malware to the WildFire Public Cloud](#), you do not need to also enable the appliance to submit malware reports to the public cloud. When malware is submitted to the WildFire public cloud, the public cloud generates a new malware report for the sample.

To enable the WildFire appliance to automatically submit malware reports to the WildFire public cloud (and not the malware sample), execute the following CLI command on the WildFire appliance:

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-report yes
```

- Verify Cloud Intelligence Settings

Check to confirm that cloud intelligence is enabled to either submit malware or submit malware reports to the WildFire public cloud by running the following command:

```
admin@WF-500> show wildfire status
```

Refer to the `Submit sample` and `Submit report` fields.

Set Up Authentication Using a Custom Certificate on a Standalone WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

By default, a WildFire appliance uses predefined certificates for mutual authentication to establish the SSL connections used for management access and inter-device communication. However, you can configure authentication using custom certificates instead. Custom certificates allow you to establish a unique chain of trust to ensure mutual authentication between your WildFire appliance and firewalls or Panorama. You can generate these certificates locally on Panorama or a the firewall, obtain them from a trusted third-party certificate authority (CA), or obtain certificates from enterprise private key infrastructure (PKI).

The following topics describe how to configure standalone WildFire appliances that are not managed by Panorama. For configuring custom certificates for WildFire appliances and WildFire cluster managed by Panorama, see the [Panorama Admin Guide](#).

- [WildFire Appliance Mutual SSL Authentication](#)
- [Configure Authentication with Custom Certificates on the WildFire Appliance](#)

WildFire Appliance Mutual SSL Authentication

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

When a firewall or Panorama sends a sample to a WildFire appliance for analysis, the firewall acts as the client and the WildFire appliance acts as the server. To mutually authenticate, each device presents a certificate to identify itself to the other device.

To deploy custom certificates for mutual authentication in your deployment, you need:

- **SSL/TLS Service Profile**—An [SSL/TLS service profile](#) defines the security of the connections by referencing your custom certificate and establishing the SSL/TLS protocol version the server device uses to communicate with client devices.
- **Server Certificate and Profile**—A WildFire appliance requires a certificate and certificate profile to identify itself to firewalls. You can [deploy this certificate](#) from your enterprise public key infrastructure (PKI), purchase one from a trusted third-party CA, or generate a self-signed certificate locally. The server certificate must include the IP address or FQDN of the WildFire appliance's management interface in the certificate common name (CN) or Subject Alt Name. The firewall matches the CN or Subject Alt Name in the certificate the server presents against the WildFire appliance's IP address or FQDN to verify the WildFire appliance's identity.

Additionally, use the certificate profile to define [certificate revocation](#) status (OCSP/CRL) and the actions taken based on the revocation status.

- **Client Certificates and Profile**—Each firewall requires a client certificate and [certificate profile](#). The client device uses its certificate to identify itself to the server device. You can [deploy certificates](#) from your enterprise PKI using Simple Certificate Enrollment Protocol (SCEP), purchase one from a trusted third-party CA, or generate a self-signed certificate locally.

Custom certificates can be unique to each client device or common across all devices. The unique device certificates uses a hash of the serial number of the managed device and CN. The server matches the CN or the subject alt name against the configured serial numbers of the client devices. For client certificate validation based on the CN to occur, the username must be set to Subject common-name.

Configure Authentication with Custom Certificates on the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Use the following workflow to replace predefined certificates to custom certificates in your WildFire deployment. When a firewall or Panorama sends a sample to a WildFire appliance for analysis, the firewall acts as the client and the WildFire appliance acts as the server.

STEP 1 | [Obtain](#) key pairs and certificate authority (CA) certificates for the WildFire appliance and firewall or Panorama.

STEP 2 | Import the CA certificate to validate the certificate one the firewall.

1. Log in to the CLI on the WildFire appliance and enter configuration mode.

```
admin@WF-500> configure
```

2. Use TFTP or SCP to import the certificate.

```
admin@WF-500#{tftp | scp} import certificate from <value>
file <value> remote-port <1-65535> source-ip <ip/netmask>
certificate-name <value> passphrase <value> format {pkcs12 |
pem}
```

STEP 3 | Use TFTP or SCP to import the keypair that contains the server certificate and private key for the WildFire appliance.

```
admin@WF-500# {tftp | scp} import keypair from <value> file <value>
remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | Configure a certificate profile that includes the root CA and intermediate CA. This certificate profile defines how the WildFire appliance and the firewalls will authenticate mutually.

1. In the CLI of the WildFire appliance, enter configuration mode.

```
admin@WF-500> configure
```

2. Name the certificate profile.

```
admin@WF-500# set shared certificate-profile <name>
```

3. Configure the CA.



The commands `default-ocsp-url` and `ocsp-verify-cert` are optional.

```
admin@WF-500# set shared certificate-profile <name> CA <name>
```

```
admin@WF-500# set shared certificate-profile <name> CA <name>  
[default-ocsp-url <value>]
```

```
admin@WF-500# set shared certificate-profile <name> CA <name>  
[ocsp-verify-cert <value>]
```

STEP 5 | Configure an SSL/TLS profile for the WildFire appliance. This profile defines the certificate and SSL/TLS protocol range that WildFire appliance and firewalls use for SSL/TLS services.

1. Identify the SSL/TLS profile.

```
admin@WF-500# set shared ssl-tls-service-profile <name>
```

2. Select the certificate.

```
admin@WF-500# set shared ssl-tls-service-profile <name>  
certificate <value>
```

3. Define the SSL/TLS range.



PAN-OS 8.0 and later releases support TLS 1.2 and later TLS versions only. You must set the max version to TLS 1.2 or max.

```
admin@WF-500# set shared ssl-tls-service-profile <name>  
protocol-settings min-version {tls1-0 | tls1-1 | tls1-2}
```

```
admin@WF-500# set shared ssl-tls-service-profile <name>  
protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 |  
max}
```

STEP 6 | Configure secure server communication on the WildFire appliance.

1. Set the SSL/TLS profile. This SSL/TLS service profile applies to all SSL connection between WildFire and client devices.

```
admin@WF-500# set deviceconfig setting management secure-conn-  
server ssl-tls-service-profile <ssl-tls-profile>
```

2. Set the certificate profile.

```
admin@WF-500# set deviceconfig setting management secure-conn-  
server certificate-profile <certificate-profile>
```

Set Up the WildFire Appliance VM Interface

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The virtual machine interface (vm-interface) provides external network connectivity from the sandbox virtual machines in the WildFire appliance to enable observation of malicious behaviors in which the file being analyzed seeks network access. The following sections describe the VM interface and the steps required for configuring it. You can optionally enable the Tor feature with the VM interface, which will mask any malicious traffic sent from the WildFire appliance through the VM interface, so the malware sites that the traffic may be sent to cannot detect your public-facing IP address.


This section also describes the steps required to connect the VM interface to a dedicated port on a Palo Alto Networks firewall to enable Internet connectivity.

- [Virtual Machine Interface Overview](#)
- [Configure the VM Interface on the WildFire Appliance](#)
- [Connect the Firewall to the WildFire Appliance VM Interface](#)

Virtual Machine Interface Overview

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The VM interface (labeled **1** on the back of the appliance) is used by WildFire to improve malware detection capabilities. The interface allows a sample running on the WildFire virtual machines to communicate with the Internet so that the WildFire appliance can better analyze the behavior of the sample file to determine if it exhibits characteristics of malware.

- 
 - *While it is recommended that you enable the VM interface, it is very important that you do not connect the interface to a network that allows access to any of your servers/hosts because malware that runs in the WildFire virtual machines could potentially use this interface to propagate itself.*
 - *This connection can be a dedicated DSL line or a network connection that only allows direct access from the VM interface to the Internet and restricts any access to internal servers/client hosts.*
 - *The VM interface on WildFire appliances operating in FIPS/CC mode is disabled.*

The following illustration shows two options for connecting the VM interface to the network.

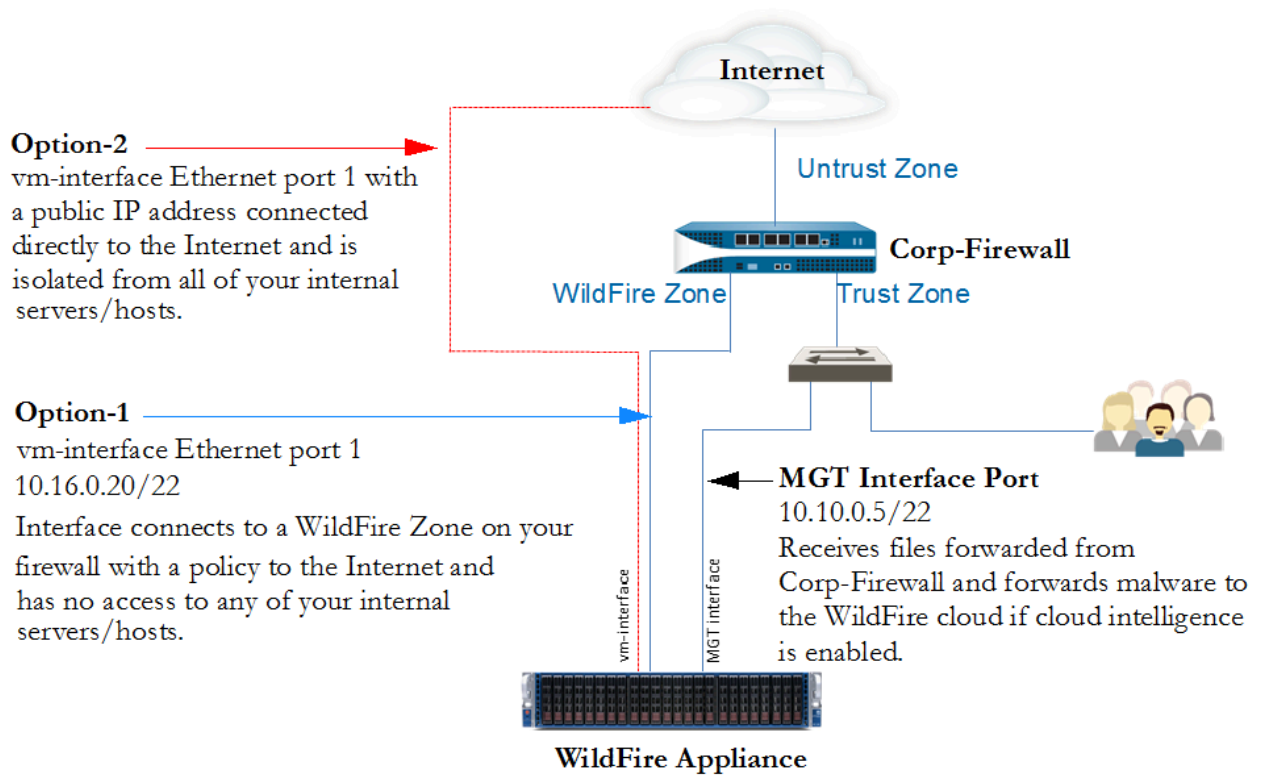


Figure 1: Virtual Machine Interface Example

- **Option-1 (recommended)**—Connect the VM interface to an interface in a dedicated zone on a firewall that has a policy that only allows access to the Internet. This is important because malware that runs in the WildFire virtual machines can potentially use this interface to propagate itself. This is the recommended option because the firewall logs will provide visibility into any traffic that is generated by the VM interface.
- **Option-2**—Use a dedicated Internet provider connection, such as a DSL, to connect the VM interface to the Internet. Ensure that there is no access from this connection to internal servers/hosts. Although this is a simple solution, traffic generated by the malware out the VM interface will not be logged unless you place a firewall or a traffic monitoring tool between the WildFire appliance and the DSL connection.

Configure the VM Interface on the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

This section describes the steps required to configure the VM interface on the WildFire appliance using the Option 1 configuration detailed in the [Virtual Machine Interface Example](#). After configuring the VM interface using this option, you must also configure an interface on a Palo Alto Networks firewall through which traffic from the VM interface is routed as described in [Connect the Firewall to the WildFire Appliance VM Interface](#).

By default, the VM interface has the following settings:

- IP Address: 192.168.2.1
- Netmask: 255.255.255.0
- Default Gateway: 192.168.2.254
- DNS: 192.168.2.254

If you plan on enabling this interface, configure it with the appropriate settings for your network. If you do not plan on using this interface, leave the default settings. Note that this interface must have network values configured or a commit failure will occur.

STEP 1 | Set the IP information for the VM interface on the WildFire appliance. The following IPv4 values are used in this example, but the appliance also supports IPv6 addresses:

- IP address - 10.16.0.20/22
- Subnet Mask - 255.255.252.0
- Default Gateway - 10.16.0.1
- DNS Server - 10.0.0.246



The VM interface cannot be on the same network as the management interface (MGT).

1. Enter configuration mode:

```
admin@WF-500> configure
```

2. Set the IP information for the VM interface:

```
admin@WF-500# set  
deviceconfig system vm-interface ip-address 10.16.0.20 netmask  
255.255.252.0  
default-gateway 10.16.0.1 dns-server 10.0.0.246
```



You can only configure one DNS server on the VM interface. As a best practice, use the DNS server from your ISP or an open DNS service.

STEP 2 | Enable the VM interface.

1. Enable the VM interface:

```
admin@WF-500# set  
deviceconfig setting wildfire vm-network-enable yes
```

2. Commit the configuration:

```
admin@WF-500# commit
```

STEP 3 | Test connectivity of the VM interface.

Ping a system and specify the VM interface as the source. For example, if the VM interface IP address is 10.16.0.20, run the following command where *ip-or-hostname* is the IP or hostname of a server/network that has ping enabled:

```
admin@WF-500> ping  
source 10.16.0.20 host ip-or-hostname
```

For example:

```
admin@WF-500> ping  
source 10.16.0.20 host 10.16.0.1
```

STEP 4 | (Optional) Send any malicious traffic that the malware generates to the Internet. The Tor network masks your public facing IP address, so the owners of the malicious site cannot determine the source of the traffic.

1. Enable the Tor network:

```
admin@WF-500# set
deviceconfig setting wildfire vm-network-use-tor
```

2. Commit the configuration:

```
admin@WF-500# commit
```

STEP 5 | (Optional) Verify that the Tor network connection is active and healthy.

1. Issue the following CLI commands to search for Tor event IDs in the appliance logs. A properly configured and operational WildFire appliance should not generate any event IDs:
 - **admin@WF-500(active-controller)>showlog system direction equal backward | match anonymous-network-unhealthy**—The Tor service is down or otherwise non-operational. Consider restarting your Tor service and verify that it is operating properly.
 - **admin@WF-500(active-controller)>show log systemdirection equal backward | match anonymous-network-unavailable**—The Tor service is operating normally but the WildFire appliance VM interface is unable to establish a connection. Verify your network connections and settings and re-test.


STEP 6 | [Connect the Firewall to the WildFire Appliance VM Interface.](#)

Connect the Firewall to the WildFire Appliance VM Interface

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

The following example workflow describes how to connect the VM interface to a port on a Palo Alto Networks firewall. Before connecting the VM interface to the firewall, the firewall must already have an Untrust zone connected to the Internet. In this example, you configure a new zone named wf-vm-zone that will contain the interface used to connect the VM interface on the appliance to the firewall. The policy associated with the wf-vm-zone will only allow communication from the VM interface to the Untrust zone.


STEP 1 | Configure the interface on the firewall that the VM interface will connect to and set the virtual router.

 *The wf-vm-zone should only contain the interface (ethernet1/3 in this example) used to connect the VM interface on the appliance to the firewall. This is done to avoid having any traffic generated by the malware from reaching other networks.*

1. From the web interface on the firewall, select **Network > Interfaces** and then select an interface, for example **Ethernet1/3**.
2. In the **Interface Type** drop-down, select **Layer3**.
3. On the **Config** tab, from the **Security Zone** drop-down box, select **New Zone**.
4. In the Zone dialog **Name** field, enter wf-vm-zone and click **OK**.
5. In the **Virtual Router** drop-down box, select **default**.
6. To assign an IP address to the interface, select the **IPv4** or **IPv6** tab, click **Add** in the IP section, and enter the IP address and network mask to assign to the interface, for example 10.16.0.0/22 (IPv4) or 2001:db8:123:1::1/64 (IPv6).
7. To save the interface configuration, click **OK**.

STEP 2 | Create a security policy on the firewall to allow access from the VM interface to the Internet and block all incoming traffic. In this example, the policy name is WildFire VM Interface. Because you will not create a security policy from the Untrust zone to the wf-vm-interface zone, all inbound traffic is blocked by default.

1. Select **Policies > Security** and click **Add**
2. In the **General** tab, enter a **Name**.
3. In the **Source** tab, set the **Source Zone** to **wf-vm-zone**.
4. In the **Destination** tab, set the **Destination Zone** to **Untrust**.
5. In the **Application** and **Service/URL Category** tabs, leave the default as **Any**.
6. In the **Actions** tab, set the **Action Setting** to **Allow**.
7. Under **Log Setting**, select the **Log at Session End** check box.

 *If there are concerns that someone might inadvertently add other interfaces to the wf-vm-zone, clone the WildFire VM Interface security policy and then in the **Action** tab for the cloned rule, select **Deny**. Make sure this new security policy is listed below the WildFire VM interface policy. This will override the implicit intra-zone allow rule that allows communications between interfaces in the same zone and will deny/block all intra-zone communication.*

STEP 3 | Connect the cables.

Physically connect the VM interface on the WildFire appliance to the port you configured on the firewall (Ethernet 1/3 in this example) using a straight through RJ-45 cable. The VM interface is labeled **1** on the back of the appliance.

Enable WildFire Appliance Analysis Features

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">☐ WildFire License

- [Set Up WildFire Appliance Content Updates](#)
- [Enable Local Signature and URL Category Generation](#)
- [Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud](#)

Set Up WildFire Appliance Content Updates

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">☐ WildFire License

Configure daily content updates for the WildFire appliance. WildFire content updates provide the appliance with threat intelligence to facilitate accurate malware detection, improve appliance capability to differentiate malicious samples from benign samples, and ensure that the appliance has the most recent information needed to generate signatures.

- [Install WildFire Content Updates Directly from the Update Server](#)
- [Install WildFire Content Updates from an SCP-Enabled Server](#)

Install WildFire Content Updates Directly from the Update Server

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">☐ WildFire License

STEP 1 | Verify connectivity from the appliance to the update server and identify the content update to install.

1. Log in to the WildFire appliance and run the following command to display the current content version:

```
admin@WF-500> show system info | match wf-content-version
```

2. Confirm that the appliance can communicate with the Palo Alto Networks Update Server and view available updates:

```
admin@WF-500> request wf-content upgrade check
```

The command queries the Palo Alto Networks Update Server and provides information about available updates and identifies the version that is currently installed on the appliance.

Version	Size	Released on	Downloaded	Installed
2-253	57MB	2014/09/20 20:00:08 PDT	no	no
2-39	44MB	2014/02/12 14:04:27 PST	yes	current

If the appliance cannot connect to the update server, you will need to allow connectivity from the appliance to the Palo Alto Networks Update Server (updates.paloaltonetworks.com), or download and install the update using SCP as described in [Install WildFire Content Updates from an SCP-Enabled Server](#).

STEP 2 | Download and install the latest content update.

1. Download the latest content update:

```
admin@WF-500> request wf-content upgrade download latest
```

2. View the status of the download:

```
admin@WF-500> show jobs all
```

You can run **show jobs pending** to view pending jobs. The following output shows that the download (job id 5) has finished downloading (Status FIN):

Enqueued	ID	Type	Status	Result	Completed
2014/04/22 03:42:20	5	Downld	FIN	OK	03:42:23

3. After the download is complete, install the update:

```
admin@WF-500> request wf-content upgrade install version latest
```

Run the **show jobs all** command again to monitor the status of the install.

STEP 3 | Verify the content update.

Run the following command and refer to the `wf-content-version` field:

```
admin@WF-500> show system info
```

The following shows an example output with content update version 2-253 installed:

```
admin@WF-500> show system info
hostname: WildFire
ip-address: 10.5.164.245
netmask: 255.255.255.0
default-gateway: 10.5.164.1
mac-address: 00:25:90:c3:ed:56
vm-interface-ip-address: 192.168.2.2
vm-interface-netmask: 255.255.255.0
vm-interface-default-gateway: 192.168.2.1
vm-interface-dns-server: 192.168.2.1
time: Mon Apr 21 09:59:07 2014
uptime: 17 days, 23:19:16
family: m
model: WildFire
serial: abcd3333
sw-version: 6.1.0
wf-content-version: 2-253
wfm-release-date: 2014/08/20 20:00:08
logdb-version: 6.1.2
platform-family: m
```

STEP 4 | (Optional) Schedule content updates to be installed on a daily or weekly basis.

1. Schedule the appliance to download and install content updates:

```
admin@WF-500# set deviceconfig system update-schedule wf-
content recurring [daily | weekly] action [download-and-
install | download-only]
```

For example, to download and install updates daily at 8:00 am:

```
admin@WF-500# set deviceconfig system update-schedule wf-
content recurring daily action download-and-install at 08:00
```

2. Commit the configuration

```
admin@WF-500# commit
```

Install WildFire Content Updates from an SCP-Enabled Server

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The following procedure describes how to install threat intelligence content updates on a WildFire appliance that does not have direct connectivity to the Palo Alto Networks Update Server. You will need a Secure Copy (SCP)-enabled server to temporarily store the content update.

STEP 1 | Retrieve the content update file from the update server.

1. Log in to the [Palo Alto Networks Support Portal](#) and click **Dynamic Updates**.
2. In the WildFire Appliance section, locate the latest WildFire appliance content update and download it.
3. Copy the content update file to an SCP-enabled server and note the file name and directory path.

STEP 2 | Install the content update on the WildFire appliance.

1. Log in to the WildFire appliance and download the content update file from the SCP server:

```
admin@WF-500> scp import wf-content from username@host:path
```

For example:

```
admin@WF-500> scp import wf-content from bart@10.10.10.5:c:/updates/panup-all-wfmeta-2-253.tgz
```



If your SCP server is running on a non-standard port or if you need to specify the source IP, you can also define those options in the `scp import` command.

2. Install the update:

```
admin@WF-500> request wf-content upgrade install file panup-all-wfmeta-2-253.tgz
```

3. View the status of the installation:

```
admin@WF-500> show jobs all
```

STEP 3 | Verify the content update.

Verify the content version:

```
admin@WF-500> show system info | match wf-content-version
```

The following output now shows version 2-253:

```
wf-content-version: 2-253
```

Enable Local Signature and URL Category Generation

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

The WildFire appliance can generate signatures locally based on the samples received from connected firewalls and the WildFire API, as an alternative to sending malware to the public cloud for signature generation. The appliance can generate the following types of signatures for the firewalls to use to block malware and any associated command and control traffic:

- **Antivirus signatures**—Detect and block malicious files. WildFire adds these signatures to WildFire and Antivirus content updates.
- **DNS signatures**—Detect and block callback domains for command and control traffic associated with malware. WildFire adds these signatures to WildFire and Antivirus content updates.
- **URL categories**—Categorizes callback domains as malware and updates the URL category in PAN-DB.

Configure the firewalls to retrieve the signatures generated by the WildFire appliance as frequently as every five minutes. You can also send the malware sample to the WildFire public cloud, in order to enable the signature to be distributed globally through Palo Alto Networks content releases.



Even if you're using the WildFire appliance for local file analysis, you can also [enable connected firewalls to receive the latest signatures distributed by the WildFire public cloud](#).

STEP 1 | [Set Up WildFire Appliance Content Updates.](#)

This allows the WildFire appliance to receive the latest threat intelligence from Palo Alto Networks.

STEP 2 | Enable signature and URL category generation.

1. Log in to the appliance and type **configure** to enter configuration mode.
2. Enable all threat prevention options:

```
admin@WF-500# set
```

```
deviceconfig setting wildfire signature-generation av yes dns
yes
url yes
```

3. Commit the configuration:


```
admin@WF-500# commit
```

 You can display the status of a signature for signatures generated in the WildFire 8.0.1 or later environment using the command:

```
admin@WF-500# show
wildfire global signature-status sha256 equal <sha-256
value>
```

WildFire appliances cannot display the status for signatures generated before the upgrade to WildFire 8.0.1.

STEP 3 | Set the schedule for connected firewalls to retrieve the signatures and URL categories the WildFire appliance generates.

 It is a best practice to configure your firewalls to retrieve content updates from both the WildFire public cloud and WildFire appliance. This ensures that your firewalls receive signatures based on threats detected worldwide, in addition to the signatures generated by the local appliance.

- For multiple firewalls managed by Panorama:

Launch Panorama and select **Panorama > Device Deployment > Dynamic Updates**, click **Schedules**, and **Add** scheduled content updates for managed devices.

For details on using Panorama to set up managed firewalls to receive signatures and URL categories from a WildFire appliance, see [Schedule Content Updates to Devices Using Panorama](#).

- For a single firewall:

1. Log in to the firewall web interface and select **Device > Dynamic Updates**.

For firewalls configured to forward files to a WildFire appliance (in either a WildFire private cloud or hybrid cloud deployment), the WF-Private section is displayed.

2. Set the **Schedule** for the firewall to [download and install content updates](#) from the WildFire appliance.

Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Enable the WildFire appliance to automatically submit malware samples to the WildFire public cloud. The WildFire public cloud further analyzes the malware and generates a signature to identify the sample. The signature is then added to WildFire signature updates, and distributed to global users to prevent future exposure to the threat. If you do not want to forward malware samples outside of your network, you can instead choose to submit only WildFire reports for the malware discovered on your network, in order to contribute to and refine WildFire statistics and threat intelligence.

- Submit Malware to the WildFire Public Cloud.

1. Execute the following CLI command from the WildFire appliance to enable the appliance to automatically submit malware samples to the WildFire public cloud:

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-sample yes
```



If the firewall that originally submitted the sample for WildFire private cloud analysis has packet captures (PCAPs) enabled, the PCAPs for the malware will also be forwarded to the WildFire public cloud.

2. Go to the [WildFire portal](#) to view analysis reports for malware automatically submitted to the WildFire public cloud. When malware is submitted to the WildFire public cloud, the public cloud generates a new analysis report for the sample.

- Submit Analysis Reports to the WildFire Public Cloud

To automatically submit malware reports to the WildFire public cloud (and not the malware sample), execute the following CLI command on the WildFire appliance:

```
admin@WF-500# set deviceconfig setting wildfire cloud-intelligence submit-report yes
```



If you have enabled the WildFire appliance to automatically submit malware to the WildFire public cloud, you do not need to enable this option—the WildFire public cloud will generate a new analysis report for the sample.

Reports submitted to the WildFire public cloud cannot be viewed on the [WildFire portal](#). The WildFire portal displays only WildFire public cloud reports.

- Verify Malware and Report Submission Settings

Check to confirm that cloud intelligence is enabled to either submit malware or submit reports to the WildFire public cloud by running the following command:

```
admin@WF-500> show wildfire status
```

Refer to the `Submit sample` and `Submitreport` fields.

Upgrade a WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Use the following workflow to upgrade the WildFire appliance operating system. If you want to upgrade an appliance that is part of a WildFire cluster, see [Upgrade WildFire Appliances in a Cluster](#). The appliance can only use one environment at a time to analyze samples, so after upgrading the appliance, review the list of available VM images and then choose the image that best fits your environment. In the case of Windows 7, if your environment has a mix of Windows 7 32-bit and Windows 7 64-bit systems, it is recommended that you choose the Windows 7 64-bit image, so WildFire will analyze both 32-bit and 64-bit PE files. Although you configure the appliance to use one virtual machine image configuration, the appliance uses multiple instances of the image to perform file analyses.

Depending on the number of samples the WildFire appliance has analyzed and stored, the time required to upgrade the appliance software varies; this is because upgrading requires the migration of all malware samples and 14 days of benign samples. Allow 30 to 60 minutes to upgrade a WildFire appliance that you have used in a production environment.

The following procedure uses an example filename from a PAN-OS 10.2.2 release. The exact filename for the release you install on your WildFire appliance may differ based on the specific release.

STEP 1 | If you're setting up a WildFire appliance for the first time, start by [configuring the WildFire appliance](#).

STEP 2 | Temporarily suspend sample analysis.

1. Stop firewalls from forwarding any new samples to the WildFire appliance.
 1. Log in to the firewall web interface.
 2. Select **Device > Setup > WildFire** and edit **General Settings**.
 3. Clear the **WildFire Private Cloud** field.
 4. Click **OK** and **Commit**.
2. Confirm that analysis for samples the firewalls already submitted to the appliance is complete:

```
admin@WF-500> show
wildfire latest samples
```



If you do not want to wait for the WildFire appliance to finish analyzing recently-submitted samples, you can continue to the next step. However, consider that the WildFire appliance then drops pending samples from the analysis queue.

STEP 3 | Install the latest WildFire appliance content update. This update equips the appliance with the latest threat information to accurately detect malware.



This process can take up to 6 hours or more on older appliances.

1. Verify that you are running the latest content update on your WildFire appliance.

```
admin@WF-500> request wf-content upgrade check
```

2. Download the latest WildFire content update package.

```
admin@WF-500> request  
wf-content upgrade download latest
```

If you do not have direct connectivity to the Palo Alto Networks Update Server, you can download and [Install WildFire Content Updates from an SCP-Enabled Server](#).

3. View the status of the download.

```
admin@WF-500> show jobs all
```

4. After the download is complete, install the update.

```
admin@WF-500> request  
wf-content upgrade install version latest
```

STEP 4 | (Required when upgrading to PAN-OS 10.2.2) Upgrade the VM images on the WildFire appliance.

1. Log in and access the [Palo Alto Networks Customer Support Portal Software Download Page](#). You can also manually navigate to the software download page from the Support homepage by going to **Updates > Software Updates**.
2. From the software updates page, select **WF-500 Guest VM Images** and download the following VM image files:



Palo Alto Networks periodically updates the VM image files; as a result, the specific filename changes based on the version that is available. Be sure to download the latest version, whereby the m-x.x.x in the filename indicates the release number; additionally, there is a release date that can be cross-referenced to help determine the latest version.

- WFWinXpAddon3_m-1.0.1.xpaddon3
 - WFWinXpGf_m-1.0.1.xpgf
 - WFWin7_64Addon1_m-1.0.1.7_64addon1
 - WFWin10Base_m-1.0.1.10base
3. Upload the VM images to the WildFire appliance.
 1. Import the VM image from the SCP server:

```
admin@WF-500>scp import wildfire-vm-image from  
<username@ip_address>/<folder_name>/<vm_image_filename>
```

For example:

```
admin@WF-500>scp import wildfire-vm-image from  
user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
```

2. To check the status of the download, use the following command:

```
admin@WF-500>show jobs all
```

3. Repeat for the remaining VM images.
4. Install the VM image.
 1.

```
admin@WF-500>request system wildfire-vm-image upgrade  
install file <vm_image_filename>
```
 2. Repeat for the remaining VM images.
5. Confirm that the VM images have been properly installed and enabled on the WildFire appliance.
 1. (Optional) View a list of available virtual machines images:

```
admin@WF-500> show wildfire vm-images
```

The output displays the available VM images.

2. Commit the configuration:

```
admin@WF-500# commit
```

3. View the active VM images by running the following command:

```
admin@WF-500> show wildfire status
```

STEP 5 | Download the PAN-OS 10.2.2 software version to the WildFire appliance.

You cannot skip any major release versions when upgrading the WildFire appliance. For example, if you want to upgrade from PAN-OS 6.1 to PAN-OS 7.1, you must first download and install PAN-OS 7.0.

The examples in this procedure demonstrate how to upgrade to PAN-OS 10.2.2. Replace 10.2.2 with the appropriate target release for your upgrade.

Download the 10.2.2 software version:

- Direct Internet Connectivity:

1.

```
admin@WF-500> request system software download version 10.2.2
```

2. To check the status of the download, use the following command:

```
admin@WF-500> show jobs all
```

- Without Internet Connectivity:

1. Navigate to the [Palo Alto Networks Support](#) site and in the Tools section, click on **Software Updates**.
2. Download the WildFire appliance software image file to be installed to a computer running SCP server software.
3. Import the software image from the SCP server:

```
admin@WF-500> scp import software from <username@ip_address>/<folder_name>/<imagefile_name>
```

For example:

```
admin@WF-500> scp import software
```

```
from user1@10.0.3.4:/tmp/WildFire_m-10.2.2
```

4. To check the status of the download, use the following command:

```
admin@WF-500> show jobs all
```

- STEP 6 |** Confirm that all services are running.

```
admin@WF-500> show system software status
```

- STEP 7 |** Install the 10.2.2 software version.

```
admin@WF-500> request system software install version 10.2.2
```

- STEP 8 |** Complete the software upgrade.

1. Confirm that the upgrade is complete. Run the following command and look for the job type `Install` and status `FIN`:

```
admin@WF-500> show jobs all
Enqueued   Dequeued ID Type   Status Result Completed
-----
02:42:36   02:42:36 5 Install FIN    OK      02:43:02
```

2. Restart the appliance:

```
admin@WF-500> request restart system
```



The upgrade process could take 10 minutes or over an hour, depending on the number of samples stored on the WildFire appliance.

- STEP 9 |** Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the `sw-version` field shows 10.2.2:

```
admin@WF-500> show system info | match sw-version
```

2. Confirm that all processes are running:

```
admin@WF-500> show
```

system software status

3. Confirm that the auto-commit (AutoCom) job is complete:

```
admin@WF-500> show
jobs all
```

STEP 10 | (Optional) Enable the VM image the WildFire appliance uses to perform analysis. Each available VM image represents a single operating system, and supports several different analysis environments based on that operating system.



- *If your network environment has a mix of Windows 7 32-bit and Windows 7 64-bit systems, it is recommended that you choose the Windows 7 64-bit image, so WildFire will analyze both 32-bit and 64-bit PE files.*
- *vm-3 (Windows XP), vm-5 (Windows 7 64-bit), and vm-7 (Windows 10 64-bit) are the currently available analysis environments.*
- View the active virtual machine image by running the following command and refer to the Selected VM field:

```
admin@WF-500> show
wildfire status
```

- View a list of available virtual machines images:

```
admin@WF-500> show
wildfire vm-images
```

The following output shows that vm-5 is the Windows 7 64-bit image:

```
vm-5 Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010.
Support PE, PDF, Office 2010 and earlier
```

- Set the image to be used for analysis:

```
admin@WF-500# set
deviceconfig setting wildfire active-vm <vm-image-number>
```

For example, to use vm-5, run the following command:

```
admin@WF-500# set
deviceconfig setting wildfire active-vm vm-5
```

And commit the configuration:

```
admin@WF-500# commit
```


STEP 11 | Next steps:

- (Optional) Upgrade firewalls to PAN-OS 10.2.2. See the [firewall upgrade instructions](#) included in the PAN-OS 10.2 New Features Guide. Firewalls running release versions earlier than PAN-OS 10.2.2 can still continue to forward samples to a WildFire appliance running 10.2.2.
- (Troubleshooting) If you notice data migration issues or an error following the upgrade, restart the WildFire appliance to restart the upgrade process—restarting the WildFire appliance will not cause data to be lost.


Install WildFire Appliance Device Certificate With an Internet Connection

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License Customer Support Portal (CSP) account with one of the following user roles: Super User, Standard User, Limited User, Threat Researcher, AutoFocus Trial Role, Group Super User, Group Standard User, Group Limited User, Group Threat Researcher, Authorized Support Center (ASC) User, and ASC Full Service User. Superuser access to the WildFire appliance

To fetch the device certificate on the WF-500 appliance when an Internet connection is available, you must log in to the [Palo Alto Networks Support Portal](#) to generate a one time password used to access the certificate. This OTP is then used to retrieve the device certificate on the specific appliance.

 *WF-500B appliances are equipped with a Trusted Platform Module (TPM) that is used to securely identify itself and automatically fetch the device certificate—no user intervention is necessary to manage WF-500B device certificates.*

If you are operating a [WildFire Private Cloud](#) and do not connect to any of the WildFire services, you do not need to update the WildFire appliance device certificates. Instead, the WildFire appliance uses predefined certificates for mutual authentication to establish the SSL connections used for management access and inter-device communication; however, you can [Set Up Authentication Using a Custom Certificate on a Standalone WildFire Appliance](#) instead.

 *If your WF-500B appliance is not connected to the Internet, you might observe failed jobs due to repeated attempts by the appliance to retrieve device certificates.*

To successfully install the device certificate on your firewall, the following FQDNs and ports must be allowed on your network.

FQDN	Ports
<ul style="list-style-type: none"> http://ocsp.paloaltonetworks.com http://crl.paloaltonetworks.com 	TCP 80

FQDN	Ports
<ul style="list-style-type: none"> • http://ocsp.godaddy.com 	
<ul style="list-style-type: none"> • https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • certificatetrusted.paloaltonetworks.com • certificate.paloaltonetworks.com 	TCP 443
<ul style="list-style-type: none"> • *.gpcloudservice.com 	TCP 444 and TCP 443

STEP 1 | Verify that you are running one of the following PAN-OS releases on the WildFire appliance:

- PAN-OS 11.0.1 and later
- PAN-OS 10.2.4 and later
- PAN-OS 10.1.10 and later (not supported on the WF-500B appliance)
- PAN-OS 10.0.12 and later (not supported on the WF-500B appliance)
- PAN-OS 9.1.17 and later (not supported on the WF-500B appliance)

STEP 2 | Generate the One Time Password (OTP).

1. Log in to the [Customer Support Portal](#) with a user role that has permission to generate an OTP.
2. Select **Products > Device Certificates and Generate OTP**.
3. For the **Device Type**, select **Generate OTP for WF-500**.
4. Select your **WF-500 Device** serial number.
5. **Generate OTP** and copy the OTP.

STEP 3 | Access the WF-500 appliance CLI with superuser [administrative privileges](#).

STEP 4 | Configure the WildFire appliance to synchronize with an NTP server:

```
admin@WF-500> configure
admin@WF-500# set deviceconfig system ntp-servers primary-ntp-
server ntp-server-address <NTP primary server IP address>
admin@WF-500# set deviceconfig system ntp-servers secondary-ntp-
server ntp-server-address <NTP secondary server IP address>
```

STEP 5 | Download and install the WF-500 appliance device certificate using the following CLI command (remember to use the correct **One-time Password** you generated in the Customer Support Portal):

```
admin@WF-500> request certificate fetch otp <otp_value>
```

STEP 6 | Your WF-500 appliance successfully retrieves and installs the device certificate.

STEP 7 | (Optional) Verify the successful download and installation of a device certificate using the following CLI command:

```
admin@WF-500> show device-certificate status
```


A successful installation of the device certificate displays the following response:

```
Device Certificate information:
Current device certificate status: Valid
Not valid before: 2022/11/30 15:17:47 PST
Not valid after: 2023/02/28 15:17:47 PST
Last fetched timestamp: 2022/11/30 15:29:42 PST
Last fetched status: success
Last fetched info: Successfully fetched Device Certificate
```

STEP 8 | Refresh the WildFire appliance settings to establish a connection to the Advanced WildFire cloud with the updated device certificate using the following CLI command:

Table 1:

PAN-OS Version Running on WildFire Appliance	CLI Command
<ul style="list-style-type: none"> • PAN-OS 11.0.1 and later • PAN-OS 10.2.5 and later • PAN-OS 10.1.10 and later 	<pre>admin@WF-500> test wildfire registration</pre>
<ul style="list-style-type: none"> • PAN-OS 10.2.4 • PAN-OS 10.0.12 and later • PAN-OS 9.1.17 and later 	<pre>admin@WF-500> request restart system</pre> <p> <i>This process can take up to 20 minutes to complete.</i></p>
Any version configured as a WildFire cluster node	<pre>admin@WF-500(active-controller)> request cluster reboot-local-node</pre>

PAN-OS Version Running on WildFire Appliance	CLI Command
	<p data-bbox="591 243 1341 338"> You can view the status of the status of the reboot task on the WildFire controller node using the following CLI command:</p> <pre data-bbox="667 380 1357 474">admin@WF-500(active-controller)> show cluster task pending</pre> <p data-bbox="667 495 1308 558">When there are no pending tasks remaining, use the following CLI command to verify a successful reboot:</p> <pre data-bbox="667 600 1357 695">admin@WF-500(active-controller)> show cluster task history</pre> <p data-bbox="667 716 1317 852">Upon completion, you should see the status <i>Finished: success at YYYY-MM-DD HH:MM:SS UTC</i>, indicating when the reboot process has completed.</p>

Monitor WildFire Appliance Activity

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

You can view the analysis results for samples submitted to the WildFire appliance by accessing the firewall that submitted the sample (or Panorama, if you are centrally managing multiple firewalls), or by [using the WildFire API](#).

After WildFire has analyzed a sample and delivered a verdict of malicious, phishing, grayware, or benign, a detailed analysis report is generated for the sample. WildFire analysis reports viewed on the firewall that submitted the sample also include details for the session during which the sample was detected. For samples identified as malware, the WildFire analysis report includes details on existing WildFire signatures that might be related to the newly-identified malware and information on file attributes, behavior, and activity that indicated the sample was malicious.

See the following topics for details on how to monitor WildFire submissions, to WildFire analysis reports for samples, and to set up alerts and notifications based on submissions and analysis results:


- [About WildFire Logs and Reporting](#)
- [Use the WildFire CLI to Monitor the WildFire Appliance](#)
- [Use the Firewall to Monitor WildFire Appliance Submissions](#)

About WildFire Logs and Reporting

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

You can monitor WildFire appliance logs on the firewall, with the WildFire portal, or with the WildFire API.

For each sample WildFire analyzes, WildFire categorizes the sample as malware, phishing, grayware, or benign and details sample information and behavior in the WildFire analysis report. [WildFire analysis reports](#) can be found on the firewall that submitted the sample and the WildFire cloud (public or private) that analyzed the sample, or can be retrieved using the WildFire API:

- On the firewall**—All samples submitted by a firewall for WildFire analysis are logged as WildFire Submissions entries (**Monitor > WildFire Submissions**). The Action column in the WildFire Submissions log indicates whether a file was allowed or blocked by the firewall. For each WildFire submission entry you can open a detailed log view to view the WildFire analysis report for the sample or to download the report as a PDF.
- On the WildFire portal**—Monitor WildFire activity, including the WildFire analysis report for each sample, which can also be downloaded as a PDF. In a WildFire private cloud deployment, the WildFire portal provides details for samples that are manually uploaded to the portal and samples submitted by a WildFire appliance with cloud intelligence enabled.
 -  *The option to view WildFire analysis reports on the portal is only supported for WildFire appliances with the [cloud intelligence](#) feature is enabled.*
- With the WildFire API**—Retrieve WildFire analysis reports from a WildFire appliance or from the WildFire public cloud.

Use the WildFire Appliance to Monitor Sample Analysis Status

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Use the WildFire CLI (command line interface) to monitor analysis-related details on your WildFire appliance. You can view analysis platform utilization information, the current sample queue, as well as sample process details.

See the following sections for details on using the WildFire appliance to monitor WildFire activity:

- [View WildFire Analysis Environment Utilization](#)
- [View WildFire Sample Analysis Processing Details](#)

View WildFire Analysis Environment Utilization

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The WildFire appliance uses various analysis environments to detect malicious behavior within samples. You can view which analysis environments are being utilized, how many are available, as well as how many files are queued for analysis. If the utilization for a particular analysis environment is always at (or near) maximum workload capacity, consider offloading analysis of less sensitive files to a Palo Alto Networks hosted WildFire public cloud, updating file forwarding policy, or redefining file forwarding limits (Palo Alto Networks recommends using the default file forwarding values for all file types).

STEP 1 | Access the CLI and one of the following commands based on the analysis environment for which you want to see utilization statistics for.

- Portable Executable Analysis Environment Utilization—**show wildfire wf-vm-pe-utilization**
- Document Analysis Environment Utilization—**show wildfire wf-vm-doc-utilization**
- Email Link Analysis Environment Utilization—**show wildfire wf-vm-elinkd-utilization**
- Archive Analysis Environment Utilization—**show wildfire wf-vm-archive-utilization**

For a given analysis environment, the appliance indicates how many are in use and how many are available:

```
{
  available: 2,
  in_use: 1,
}
```

STEP 2 | View the number and breakdown of WildFire appliance samples that are waiting to be analyzed. Samples are processed as analysis environments become available.

show wildfire wf-sample-queue-status

```
{
  DW-ARCHIVE: 4,
  DW-DOC: 2,
  DW-ELINK: 0,
  DW-PE: 21,
  DW-URL_UPLOAD_FILE: 2,
}
```

View WildFire Sample Analysis Processing Details

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

The WildFire appliance retains records of analysis activity within an event log. You can view details about which connected services or appliances in your network analyzed a particular sample, as well as how many samples were analyzed in a given time-frame. You can use this information to monitor activity and develop policies and countermeasures against malicious activity. Unusually heavy activity can indicate suspicious activity. Also consider using a threat intelligence tool such as AutoFocus to investigate and determine the nature of a threat.

STEP 1 | View the number of samples processed locally within a specified timespan or based on a maximum number of samples.

show wildfire local sample-processed {time [last-12-hrs| last-15-minutes | last-1-hr | last-24-hrs | last-30-days | last-7-days| last-calender-day | last-calender-month] \ count <number_of_samples>}.

```
Latest samples information:
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          Create Time          |          SHA256          | File Type | File Size |
| Malicious | Status |          |          |          |          |
+-----+-----+-----+-----+
| ce752b7b76ac2012bdff2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
| 2018-12-09 16:55:53 |          | Email Link | 31,522 |
|          | download complete |          |          |
| 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
| 2018-12-09 16:53:40 |          | Email Link | 39,679 |
|          | download complete |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

STEP 2 | Identify the device(s) that submitted a specified sample for WildFire analysis.

show wildfire global sample-device-lookup sha256equal <SHA_256>.

```
Sample
1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
last seen on following devices:
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|          SHA256          |
| Device ID | Device IP | Submitted Time |
+-----+-----+-----+-----+
| 1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e |
| Manual | Manual | 2019-08-05 19:24:39 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

Use the WildFire CLI to Monitor the WildFire Appliance

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

Use the WildFire™ CLI (command line interface) to view the internal system logs. You can review the logging events to monitor the health and status of WildFire components, such as cluster nodes, core and analyzer services, as well as to troubleshoot, and verify system configuration. For information on the other PAN-OS commands, refer to the [PAN-OS CLI Quick Start](#).

- [View the WildFire Appliance System Logs](#)

View the WildFire Appliance System Logs

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

Use a terminal emulator, such as PuTTY, connect to the WildFire appliance using either a secure shell connection (SSH) or a physical direct serial connection from a serial interface on your management computer to the Console port on the device.

STEP 1 | Launch the terminal emulation software and select the type of connection (Serial or SSH).

- To establish an SSH connection, enter the WildFire hostname or IP address of the device you want to connect to and set the port to **22**.
- To establish a Serial connection, connect a serial interface on management computer to the Console port on the device. Configure the Serial connection settings in the terminal emulation software as follows:
 - Data rate: **9600**
 - Data bits: **8**
 - Parity: **none**
 - Stop bits: **1**
 - Flow control: **none**

STEP 2 | When prompted to log in, enter your administrative credentials.

STEP 3 | On a WildFire appliance, enter the following command:

```
admin@WF-500>show log system subtype direction equal backward
```

This command displays all WildFire logged events categorized as a wildfire-appliance subtype from oldest to newest.

- You can reverse the display of the logs to newest to oldest by adding the command argument `direction equal backward`.
- The log messages returned by the WildFire appliance CLI can include numerous subtypes. You can filter the logs based on a common keyword. Use the following command argument to filter based on a specific string: `match queue < keyword>`

The following WildFire appliance log shows the system initialization processes during startup.

Time	Severity	Subtype	Object	EventID	ID	Description
2017/03/29 12:04:33	medium	general	general	0		Hostname changed to WF-500
2017/03/29 12:04:40	info	general	general	0		VPN Disable mode = off
2017/03/29 12:04:41	info	hw	ps-inse	0		Power Supply #1 (top) inserted
2017/03/29 12:04:41	high	general	system-	1		The system is starting up.
2017/03/29 12:04:41	info	raid	pair-de	0		New Disk Pair A detected.
2017/03/29 12:04:41	info	raid	pair-de	0		New Disk Pair A detected.
2017/03/29 12:04:41	info	raid	pair-de	0		New Disk Pair B detected.
2017/03/29 12:04:41	info	raid	pair-de	0		New Disk Pair B detected.
2017/03/29 12:04:41	info	cluster	cluster	0		Cluster daemon is initializing.
2017/03/29 12:04:41	info	port	eth1	link-ch	0	Port eth1: Up 1Gb/s Full duplex
2017/03/29 12:04:41	info	port	MGT	link-ch	0	Port MGT: Up 1Gb/s Full duplex
2017/03/29 12:04:41	info	port	eth3	link-ch	0	Port eth3: Up 1Gb/s Full duplex
2017/03/29 12:04:41	info	port	eth2	link-ch	0	Port eth2: Up 1Gb/s Full duplex
2017/03/29 12:04:41	info	general	general	0		Power Supply #1 (top) is not present on startup
2017/03/29 12:04:41	info	general	general	0		Power Supply #2 (bottom) is not present on startup

Use the Firewall to Monitor WildFire Appliance Submissions

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

Samples forwarded by the firewall (to the WildFire private and/or public clouds) are added as entries to the **WildFire Submissions** logs. A detailed WildFire analysis report is displayed in the expanded view for each WildFire Submissions entry. For more information about using the firewall to monitor malware, refer to [Monitor WildFire Activity](#).

View WildFire Appliance Logs and Analysis Reports

WildFire Appliance Clusters

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

A *WildFire appliance cluster* is an interconnected group of WildFire appliances that pool resources to increase sample analysis and storage capacity, support larger groups of firewalls, and simplify configuration and management of multiple WildFire appliances. This is especially useful in environments where access to the WildFire public cloud is not permitted. You can configure and manage up to twenty WildFire appliances as a WildFire appliance cluster on a single network. Clusters also provide a single signature package that the cluster distributes to all connected firewalls, high-availability (HA) architecture for fault tolerance, and the ability to manage clusters centrally using Panorama. You can also manage [standalone WildFire appliances](#) using Panorama.

To create WildFire appliance clusters, all of the WildFire appliances that you want to place in a cluster must run PAN-OS 8.0.1 or later. When you use Panorama to manage WildFire appliance clusters, Panorama also must run PAN-OS 8.0.1 or later. You do not need a separate license to create and manage WildFire appliance clusters.

- [WildFire Appliance Cluster Resiliency and Scale](#)
- [WildFire Appliance Cluster Management](#)
- [Configure a Cluster Locally on WildFire Appliances](#)
- [Configure WildFire Appliance-to-Appliance Encryption](#)
- [Monitor a WildFire Cluster](#)
- [Upgrade WildFire Appliances in a Cluster](#)
- [Troubleshoot a WildFire Cluster](#)

WildFire Appliance Cluster Resiliency and Scale

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

WildFire appliance clusters aggregate the sample analysis and storage capacity of up to twenty WildFire appliances so that you can support large firewall deployments on a single network. You have the flexibility to manage and [Configure a Cluster Locally on WildFire Appliances](#) using the CLI, or manage and [Configure a Cluster Centrally on Panorama M-Series](#) or virtual appliance servers. A WildFire appliance cluster environment includes:

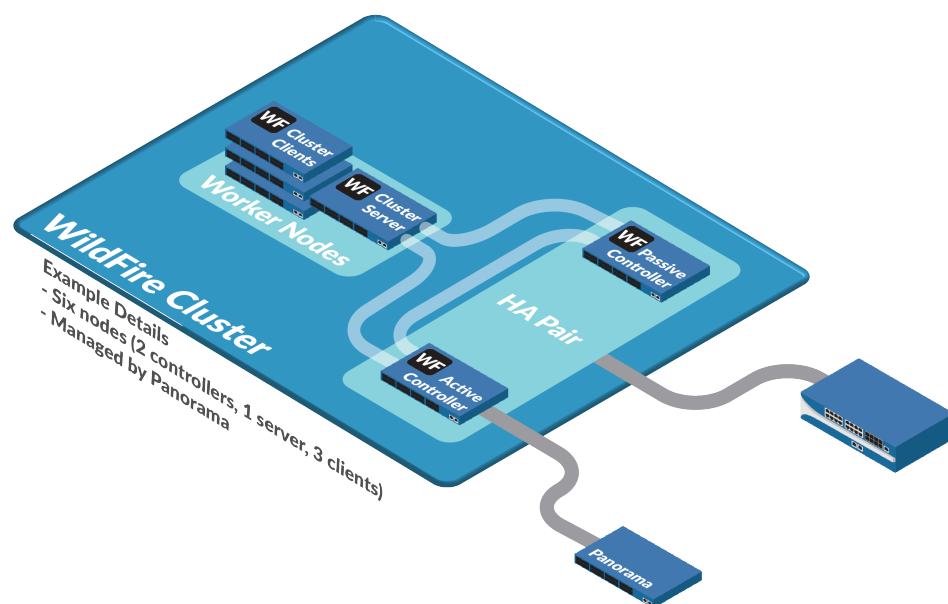
- From 2 to 20 WildFire appliances that you want to group and manage as a cluster. At a minimum, a cluster must have two WildFire appliances configured in a high-availability (HA) pair.
- Firewalls that forward samples to the cluster for traffic analysis and signature generation.
- **(Optional)** One or two Panorama appliances for centralized cluster management if you choose not to manage the cluster locally. To provide HA, use two Panorama appliances configured as an HA pair.

Each WildFire appliance you add to a WildFire appliance cluster becomes a node in that cluster (as opposed to a standalone WildFire appliance). Panorama can manage up to 10 WildFire appliance clusters with a total of 200 WildFire *cluster nodes* (10 clusters, each with the maximum of 20 nodes).



Panorama can manage [standalone WildFire appliances](#) as well as WildFire appliance clusters. The combined total of standalone WildFire appliances and WildFire appliance cluster nodes that Panorama can manage is 200. For example, if Panorama manages three clusters with a total of 15 WildFire cluster nodes and eight standalone WildFire appliances, then Panorama manages a total of 23 WildFire appliances and can manage up to 177 more WildFire appliances.

WildFire appliances connected to a Panorama do not have registration limit—you can connect as many devices without impacting your [Capacity License](#). For more information on Panorama licensing, refer to [Register Panorama and Install Licenses](#).



Cluster nodes play one of three roles:

- **Controller Node**—Two controller nodes manage the queuing service and database, generate signatures, and manage the cluster locally if you don't manage the cluster with a Panorama M-Series or virtual appliance. Each cluster can have a maximum of two controller nodes. For fault tolerance, each WildFire appliance cluster should have a minimum of two nodes configured as a primary controller node and a controller backup node HA pair. Except during normal maintenance or failure conditions, each cluster should have two controller nodes.
- **Worker Node (cluster client)**—Cluster nodes that are not controller nodes are worker nodes. Worker nodes increase the analysis capacity, storage capacity, and data resiliency of the cluster.
- **Server Node (cluster server)**—The third node in a WildFire cluster is automatically configured as a server node, a special type of worker node that provides database and infrastructure redundancy features in addition to standard worker node capabilities.

When a firewall registers with a cluster node, or when you add a WildFire appliance that already has registered firewalls to a cluster, the cluster pushes a registration list to the connected firewalls. The registration list contains every node in the cluster. If a cluster node fails, the firewalls connected to that node reregister with another cluster node. This type of resiliency is one of the benefits of creating WildFire appliance clusters.

Benefit	Description
Scale	A WildFire appliance cluster increases the analysis throughput and storage capacity available on a single network so that you can serve a larger network of firewalls without segmenting your network.
High availability	If a cluster node goes down, HA configuration provides fault tolerance to prevent the loss of critical data and services. If you manage clusters centrally using Panorama, Panorama HA configuration provides central management fault tolerance.

Benefit	Description
Single signature package distribution	All firewalls connected to a cluster receive the same signature package, regardless of the cluster node that received or analyzed the data. The signature package is based on the activity and results of all cluster members, which means that each connected firewall benefits from the combined cluster knowledge.
Centralized management (Panorama)	You save time and simplify the management process when you use Panorama to manage WildFire appliance clusters. Instead of using the CLI and scripting to manage a WildFire appliance or cluster, Panorama provides a single-pane-of-glass view of your network devices. You can also push common configurations, configuration updates, and software upgrades to multiple WildFire appliance clusters, and you can do all of this using the Panorama web interface instead of the WildFire appliance CLI.
Load balancing	When a cluster has two or more active nodes, the cluster automatically distributes and load balances analysis, report generation, signature creation, storage, and WildFire content distribution among the nodes.

WildFire Cluster High Availability

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

High availability is a crucial advantage of WildFire appliance clusters because HA prevents the loss of critical data and services. An HA cluster copies and distributes critical data, such as analysis results, reports, and signatures, across nodes so that a node failure does not result in data loss. An HA cluster also provides redundant critical services, such as analysis functionality, WildFire API, and signature generation, so that a node failure doesn't interrupt service. A cluster must have at least two nodes to provide high availability benefits. Cluster node failure doesn't affect firewalls, because firewalls registered to a failed node use the cluster registration list to register with another cluster node.

Each of the two devices in the HA pair is configured by the user as a primary and secondary appliance. Based on this initial priority value configuration, WildFire also assigns an operational status of active to the primary appliance and passive to the secondary device. This status determines which WildFire appliance is used as the point of contact for management and infrastructure controls. The passive device is always synchronized with the active appliance and is ready to assume that role should a system or network failure occur. For example, when the primary appliance in an active state (active-primary) suffers a failure, a failover event occurs and transitions to a passive-primary state, while the secondary appliance transitions to active-secondary. The originally assigned priority value remains the same regardless of the status of the appliance.

Failover occurs when the HA pair is no longer able to communicate with each other, becomes unresponsive, or suffers a fatal error. While the WildFire HA pair will attempt to auto-resolve minor disruptions, major events require user-intervention. Failover can also be triggered when a controller is suspended or decommissioned by the user.



Do not configure a cluster with only one controller node. Each cluster should have an HA controller pair. A cluster should have a single controller node only in temporary situations, for example, when you swap controller nodes or if a controller node fails.

In a two-node cluster HA pair, if one controller node fails, the other controller node cannot process samples. For the remaining cluster node to process samples, you must configure it to function as a standalone WildFire appliance: delete the HA and cluster configurations on the remaining cluster node and reboot the node. The node comes back up as a standalone WildFire appliance.

Three-node clusters operate a HA pair with the addition of server node to provide additional redundancy. The server operates the same database and server infrastructure services as a controller, but does not generate signatures. This deployment enables the cluster to function if a controller node fails.

Additional nodes that are added to a WildFire cluster function as a worker or server node. The third node is automatically configured as a server, while each subsequent addition is added as a worker.

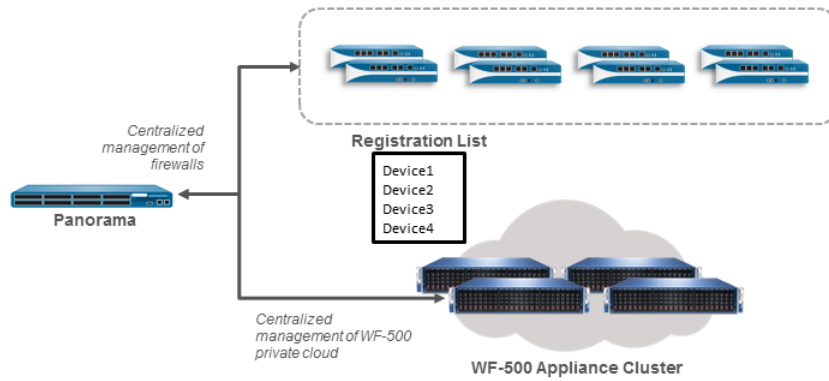
Benefits of Managing WildFire Clusters Using Panorama

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

If you manage WildFire appliance clusters with Panorama, you can [configure two Panorama M-Series or virtual appliances as an HA pair](#) to provide management redundancy. If you don't configure redundant Panorama appliances and the Panorama fails, then you can still manage clusters locally from a controller node.

If you are using a Panorama HA pair to manage the cluster and one Panorama fails, the other Panorama appliance takes over management of the cluster. If a Panorama HA peer fails, restore service from the failed Panorama peer as soon as possible to restore management HA.

Providing analysis, storage, and centralized management HA requires at least two WildFire appliances configured as cluster controller and controller backup nodes, and two Panorama M-Series or virtual appliances.



Firewalls receive a registration list that contains all of the WildFire appliances that are members of the cluster. Firewalls can register with any node in the cluster and the cluster automatically balances the load among its nodes.


WildFire Appliance Cluster Management

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

To manage a WildFire appliance cluster, you need to know the capabilities of clusters and management recommendations.

Category	Description
Cluster operation and configuration	<p>Configure all cluster nodes identically to ensure consistency in analysis and appliance-to-appliance communication:</p> <ul style="list-style-type: none"> • All cluster nodes must run the same version of PAN-OS (PAN-OS 8.0.1 or later). Panorama must run the same software version as the cluster nodes or a newer version. Firewalls can run the same software versions that enable them to submit samples to a WildFire appliance. Firewalls do not require a particular software version to submit samples to a WildFire appliance cluster. • Cluster nodes inherit their configuration from the controller node, with the exception of interface configuration. Cluster members monitor the controller node configuration and update their own configurations when the controller node commits an updated configuration. Worker nodes inherit settings such as content update server settings, WildFire cloud server settings, the sample analysis image, sample data retention time frames, analysis environment settings, signature generation settings, log settings, authentication settings, and Panorama server, DNS server, and NTP server settings, • When you manage a cluster with Panorama, the Panorama appliance pushes a consistent configuration to all cluster nodes. Although you can change the configuration locally on a WildFire appliance node, Palo Alto Networks does not recommend that you do this, because the next time the Panorama appliance pushes a configuration, it replaces the running configuration on the node. Local changes to cluster nodes that Panorama manages often cause Out of Sync errors. • If the cluster node membership list differs on the two controller nodes, the cluster generates an Out of Sync warning. To avoid a condition where both controller nodes continually update the out-of-sync membership list for the other node, cluster membership enforcement stops. When this happens, you can synchronize the cluster membership lists from the local CLI on the controller and controller backup nodes by running the operational command request high-availability sync-to-remote running-

Category	Description
	<p>configuration. If there is a mismatch between the primary controller node's configuration and the configuration on the controller backup node, the configuration on the primary controller node overrides the configuration on the controller backup node. On each controller node, run show cluster all-peers and compare and correct the membership lists.</p> <ul style="list-style-type: none"> • A cluster can have only two controller nodes (primary and backup); attempts to locally add a third controller node to a cluster fail. (The Panorama web interface automatically prevents you from adding a third controller node.) The third and all subsequent nodes added to a cluster must be worker nodes. • A characteristic of HA configurations is that the cluster distributes and retains multiple copies of the database, queuing services, and sample submissions to provide redundancy in case of a cluster node failure. Running the additional services required to provide redundancy for HA has a minimal impact on throughput. • The cluster automatically checks for duplicate IP addresses used for the analysis environment network. • If a node belongs to a cluster and you want to move it to a different cluster, you must first remove the node from its current cluster. • Do not change the IP address of WildFire appliances that are currently operating in a cluster. Doing so causes the associated firewall to deregister from the node.
Cluster data retention policies	<p>Data retention policies determine how long the WildFire appliance cluster stores different types of samples.</p> <ul style="list-style-type: none"> • Benign and grayware samples—The cluster retains benign and grayware samples for 1 to 90 days (default is 14). • Malicious samples—The cluster retains malicious samples for a minimum of 1 day (default is indefinite—never deleted). Malicious samples may include phishing verdict samples. <p>Configure the same data retention policy throughout a cluster (4 in Configure General Cluster Settings Locally or 4 in Configure General Cluster Settings on Panorama).</p>
Networking	<p>No communication between WildFire appliance clusters is allowed. Nodes communicate with each other within a given cluster, but do not communicate with nodes in other clusters.</p> <p>All cluster members must:</p> <ul style="list-style-type: none"> • Use a dedicated cluster management interface for cluster management and communication (enforced in Panorama). • Have a static IP address in the same subnet.

Category	Description
Dedicated cluster management interface	<ul style="list-style-type: none"> • Use low-latency connections between cluster nodes. The maximum latency for a connection should be no greater than 500 ms. <p>The dedicated cluster management interface enables the controller nodes to manage the cluster and is a different interface than the standard management interface (Ethernet0). Panorama enforces configuring a dedicated cluster management interface.</p> <p> <i>If the cluster management link goes down between two controller nodes in a two-node configuration, the controller backup node services and sample analysis continue to run even though there is no management communication with the primary controller node. This is because when the cluster management link goes down, the controller backup node does not know if the primary controller node is still functional, resulting in a split-brain condition. The controller backup node must continue to provide cluster services in case the primary controller node is not functional. When the cluster management link is restored, the data from each controller node is merged.</i></p>
DNS	<p>You can use the controller node in a WildFire appliance cluster as the authoritative DNS server for the cluster. (An authoritative DNS server serves the actual IP addresses of the cluster members, as opposed to a recursive DNS server, which queries the authoritative DNS server and passes the requested information to the host that made the initial request.)</p> <p>Firewalls that submit samples to the WildFire appliance cluster should send DNS queries to their regular DNS server, for example, an internal corporate DNS server. The internal DNS server forwards the DNS query to the WildFire appliance cluster controller (based on the query's domain). Using the cluster controller as the DNS server provides many advantages:</p> <ul style="list-style-type: none"> • Automatic load balancing—When the cluster controller resolves the service advertisement hostname, the host cluster nodes are in a random order, which has the effect of organically balancing the load on the nodes. • Fault tolerance—If one cluster node fails, the cluster controller automatically removes it from the DNS response, so firewalls send new requests to nodes that are up and running. • Flexibility and ease of management—When you add nodes to the cluster, because the controller updates the DNS response automatically, you don't need to make any changes on the firewall and requests automatically go to the new nodes as well as the previously existing nodes.

Category	Description
	Although the DNS record should not be cached, for troubleshooting, if the DNS lookup succeeds, the TTL is 0. However, when the DNS lookup returns NXDOMAIN, the TTL and “minimum TTL” are both 0.
Administration	<p>You can administer WildFire clusters using the local WildFire CLI or through Panorama. There are two administrative roles available locally on WildFire cluster nodes:</p> <ul style="list-style-type: none">• Superreader—Read-only access.• Superuser—Read and write access.
Firewall registration	<p>WildFire appliance clusters push a registration list that contains all of the nodes in a cluster to every firewall connected to a cluster node. When you register a firewall with an appliance in a cluster, the firewall receives the registration list. When you add a standalone WildFire appliance that already has connected firewalls to a cluster so that it becomes a cluster node, those firewalls receive the registration list.</p> <p>If a node fails, the connected firewalls use the registration list to register with the next node on the list.</p>
Data Migration	<p>To provide data redundancy, WildFire appliance nodes in a cluster share database, queuing service, and sample submission content, however the precise location of this data depends on the cluster topology. As a result, WildFire appliances in a cluster undergo data migration or data rearrangement whenever topology changes are made. Topology changes include adding and removing nodes, as well as changing the role of a pre-existing node. Data migration can also occur when databases are converted to a newer version, as with the upgrade from WildFire 7.1 to 8.0.</p> <p>Data migration status can be viewed by issuing status commands from the WildFire CLI. This process can take several hours depending on the quantity of data on the WildFire appliances.</p>

Deploy a WildFire Cluster

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

To deploy a WildFire appliance cluster you must upgrade all of the appliances that will be enrolled into the cluster, create the WildFire cluster, and then finally configure the settings to best suit your needs. You can perform these tasks locally from the WildFire appliance CLI or through Panorama, which enables you to quickly apply configuration changes and upgrades to connected WildFire appliances.

The following procedure shows how to create and configure a WildFire HA (high availability) pair and to add additional appliance nodes to a cluster.

- STEP 1 |** [Upgrade your WildFire appliances locally](#) to PAN-OS 8.0.1 or later, the minimum supported release to operate clusters.
- STEP 2 |** Create, configure, and add nodes to a WildFire appliance cluster.
- [Configure a Cluster and Add Nodes Locally](#)
 - [Configure a Cluster and Add Nodes on Panorama](#)
- STEP 3 |** Configure general WildFire appliance cluster settings.
- [Configure General Cluster Settings Locally](#)
 - [Configure General Cluster Settings on Panorama](#)
- STEP 4 |** (Optional) Encrypt WildFire cluster appliance-to-appliance communications.
- [Configure Appliance-to-Appliance Encryption Using Predefined Certificates Through the CLI](#)
 - [Configure Appliance-to-Appliance Encryption Using Custom Certificates Through the CLI](#)
 - [Configure Appliance-to-Appliance Encryption Using Predefined Certificates Centrally on Panorama](#)
 - [Configure Appliance-to-Appliance Encryption Using Custom Certificates Centrally on Panorama](#)
- STEP 5 |** Verify that your WildFire appliance cluster is operating normally.
- [View WildFire Cluster Status Using the CLI](#)
 - [View WildFire Cluster Status Using Panorama](#)

STEP 6 | (Optional) Upgrade the WildFire appliances that are already enrolled in a cluster.

- [Upgrade a Cluster Locally with an Internet Connection](#)
- [Upgrade a Cluster Locally without an Internet Connection](#)
- [Upgrade a Cluster Centrally on Panorama with an Internet Connection](#)
- [Upgrade a Cluster Centrally on Panorama without an Internet Connection](#)

Configure a Cluster Locally on WildFire Appliances

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Before you configure a WildFire appliance cluster locally, have two WildFire appliances available to configure as a high availability controller node pair and any additional WildFire appliances needed to serve as worker nodes to increase the analysis, storage capacity, and resiliency of the cluster.

If the WildFire appliances are new, check [Get Started with WildFire](#) to ensure that you complete basic steps such as confirming your WildFire license is active, enabling logging, connecting firewalls to WildFire appliances, and configuring basic WildFire features.

If you are managing your WildFire appliance cluster using Panorama, you can also [configure your WildFire cluster centrally on Panorama](#).



To create WildFire appliance clusters, you must [upgrade all of the WildFire appliances that you want to place in a cluster to PAN-OS 8.0.1 or later](#). On each WildFire appliance that you want to add to a cluster, run **show system info | match version** on the WildFire appliance CLI to ensure that the appliance is running PAN-OS 8.0.1 or later.

When your WildFire appliances are available, perform the appropriate tasks:

- [Configure a Cluster and Add Nodes Locally](#)
- [Configure General Cluster Settings Locally](#)
- [Remove a Node from a Cluster Locally](#)

Configure a Cluster and Add Nodes Locally

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

When you add nodes to a cluster, the cluster automatically sets up communication between nodes based on the interfaces you configure for the controller node.

STEP 1 | Ensure that each WildFire appliance that you want to add to the cluster is running PAN-OS 8.0.1 or later.

On each WildFire appliance, run:

```
admin@WF-500> show system info | match version
```

STEP 2 | Verify that the WildFire appliances are not analyzing samples and are in standalone state (not members of another cluster).

1. On each appliance, display whether the appliance is analyzing samples:

```
admin@WF-500> show wildfire global sample-analysis
```

No sample should show as pending. All samples should be in a finished state. If samples are pending, wait for them to finish analysis. Pending samples display separately from malicious and non-malicious samples. Finish Date displays the date and time the analysis finished.

2. On each appliance, verify that the all processes are running:

```
admin@WF-500> show system software status
```

3. On each appliance, check to ensure the appliance is in a standalone state and does not already belong to a cluster:

```
admin@WF-500> show cluster membership
Service Summary: wfpc signature
Cluster name:
Address:         10.10.10.100
Host name:       WF-500
Node name:       wfpc-000000000000-internal
Serial number:   000000000000
Node mode:       stand_alone
Server role:     True
HA priority:
Last changed:   Mon, 06 Mar 2017 16:34:25 -0800
Services:       wfcore signature wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable

Application status:
global-db-service: ReadyStandalone
wildfire-apps-service: Ready
global-queue-service: ReadyStandalone
wildfire-management-service: Done
siggen-db: ReadyMaster

Diag report:
10.10.10.100: reported leader
'10.10.10.100', age 0.
10.10.10.100: local node passed sanity
check.
```

The highlighted lines show that the node is in standalone mode and is ready to be converted from a standalone appliance to a cluster node.



The 12-digit serial number in these examples (000000000000) is a generic example and is not a real serial number. WildFire appliances in your network have unique, real serial numbers.

STEP 3 | Configure the primary controller node.

This includes configuring the node as the primary controller of the HA pair, enabling HA, and defining the interfaces the appliance uses for the HA control link and for cluster communication and management.

1. Enable high availability and configure the control link interface connection to the controller backup node, for example, on interface eth3:

```
admin@WF-500# set deviceconfig high-availability enabled yes
interface ha1 port eth3 peer-ip-address <secondary-node-eth3-
ip-address>
```

2. Configure the appliance as the primary controller node:

```
admin@WF-500# set deviceconfig high-availability election-
option priority primary
```

3. (Optional) Configure the backup high-availability interface between the controller node and the controller backup node, for example, on the management interface:

```
admin@WF-500# set deviceconfig high-availability interface
ha1-backup port management peer-ip-address <secondary-node-
management-ip-address>
```

4. Configure the dedicated interface for communication and management within the cluster, including specifying the cluster name and setting the node role to controller node:

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
interface eth2 mode controller
```

This example uses eth2 as the dedicated cluster communication port.

The cluster name must be a valid sub-domain name with a maximum length of 63 characters. Only lower-case characters and numbers are allowed, and hyphens and periods if they are not at the beginning or end of the cluster name.

STEP 4 | Configure the controller backup node.

This includes configuring the node as the backup controller of the HA pair, enabling HA, and defining the interfaces the appliance uses for the HA control link and for cluster communication and management.

1. Enable high availability and configure the control link interface connection to the primary controller node on the same interface used on the primary controller node (eth3 in this example):

```
admin@WF-500# set deviceconfig high-availability enabled yes
interface hal port eth3 peer-ip-address <primary-node-eth3-
ip-address>
```

2. Configure the appliance as the controller backup node:

```
admin@WF-500# set deviceconfig high-availability election-
option priority secondary
```

3. (**Recommended**) Configure the backup high-availability interface between the controller backup node and the controller node, for example, on the management interface:

```
admin@WF-500# set deviceconfig high-availability interface
hal-backup port management peer-ip-address <primary-node-
management-ip-address>
```

4. Configure the dedicated interface for communication and management within the cluster, including specifying the cluster name and setting the node role to controller node:

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
interface eth2 mode controller
```

STEP 5 | Commit the configurations on both controller nodes.

On each controller node:

```
admin@WF-500# commit
```

Committing the configuration on both controller nodes forms a two-node cluster.

STEP 6 | Verify the configuration on the primary controller node.

On the primary controller node:

```
admin@WF-500(active-controller)> show cluster membership
Service Summary: wfpc signature
Cluster name:      mycluster
Address:           10.10.10.100
Host name:         WF-500
Node name:         wfpc-00000000000000-internal
Serial number:    000000000000
```

```
Node mode: controller
Server role: True
HA priority: primary
Last changed: Sat, 04 Mar 2017 12:52:38 -0800
Services: wfcore signature wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable
Application status:
global-db-service: JoinedCluster
wildfire-apps-service: Ready
global-queue-service: JoinedCluster
wildfire-management-service: Done
siggen-db: ReadyMaster
Diag report:
                10.10.10.110: reported leader '10.10.10.100', age
0.
                10.10.10.100: local node passed sanity check.
```

The prompt (active-controller) and the highlighted Application status lines show that the node is in controller mode, is ready, and is the primary controller node.

STEP 7 | Verify the configuration on the secondary controller node.

On the secondary controller node:

```
admin@WF-500(passive-controller)> show cluster membership
Service Summary: wfpc signature
Cluster name: mycluster
Address: 10.10.10.110
Host name: WF-500
Node name: wfpc-00000000000000-internal
Serial number: 000000000000
Node mode: controller
Server role: True
HA priority: secondary
Last changed: Fri, 02 Dec 2016 16:25:57 -0800
Services: wfcore signature wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable
Application status:
global-db-service: JoinedCluster
wildfire-apps-service: Ready
global-queue-service: JoinedCluster
wildfire-management-service: Done
siggen-db: ReadySlave
Diag report:
                10.10.10.110: reported leader '10.10.10.100', age
0.
                10.10.10.110: local node passed sanity check.
```

The prompt (passive-controller) and the highlighted Application status lines show that the node is in controller mode, is ready, and is the backup controller node.

STEP 8 | Test the node configuration.

Verify that the controller node API keys are viewable globally:

```
admin@WF-500(passive-controller)> show wildfire global api-keys  
allService Summary: wfpc signatureCluster name: mycluster
```

The API keys for both appliances should be viewable.

STEP 9 | Manually synchronize the high availability configurations on the controller nodes.

Synchronizing the controller nodes ensures that the configurations match and should only need to be done one time. After the high availability configurations are synchronized, the controller nodes keep the configurations synchronized and you do not need to synchronize them again.

1. On the primary controller node, synchronize the high availability configuration to the remote peer controller node:

```
admin@WF-500(active-controller)> request high-availability  
sync-to-remote running-config
```

If there is a mismatch between the primary controller node's configuration and the configuration on the controller backup node, the configuration on the primary controller node overrides the configuration on the controller backup node.

2. Commit the configuration:

```
admin@WF-500# commit
```


STEP 10 | Verify that the cluster is functioning properly.

To verify firewall-related information, you must first connect at least one firewall to a cluster node by selecting **Device > Setup > WildFire** and editing the **General Settings** to point to the node.

1. Display the cluster peers to ensure that both controllers are cluster members:

```
admin@WF-500(active-controller)> show cluster all-peers
```

2. Display API keys from both nodes (if you created [API keys](#)), from either controller node:

```
admin@WF-500(active-controller)> show wildfire global api-keys  
all
```

3. Access any sample from either controller node:

```
admin@WF-500(active-controller)> show wildfire global sample-  
status sha256 equal <value>
```

4. Firewalls can register and upload files to both nodes. [Confirm that the firewall is successfully forwarding samples](#).
5. Both nodes can download and analyze files.
6. All files analyzed after the cluster was created show two storage locations, one on each node.

STEP 11 | (Optional) Configure a worker node and add it to the cluster.

Worker nodes use the controller node's settings so that the cluster has a consistent configuration. You can add up to 18 worker nodes to a cluster for a total of 20 nodes in a cluster.

1. On the primary controller node, add the worker to the controller node's worker list:

```
admin@WF-500(active-controller)> configure  
admin@WF-500(active-controller)# set deviceconfig cluster mode  
controller worker-list <ip>
```

The `<ip>` is the [cluster management interface](#) IP address of the worker node you want to add to the cluster. Use separate commands to add each worker node to the cluster.

2. Commit the configuration the controller node:

```
admin@WF-500(active-controller)# commit
```

3. On the WildFire appliance you want to convert to a cluster worker node, configure the cluster to join, set the cluster communications interface, and place the appliance in worker mode:

```
admin@WF-500> configure
```

```
admin@WF-500# set deviceconfig cluster cluster-name <name>
interface eth2 mode worker
```

The cluster communications interface must be the same interface specified for intracluster communications on the controller nodes. In this example, `eth2` is the interface configured on the controller nodes for cluster communication.

4. Commit the configuration on the worker node:

```
admin@WF-500# commit
```

5. Wait for all services to come up on the worker node. Run `show cluster membership` and check the `Applicationstatus`, which shows all services and the `siggen-db` in a Ready state when all services are up.
6. On either cluster controller node, check to ensure that the worker node was added:

```
admin@WF-500> show cluster all-peers
```

The worker node you added appears in the list of cluster nodes. If you accidentally added the wrong WildFire appliance to a cluster, you can [Remove a Node from a Cluster Locally](#).

STEP 12 | Verify the configuration on the worker node.

1. On the worker node, check to ensure that the `Node mode` field shows that the node is in worker mode:

```
admin@WF-500> show cluster membership
```

2. Verify that firewalls can register on the worker node and that the worker node can download and analyze files.

Configure General Cluster Settings Locally

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

Some general settings are optional and some general settings are pre-populated with default values. It's best to at least check these settings to ensure that the cluster configuration matches your needs. General settings include:

- Connecting to the WildFire public cloud and submitting samples to the public cloud.
- Configuring data retention policies.
- Configuring logging.
- Setting the analysis environment (the VM image that best matches your environment) and customizing the analysis environment to best service the types of samples the firewalls submit to WildFire.

- Set IP addresses for the DNS server, NTP server, and more.

Configure WildFire settings using the CLI on the cluster's primary controller node. The rest of the cluster nodes use the settings configured on the cluster controller.

STEP 1 | Configure the general settings for the WildFire cluster. This process is similar to [Configuring the WildFire Appliance](#) settings.

1. **(Recommended)** [Reset the admin password](#).
2. [Configure the management interface settings](#). Set WildFire appliance cluster node IP addresses and the default gateway. Each WildFire appliance cluster node must have a static IP address in the same subnet. Also set the DNS server IP addresses.
3. [Set the WildFire appliance clock](#). Set the clock either manually or by specifying NTP servers, and set NTP Server authentication.
4. [Choose the virtual machine image for the appliance to use to analyze files](#).
5. **(Optional)** [Allow additional users to manage the WildFire appliance](#). Add administrator accounts and assign them roles to manage the cluster.
6. [Configure RADIUS authentication for administrator access](#).

STEP 2 | **(Optional)** Connect the cluster to the WildFire public cloud and configure the cloud services the cluster will use.

If business reasons don't prevent you from connecting the WildFire appliance cluster to the public WildFire cloud, connecting the cluster to the cloud provides benefits such as:

- Using the cloud's resources to perform sample analysis in multiple environments, using different methods.
- Automatically querying the cloud for verdicts before performing local analysis to offload work from the cluster. (Disabled by default.)
- Benefiting from and contributing to the intelligence of the global WildFire community.



The features described in this table row are not cluster-specific You can also configure these features on standalone WildFire appliances.

1. Benefit from the intelligence gathered from all connected WildFire appliances:

```
admin@WF-500(active-controller)# set deviceconfig setting  
wildfire cloud-server <hostname-value>
```

The default value for the WildFire public cloud server hostname is `wildfire-public-cloud`. You can [Forward Files for WildFire Analysis](#) to any public WildFire cloud.

2. If you connect the cluster to a WildFire public cloud, configure whether to automatically query the public cloud for verdicts before performing local analysis. Querying the public cloud first reduces the load on the local WildFire cluster:

```
admin@WF-500(active-controller)# set deviceconfig setting  
wildfire cloud-intelligence cloud-query (no | yes)
```

3. If you connect the cluster to a WildFire public cloud, configure the types of information for which you want to [Submit Locally-Discovered Malware or Reports to the WildFire](#)

Public Cloud (diagnostic data, XML reports about malware analysis, malware samples). If you send malware samples, the cluster doesn't send reports.

```
admin@WF-500(active-controller)# set deviceconfig setting
wildfire cloud-intelligence submit-diagnostics (no | yes)
submit-report (no | yes) submit-sample (no | yes)
```

STEP 3 | (Optional) Configure the controller node to publish the service status using the DNS protocol.

```
admin@WF-500(active-controller)# set deviceconfig cluster mode
controller service-advertisement dns-service enabled yes
```

STEP 4 | (Optional) Configure data retention policies for malicious and benign or grayware samples.

1. Select the amount of time to retain different types of data:

```
admin@WF-500(active-controller)# set deviceconfig setting
wildfire file-retention malicious <indefinite | 1-2000> non-
malicious <1-90>
```

The default for retaining malicious samples is indefinite (do not delete). The default for retaining non-malicious (benign and grayware) samples is 14 days.

STEP 5 | (Optional) Configure the preferred analysis environment.

1. If your analysis environment analyzes mostly executable samples or mostly document samples, you can allocate the majority of the cluster resources to analyzing those sample types:

```
admin@WF-500(active-controller)# set deviceconfig setting
wildfire preferred-analysis-environment (Documents |
Executables | default)
```

For each WildFire appliance in the cluster:

- The default option concurrently analyzes 16 documents, 10 portable executables (PE), and 2 email links.
- The Documents option concurrently analyzes 25 documents, 1 PE, and 2 email links.
- The Executables option concurrently analyzes 25 PEs, 1 document, and 2 email links.

You can configure a different preferred analysis environment for each node in the cluster. (If you manage the cluster from Panorama, Panorama can set the analysis environment for the entire cluster.)

STEP 6 | Configure node analysis settings.

1. (Optional) [Set Up Content Updates](#) to improve malware analysis.
2. [Set Up the VM Interface](#) to enable the cluster to observe malicious behaviors where the sample being analyzed seeks network access.
3. (Optional) [Enable Local Signature and URL Category Generation](#) to generate DNS and antivirus signatures and URL categories.

STEP 7 | Configure logging.

1. [Configure WildFire Submissions Log Settings](#).

Remove a Node from a Cluster Locally

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

You can remove nodes from a cluster using the local CLI. The procedure to remove a node is different in a two-node cluster than in a cluster with three or more nodes.

- Remove a worker node from a cluster with three or more nodes.

1. Decommission the worker node from the worker node's CLI:

```
admin@WF-500> request cluster decommission start
```



The `decommission` command only works with clusters that have three or more nodes. Do not use `decommission` to remove a node in a two-node cluster.

2. Confirm that decommissioning the node was successful:

```
admin@WF-500> show cluster membership
```

This command reports `decommission: success` after the worker node is removed from the cluster. If the command does not display successful decommission, wait a few minutes to allow the decommission to finish and then run the command again.

3. Delete the cluster configuration from the worker node's CLI:

```
admin@WF-500># delete deviceconfig cluster
```

4. Commit the configuration:

```
admin@WF-500># commit
```

5. Check that all processes are running:

```
admin@WF-500> show system software status
```

6. Remove the worker node from the controller node's worker list:

```
admin@WF-500(active-controller)# delete deviceconfig cluster  
mode controller worker-list <worker-node-ip>
```

7. Commit the configuration:

```
admin@WF-500(active-controller)# commit
```

8. On the controller node, check to ensure that the worker node was removed:

```
admin@WF-500(active-controller)> show cluster all-peers
```

The worker node you removed does not appear in the list of cluster nodes.

- Remove a controller node from a two-node cluster.

Each cluster must have two controller nodes in a high availability configuration under normal conditions. However, maintenance or swapping out controller nodes may require removing a controller node from a cluster using the CLI:

1. Suspend the controller node you want to remove:

```
admin@WF-500(passive-controller)> debug cluster suspend on
```

2. On the controller node you want to remove, delete the high-availability configuration. This example shows removing the controller backup node:

```
admin@WF-500(passive-controller)> configure  
admin@WF-500(passive-controller)# delete deviceconfig high-availability
```

3. Delete the cluster configuration:

```
admin@WF-500(passive-controller)# delete deviceconfig cluster
```

4. Commit the configuration:

```
admin@WF-500(passive-controller)# commit
```

5. Wait for services to come back up. Run **show cluster membership** and check the `Application` status, which shows all services and the `siggen-db` in a Ready state when all services are up. The `Node` mode should be `stand_alone`.
6. On the remaining cluster node, check to ensure that the node was removed:

```
admin@WF-500(active-controller)> show cluster all-peers
```

The controller node you removed does not appear in the list of cluster nodes.

7. If you have another WildFire appliance ready, add it to the cluster as soon as possible to restore high-availability ([Configure a Cluster and Add Nodes Locally](#)).

If you do not have another WildFire appliance ready to replace the removed cluster node, you should remove the high availability and cluster configurations from the remaining cluster node because one-node clusters are not recommended and do not provide high availability. It is better to manage a single WildFire appliance as a standalone appliance, not as a one-node cluster.

To remove the high availability and cluster configurations from the remaining node (in this example, the primary controller node):

```
admin@WF-500(active-controller)> configure  
admin@WF-500(active-controller)# delete deviceconfig high-availability  
admin@WF-500(active-controller)# delete deviceconfig cluster
```

```
admin@WF-500(active-controller)# commit
```

Wait for services to come back up. Run **show cluster membership** and check the `Application status`, which shows all services and the `siggen-db` in a Ready state when all services are up. The `Node mode` should be `stand_alone`.

Configure WildFire Appliance-to-Appliance Encryption

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

You can encrypt WildFire communications between appliances deployed in a cluster. By default, WildFire appliances send data using cleartext when communicating with management appliances as well as WildFire cluster peers. You can use either predefined or custom certificates to authenticate connections between WildFire appliance peers using the IKE/IPsec protocol. The predefined certificates meet current FIPS/CC/UCAPL-approved certification and compliance requirements. If you want to use custom certificates instead, you must select a FIPS/CC/UCAPL-compliant certificate or you will not be able to import the certificate.

You can configure WildFire appliance-to-appliance encryption locally using the WildFire CLI or centrally through Panorama. Keep in mind, all WildFire appliances within a given cluster must run a version of PAN-OS that supports encrypted communications.



If the WildFire appliances in your cluster uses FIPS/CC mode, encryption is automatically enabled using predefined certificates.

Depending on how you want to deploy appliance to appliance encryption, perform one of the following tasks:

- [Configure Appliance-to-Appliance Encryption Using Predefined Certificates Centrally on Panorama](#)
- [Configure Appliance-to-Appliance Encryption Using Custom Certificates Centrally on Panorama](#)
- [Configure Appliance-to-Appliance Encryption Using Predefined Certificates Through the CLI](#)
- [Configure Appliance-to-Appliance Encryption Using Custom Certificates Through the CLI](#)

Configure Appliance-to-Appliance Encryption Using Predefined Certificates Through the CLI

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

When configuring appliance-to-appliance encryption using the CLI, you must issue all commands from the WildFire appliance designated as the active-controller. The configuration changes are automatically distributed to the passive-controller. If you are operating a cluster with 3 or more nodes, you must also configure the WildFire cluster appliances acting as server nodes with the same settings as the active-controller.

STEP 1 | [Upgrade](#) each managed WildFire appliance to PAN-OS 9.0.

STEP 2 | Verify that your WildFire appliance cluster has been properly configured and is [operating in a healthy state](#).

STEP 3 | Enable secure cluster communication on the WildFire appliance designated as the active-controller.

```
set deviceconfig cluster encryption enabled yes
```

STEP 4 | (Recommended) **Enable HA Traffic Encryption.** This optional setting encrypts the HA traffic between the HA pair and is a Palo Alto Networks recommended best practice.



HA Traffic Encryption cannot be disabled when operating in FIPS/CC mode.

```
set deviceconfig high availability encryption enabled yes
```

STEP 5 | (Appliance clusters with 3 or more nodes only) Repeat steps 2-4 for the third WildFire appliance server node enrolled in the cluster.

Configure Appliance-to-Appliance Encryption Using Custom Certificates Through the CLI

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

When configuring appliance-to-appliance encryption using the CLI, you must issue all commands from the WildFire appliance designated as the active-controller. The configuration changes are automatically distributed to the passive-controller. If you are operating a cluster with 3 or more nodes, you must also configure the WildFire cluster appliances acting as server nodes with the same settings as the active-controller.

STEP 1 | [Upgrade](#) each managed WildFire appliance to PAN-OS 9.0.

STEP 2 | Verify that your WildFire appliance cluster has been properly configured and is [operating in a healthy state](#).

STEP 3 | Import (or optionally, generate) a certificate with a private key and its CA certificate. Keep in mind, if you previously configured the WildFire appliance and the firewall for [secure communications](#) using a custom certificate, you can also use that custom certificate for secure communications between WildFire appliances.

- To import a custom certificate, enter the following from the WildFire appliance
CLI: **scp import certificate from <value> file <value> remote-port <1-65535> source-ip <ip/netmask> certificate-name <value> passphrase <value> format <value>**
- To generate a custom certificate, enter the following from the WildFire appliance
CLI: **request certificate generate certificate-name name digest country-code state locality organization email filename ca**

```
signed-by | ocsf-responder-url days-till-expiry hostname [ ... ]  
request certificate generate certificate-name name digest  
country-code state locality organization email filename ca  
signed-by | ocsf-responder-url days-till-expiry ip [ ... ]  
request certificate generate certificate-name name
```

STEP 4 | Import the WildFire appliance keypair containing the server certificate and private key.

```
scp import keypair from <value> file <value> remote-port <1-65535>  
source-ip <ip/netmask> certificate-name <value> passphrase <value>  
format <pkcs12|pem>
```

STEP 5 | Configure and specify a SSL/TLS profile to define the certificate and protocol that WildFire appliances use for SSL/TLS services.

```
set deviceconfig setting management secure-conn-server ssl-tls-  
service-profile <profile name>
```

1. Create the SSL/TLS profile.

```
set shared ssl-tls-service-profile <name>
```

2. Specify the custom certificate.

```
set shared ssl-tls-service-profile <name> certificate <value>
```

3. Define the SSL/TLS range.

```
set shared ssl-tls-service-profile <name> protocol-settings  
min-version <tls1-0|tls1-1|tls1-2>
```

```
set shared ssl-tls-service-profile <name> protocol-settings  
max-version <tls1-0|tls1-1|tls1-2|max>
```

4. Specify the SSL/TLS profile. This SSL/TLS service profile applies to all connections between WildFire appliances and the firewall as well as WildFire appliance peers.

```
set deviceconfig setting management secure-conn-server ssl-  
tls-service-profile <ssltls-profile>
```

STEP 6 | Configure and specify a certificate profile to define the certificate and protocol that WildFire appliances use for SSL/TLS services.

1. Create the certificate profile.

```
set shared certificate-profile <name>
```

2. (Optional) Set the subject (common-name) or subject-alt name.

```
set shared certificate-profile <name> username-field subject  
<common-name>
```

```
set shared certificate-profile <name> username-field subject-  
alt <email|principal-name>
```

3. (Optional) Set the user domain.

```
set shared certificate-profile <name> domain <value>
```

4. Configure the CA.

```
set shared certificate-profile <name> CA <name>
```

```
set shared certificate-profile <name> CA <name> default-ocsp-  
url <value>
```

```
set shared certificate-profile <name> CA <name> ocsp-verify-  
cert <value>
```

5. Specify the certificate profile.

```
set deviceconfig setting management secure-conn-server  
certificate-profile <certificate-profile>
```

STEP 7 | [Import the certificate and private key pair.](#)

STEP 8 | Configure the firewall **Secure Communication Settings** on Panorama to associate the WildFire appliance cluster with the firewall custom certificate. This provides a secure communications channel between the firewall and WildFire appliance cluster. If you already

configured secure communications between the firewall and the WildFire appliance cluster and are using the existing custom certificate, proceed to step 9.

1. Select **Device > Certificate Management > Certificate Profile**.
2. [Configure a Certificate Profile](#).
3. Select **Device > Setup > Management > Secure Communication Settings** and click the **Edit** icon in **Secure Communication Settings** to configure the firewall custom certificate settings.
4. Select the **Certificate Type**, **Certificate**, and **Certificate Profile** from the respective drop-downs and configure them to use the custom certificate created in step 2.
5. Under Customize Communication, select **WildFire Communication**.
6. Click **OK**.

STEP 9 | Disable the use of the predefined certificate.

```
set deviceconfig setting management secure-conn-server disable-pre-defined-cert yes
```

STEP 10 | Specify the DNS name used for authentication found in the custom certificate (typically the SubjectName or the SubjectAltName). For example, the default domain name is **wfpc.service.mycluster.paloaltonetworks.com**

```
set deviceconfig setting wildfire custom-dns-name <custom_dns_name>.
```

STEP 11 | (Appliance clusters with 3 or more nodes only) Repeat steps 2-10 for the third WildFire appliance server node enrolled in the cluster.

Monitor a WildFire Cluster

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

You can check the operational status of your WildFire cluster using the CLI or Panorama. This allows you to verify that the [applications](#) and [services](#) running on a given node is functioning correctly. For a WildFire cluster to run correctly, the appropriate services and applications must be active on each node, and the status for each must be in the healthy state. Clusters operating outside these parameters might not run under optimal conditions or might indicate other problems and configuration issues.



The CLI displays information that is not available from Panorama. It's highly recommended to use the WildFire CLI when troubleshooting cluster-related issues.

You can view the current status of a WildFire controller node by executing a series of show commands from the WildFire CLI. The commands display configuration details, the current applications and services running on the appliance, as well as status/error messages. You can then use these details to determine the status of your cluster. Viewing the status does not interrupt any WildFire services and can be run at any time.

See the following sections for details on monitoring your WildFire appliance:

- [View WildFire Cluster Status Using the CLI](#)
- [View WildFire Cluster Status Using Panorama](#)
- [WildFire Application States](#)
- [WildFire Service States](#)

View WildFire Cluster Status Using the CLI

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

To confirm that your WildFire cluster is running within normal operating parameters, you must execute the following show commands:

- **show cluster controller**—Displays the status of active/passive WildFire cluster nodes.
- **show cluster all-peers**—Displays information about all of the members in a given WildFire cluster.
- **show cluster membership**—Displays WildFire appliance information for cluster and standalone nodes.
- **show cluster data-migration-status**—Displays the current status of the data migration process.

- **show log system**—Displays the WildFire event log, including system status details.

STEP 1 | On a WildFire appliance controller node, run:

```
admin@WF-500(active-controller)>show clustercontroller
```

A healthy WildFire cluster displays the following details:

- The name of the cluster the appliance has been enrolled in and its configured role.
- The K/V API online status indicates True when the internal cluster interface is functioning properly. A status of False can indicate an improperly configured node or a network issue.
- Task processing indicates True on active-controllers (primary) and False on passive-controllers (backup).
- The IP addresses for all WildFire nodes in the cluster are listed under App Service Avail.
- Up to three Good Core Servers. The number of Good Core Servers depends on the number of nodes running in the cluster. If you have a third node operating within a cluster, it automatically get configured as a server node to maximize cluster integrity.
- No Suspended Nodes.
- The Current Task provides background information about cluster-level operations, such as reboot, decommission, and suspend tasks.

The following example shows the output from an active controller configured in a 2-node WildFire cluster operating in a healthy state:

```
Cluster name:           WildFire_Cluster
K/V API online:        True
Task processing:       on
Active Controller:     True
DNS Advertisement:
App Service DNS Name:
App Service Avail:     2.2.2.14, 2.2.2.15
Core Servers:
    009701000026:      2.2.2.15
    009701000043:      2.2.2.14
Good Core Servers:     2
Suspended Nodes:
Current Task:
    * Showing latest completed task

    Request: startup from qa14 (009701000043/80025) at
2017-09-18 21:43:34 UTC
    null
    Response: permit by qa15 at 2017-09-18 21:45:15 UTC
    1/2 core servers available.
    Finished: success at 2017-09-18 21:43:47 UTC
```

STEP 2 | On a WildFire appliance controller node, run:

```
admin@WF-500>show cluster all-peers
```

A healthy WildFire cluster displays the following details:

- The general information about the WildFire nodes in the cluster are listed under `Address`, `Mode`, `Server`, `Node`, and `Name`.
- All WildFire cluster nodes are running the `wfpc` service, an internal file sample analysis service.
- Nodes operating as an active, passive, or server display `Serverrole` applied next to `Status`. If the node has been configured to be a server, but isn't operating as a server, the status displays `Serverrole assigned`.



In a 3-node deployment, the third server node is categorized as a worker.

- Recently removed nodes might be present but displays as `Disconnected`. It can take several days for a disconnected node to be removed from the cluster node list.
- The active controller node displays `siggen-db:ReadyMaster`.
- The passive controller node displays `siggen-db:ReadySlave`.



For more information about general WildFire application and service status details, refer to [WildFire Application States](#) and [WildFire Service States](#).

- The `TheDiag` report displays cluster system events and error messages:

Error Message	Description
Unreachable	The node was never reachable from the cluster controller.
Unexpected member	The node is not part of the cluster configuration. The node might have recently deleted from the cluster configuration or the result of misconfiguration.
Left cluster	The node is no longer reachable from the cluster controller.
Incorrect cluster name	The node has an incorrectly configured cluster name.
Connectivity unstable	The node's connection to the cluster controller is unstable.
Connectivity lost	The node's connectivity to the cluster controller has been lost.

Error Message	Description
Unexpected server serial number	The unexpected presence of a server node has been detected.

The following example shows a 3-node WildFire cluster operating in a healthy state:

```

Address      Mode      Server  Node Name
-----
2.2.2.15    controller Self   True  qa15
wfpc
applied
15:37:40 -0700
JoinedCluster
Stopped
JoinedCluster
service: Done
Service: infra signature wfcore
Status: Connected, Server role
Changed: Mon, 18 Sep 2017
WF App:
  global-db-service:
  wildfire-apps-service:
  global-queue-service:
  wildfire-management-
  siggen-db: ReadySlave

2.2.2.14    controller Peer   True  qa14
wfpc
applied
15:37:40 -0700
commit-lock
Stopped
ReadyStandalone
service: Done
Service: infra signature wfcore
Status: Connected, Server role
Changed: Mon, 18 Sep 2017
WF App:
  global-db-service:
  wildfire-apps-service:
  global-queue-service:
  wildfire-management-
  siggen-db: ReadyMaster

2.2.2.16    worker           True  wf6240
applied
11:11:15 -0800
Ready
Service: infra wfcore wfpc
Status: Connected, Server role
Changed: Wed, 22 Feb 2017
WF App:
  wildfire-apps-service:
  
```

```

JoinedCluster          global-db-service:
JoinedCluster          global-queue-service:
DataMigrationFailed    local-db-service:
Diag report:           2.2.2.14: reported leader '2.2.2.15', age 0.
                       2.2.2.15: local node passed sanity check.

```

STEP 3 | On a WildFire appliance controller node, run:

```
admin@WF-500>show cluster membership
```

A healthy WildFire cluster displays the following details:

- The general WildFire appliance configuration details, such as the cluster name, IP address of the appliance, serial number, etc.
- `Server role` indicates whether or not the WildFire appliance is operating as a cluster server. Cluster servers operate additional infrastructure applications and services. You can have a maximum of three servers per cluster.
- `Node mode` describes the role of a WildFire appliance. WildFire appliances enrolled in a cluster can be either a `controller` or `worker` node depending on your configuration and the number of nodes in your deployment. Appliances that are not a part of a cluster displays `stand_alone`.
- Operates the following Services based on the cluster node role:

Node Type	Services Operating on the Node
Controller Node (Active or Passive)	<ul style="list-style-type: none"> • <code>infra</code> • <code>wfpc</code> • <code>signature</code> • <code>wfcore</code>
Server Node	<ul style="list-style-type: none"> • <code>infra</code> • <code>wfpc</code> • <code>wfcore</code>
Worker Node	<ul style="list-style-type: none"> • <code>infra</code>

Node Type	Services Operating on the Node
	<ul style="list-style-type: none"> • wfpc

- **HA priority** displays primary or secondary depending on its configured role, however this setting is independent of the current HA state of the appliance.
- **Work queue status** shows the sample analysis backlog as well as samples that are currently being analyzed. This also indicates how much load a particular WildFire appliance receives.



For more information about WildFire application and service status details, refer to [WildFire Application States](#) and [WildFire Service States](#).

The following example shows a WildFire controller operating in a healthy state:

```

Service Summary: wfpc signature
Cluster name: qa-auto-0ut1
Address: 2.2.2.15
Host name: qa15
Node name: wfpc-009701000026-internal
Serial number: 009701000026
Node mode: controller
Server role: True
HA priority: secondary
Last changed: Fri, 22 Sep 2017 11:30:47 -0700
Services: wfcore signature wfpc infra
Monitor status:
    Serf Health Status: passing
    Agent alive and reachable
    Service 'infra' check: passing
Application status:
    global-db-service: ReadyLeader
    wildfire-apps-service: Ready
    global-queue-service: ReadyLeader
    wildfire-management-service: Done
    siggen-db: Ready
Work queue status:
    sample anaysis queued: 0
    sample anaysis running: 0
    sample copy queued: 0
    sample copy running: 0
Diag report:
    2.2.2.14: reported leader '2.2.2.15', age 0.
    2.2.2.15: local node passed sanity check.

```

STEP 4 | On a WildFire appliance controller node, run:

```
admin@WF-500(active-controller)>show clusterdata-migration-status
```

The WildFire appliance displays the following data migration details:

- Do not forward files to the WildFire appliance cluster when data migration is in progress. When data migration is finishes, the completion timestamp displays.
- Topology changes to the WildFire cluster (for examples, adding or removing nodes and changing node roles) triggers data migration events.
- Data migration can occur upon upgrade to a new version of WildFire. After upgrading, be sure to check the operational status of your WildFire cluster to verify proper functionality.

The following example shows the progress of data migration in a WildFire appliance cluster:

```
admin@WF-500(active-controller)>: show data-migration-status  
100% completed on Mon Sep 9 21:44:48 PDT 2019
```

STEP 5 | On a WildFire appliance active, passive, and server nodes, run:

```
admin@WF-500(active-controller)>show log systemsubtype direction
equal backward
```

This command displays all WildFire logged events categorized as a wildfire-appliance subtype from newest to oldest.

- You must issue this command to all nodes in a cluster. For example, if you are operating a 3-node cluster, you must verify the status on the active controller, passive controller, and the server node.
- The log messages returned by the WildFire appliance CLI can include numerous subtypes. You can filter the logs based on a common subtype keyword. Use the following command argument to filter based on a specific component:
 - global-queue—**matchqueue**, for example **show log system directionequal backward | match queue**
 - global-database—**match global**, for example **show log system direction equal backward | matchglobal**
 - signature-generation—**match signature**, for example **show log system direction equal backward| match signature**
- WildFire appliance clusters operating normally return the following status readouts for each node in a 2-node cluster. Healthy WildFire cluster nodes have differing status readouts based on the role of an appliance.

Use the following checklist to verify that the WildFire appliance services are running correctly in your cluster deployment.

❑ **Active Controller**

Component	Active Controller Status
global-queue	<ul style="list-style-type: none"> ❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	<ul style="list-style-type: none"> ❑ infogeneral general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	<ul style="list-style-type: none"> ❑ infowildfir cluster 0 Signature generation service status set to ReadyMaster ❑ info wildfir cluster 0 Signature generationservice status set to ReadyMaster

Component	Active Controller Status
-----------	--------------------------



The log messages returned by the WildFire appliance(s) are shown from newest to oldest. If you do not use the **direction equal backward** command argument as shown in the above procedure, the WildFire appliance CLI returns the log messages from oldest to newest.

❑ Passive Controller

Component	Passive Controller Status Example
-----------	-----------------------------------

global-queue

- ❑ infogeneral general 0 Setup policy for global-queue service
- ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status JoinedCluster
- ❑ info general general 0 Join cluster for global-queueservice - succeeded
- ❑ info general general 0 Setup policy for global-queue service

global-database

- ❑ infogeneral general 0 Setup policy for global-queue service
- ❑ info general general 0 Restore applications:done, For global-db bootstrap and join cluster
- ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster
- ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster
- ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster
- ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster
- ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster
- ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster
- ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster

Component	Passive Controller Status Example
	<pre>❑ info general general 0 Bootstrap and join clusterfor global-db service</pre>
signature-generation	<pre>❑ infowildfir cluster 0 Signature generation service status set to ReadySlave ❑ info wildfir cluster 0 Signature generationservice status set to ReadySlave</pre>



The log messages returned by the WildFire appliance(s) are shown from newest to oldest. If you do not use the **direction equal backward** command argument as shown in the above procedure, the WildFire appliance CLI returns the log messages from oldest to newest.

- WildFire appliance clusters operating normally return the following status readouts for each node in a 3-node cluster. Healthy WildFire cluster nodes have differing status readouts based on the role of an appliance.

Use the following checklist to verify that the WildFire appliance services are running correctly in your cluster deployment.

- **Active Controller**

Component	Active Controller Status
global-queue	<pre>❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global- queueservice - succeeded ❑ info general general 0 Setup policy for global- queue service</pre>
global-database	<pre>❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global- dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global- dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster</pre>

Component	Active Controller Status
	<ul style="list-style-type: none"> ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, For global-db bootstrap and join cluster ❑ 2019/07/19 14:40:19 info general general 0 Bootstrap and join cluster for global-db service
signature-generation	<ul style="list-style-type: none"> ❑ infowildfire cluster 0 Signature generation service status set to ReadyMaster



The log messages returned by the WildFire appliance(s) are shown from newest to oldest. If you do not use the **direction equal backward** command argument as shown in the above procedure, the WildFire appliance CLI returns the log messages from oldest to newest.

- **Passive Controller**

Component	Passive Controller Status
global-queue	<ul style="list-style-type: none"> ❑ info general general 0 Setup policy for global-queue service ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status ReadyLeader ❑ info general general 0 Setup policy for global-queue service
global-database	<ul style="list-style-type: none"> ❑ info general general 0 I'm cluster leader, bootstrap for global-db service ❑ info general general 0 Setup policy for global-queue service
signature-generation	<ul style="list-style-type: none"> ❑ infowildfire cluster 0 Signature generation service status set to ReadySlave ❑ info wildfire cluster 0 Signature generationservice status set to ReadySlave

Component	Passive Controller Status
-----------	---------------------------



The log messages returned by the WildFire appliance(s) are shown from newest to oldest. If you do not use the **direction equal backward** command argument as shown in the above procedure, the WildFire appliance CLI returns the log messages from oldest to newest.

- Server Node

Component	Server Node Status
global-queue	<ul style="list-style-type: none"> ❑ infowildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded withstatus JoinedCluster ❑ info general general 0 Join cluster for global-queueservice - succeeded ❑ info general general 0 Setup policy for global-queue service ❑ info wildfire cluster 0 Global queue (rabbitmq)cluster formation succeeded with status StandbyAsWorker
global-database	<ul style="list-style-type: none"> ❑ infogeneral general 0 Restore applications: done, For global-db bootstrap andjoin cluster ❑ info general general 0 Start vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Start wf_services, Forglobal-db bootstrap and join cluster ❑ info general general 0 Suspend applications:done, For global-db bootstrap and join cluster ❑ info general general 0 Stop vm_mgr, For global-dbbootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-dbbootstrap and join cluster ❑ info general general 0 Stop wf_services, Forglobal-db bootstrap and join cluster ❑ 2019/07/19 14:32:50 info general general 0Promote worker node and join cluster for global-db service

Component	Server Node Status
signature-generation	<ul style="list-style-type: none"> ❑ infowildfire cluster 0 Signature generation service status set to Stopped ❑ critical wildfire cluster 0 Signature DataMigrationDone



The log messages returned by the WildFire appliance(s) are shown from newest to oldest. If you do not use the **direction equal backward** command argument as shown in the above procedure, the WildFire appliance CLI returns the log messages from oldest to newest.

WildFire Application States

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ❑ WildFire License

The WildFire appliance operates a series of internal applications to manage and coordinate processing of sample data. These applications and their requisite statuses are shown when viewing the status of a WildFire appliance cluster.

The following list shows the cluster components, purpose, and status conditions:

Name	Description	Possible Status Conditions	Definition
global-db-service	This application database is used to store WildFire analysis data.	AcquiringSessionSpinLock	Waiting for the session spin lock until acquiring the lock or timeout.
		Bootstrapping	The sample database application is currently in a bootstrapping state.
		BootstrappingNoMeet	The local sample database service started without forming a cluster with other WildFire appliances.
		FailedToBecomeWorker	Failed to join the cluster as a worker node.
		FailedToBootstrap	The bootstrapping process has failed.
		FailedToJoinCluster	Failed to join the cluster.

Name	Description	Possible Status Conditions	Definition
		FailedToStartServices	Internal database services failed to start.
		MaintenanceDecommission	Starting decommission process for database services.
		MaintenanceDecommissionDone	Database service has been decommissioned.
		MaintenanceFailover	Starting the process to demote local service and failover backup replica.
		MaintenanceFailed	Service failover has failed.
		MaintenanceFailoverDone	Service failover is done.
		MaintenanceRecoverFromSplitbrain	In the WildFire appliance is currently in split-brain mode, the database service state will be set to MaintenanceRecoverFromSplitbrain upon the start of the service.
		MaintenanceSuspend	The database service is in the process of being suspended as a result of the user issuing one of the following commands: debug cluster suspend or request cluster decommission.
		MaintenanceSuspendDone	The database service has completed the suspension process.
		DataMigration	The contents of the local database is being merged with the primary database. This occurs when a WildFire appliance joins a cluster.

Name	Description	Possible Status Conditions	Definition
		DataMigrationDone	The data migration process is complete.
		DataMigrationFailed	The data migration process has failed.
		JoinedCluster	The local database service has joined the cluster.
		Ready	The database service is in a ready state.
		ReadyLeader	The database service is in a ready state and the appliance is set as the leader.
		ReadyStandalone	The database service is in a ready state and the appliance is operating as a standalone appliance.
		Splitbrain	A split-brain condition has been detected and the database services has entered split-brain mode. The service will transition to ReadyStandalone shortly.
		StandbyAsWorker	The worker node database service is in a standby state.
		WaitingforLeaderReady	The local node is waiting to join the leader node.

Name	Description	Possible Status Conditions	Definition
global-queue-service	Handles the management and prioritization of samples sent for WildFire analysis.	Bootstrapping	Queuing service application is currently in a bootstrapping state.
		FailedToBecomeWorker	Failed to join the cluster as a worker node.

Name	Description	Possible Status Conditions	Definition
		FailedToBootstrap	The bootstrapping process has failed.
		FailedToJoinCluster	Failed to join the cluster.
		FailedToStartServices	Internal queuing services failed to start.
		MaintenanceDecommission	Starting decommission process for queuing services.
		MaintenanceDecommissionDone	Queuing service has been decommissioned.
		MaintenanceFailover	Starting the process to demote local service and failover backup replica.
		MaintenanceFailed	Service failover has failed.
		MaintenanceFailoverDone	Service failover is done.
		MaintenanceRecoverFromSplitbrain	If the WildFire appliance is currently in split-brain mode, the queuing service state will be set to
		MaintenanceSuspend	The queuing service is in the process of being suspended as a result of the user issuing one of the following commands: debug cluster suspend or request cluster decommission.
		MaintenanceSuspendDone	The queuing service has completed the suspension process.
		JoinedCluster	The queuing service has joined the cluster.
		Ready	The queuing service is in a ready state.

Name	Description	Possible Status Conditions	Definition
		ReadyLeader	The queuing service is in a ready state and the appliance is set as the leader.
		ReadyStandalone	The queuing service is in a ready state and the appliance is operating as a standalone appliance.
		Splitbrain	A split-brain condition has been detected and the queuing services has entered split-brain mode. The service will transition to ReadyStandalone shortly.
		StandbyAsWorker	The worker node queuing service is in a standby state.

Name	Description	Possible Status Conditions	Definition
siggen-db	Generates WildFire private signatures and analysis samples.	DatabaseFailover	When HA failover occurs, the passive controller becomes the active controller. The signature service in the passive controller becomes the primary and the state is set to DatabaseFailover.
		DatabaseFailoverFailed	The signature database failover has failed.
		DataMigration	The contents of the local signature database is being merged with the primary database. This occurs when a WildFire appliance joins a cluster.
		DataMigrationDone	The data migration process is complete.

Name	Description	Possible Status Conditions	Definition
		DataMigrationFailed	The data migration process has failed.
		Deregistered	Signature database service has been deregistered.
		MaintenanceDecommission	Starting decommission process for signature database services.
		MaintenanceDecommissionDone	Queuing service has been decommissioned.
		MaintenanceFailover	Starting the process to demote local service and failover backup replica.
		MaintenanceFailoverDone	Service failover is done.
		MaintenanceSuspend	The signature database service is in the process of being suspended as a result of the user issuing one of the following commands: debug cluster suspend or request cluster decommission.
		MaintenanceSuspendDone	The signature database service has completed the suspension process.
		MigrateMalwareDatabase	When upgrading PAN-OS from version 7.1 to 8.0, the sample data is converted to a different format. These states indicate the progress of the data migration process.
		MigrateSiggenDatabaseStage1	
		MigrateSiggenDatabaseStage2	
		MigrateSiggenDatabaseStage3	
		Ready	The signature database service is in a ready state.
		ReadyMaster	The signature database service is in primary mode and is operating on the active controller.

Name	Description	Possible Status Conditions	Definition
		ReadySlave	The signature database service is in backup mode and is operating on the passive controller.
		ReadyStandalone	The signature database service is in a ready state and the appliance is operating as a standalone appliance.
		Splitbrain	A split-brain condition has been detected and the signature database service has entered split-brain mode. The service will transition to ReadyStandalone shortly.
		Stopped	The signature database service has stopped on the appliance.

Name	Description	Possible Status Conditions	Definition
wildfire-management-service	WildFire work mode management service.	Running	The WildFire management service is in an operational state.
		Done	The WildFire management service has finished running.

Name	Description	Possible Status Conditions	Definition
wildfire-apps-service	WildFire infrastructure applications.	Deregistered	The WildFire applications service has been deregistered.
		Ready	The WildFire applications service is in a ready state.
		Restored	The WildFire applications service has finished maintenance procedures.

Name	Description	Possible Status Conditions	Definition
		Scheduling	The WildFire applications service is in a scheduling state.
		SetupSampleStorage	This WildFire applications service operates when WildFire is being upgraded from 7.1 to 8.0.
		Stopped	The WildFire applications service has stopped on the appliance.
		Suspended	The WildFire applications service has been suspended due to maintenance.

WildFire Service States

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

The WildFire appliance operates a series of internal services to manage and coordinate processing of sample data. These services and their requisite statuses are shown when viewing the status of a WildFire appliance cluster.

The following list shows the WildFire service components, description, status conditions, and other relevant details:

Name	Purpose	Impacted Nodes	Status
infra	Indicates that a WildFire cluster infrastructure service is operating on a given node.	All nodes	Displays in CLI status screen when the service is operating. If these services are not present for a given node, verify the configuration of the appliance.
wfpc	Indicates that the file sample analysis service (WildFire Private Cloud) is capable of file analysis and report generation.		
signature	Generates WildFire private signatures and analysis samples.	Active (primary) /	

Name	Purpose	Impacted Nodes	Status
		passive (backup) controller	
wfc core	Indicates that the node is running as a server for WildFire cluster infrastructure services.	Server node	

Upgrade WildFire Appliances in a Cluster

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

You can use the CLI to upgrade WildFire appliances enrolled in a cluster individually, or use Panorama to upgrade the cluster as a group.

Depending on the number of samples the WildFire appliance has analyzed and stored, the time required to upgrade the appliance software varies; this is because upgrading requires the migration of all malware samples and 14 days of benign samples. Allow 30 to 60 minutes for each WildFire appliance that you have used in a production environment.



- *All nodes in a cluster must run the same version of the operating system.*
- *Panorama can manage WildFire appliances and appliance clusters running PAN-OS software versions 8.0.1 or later.*
- *Ensure the devices are connected to a reliable power source. A loss of power during an upgrade can make the devices unusable.*

Depending on your deployment, perform one of the following tasks to upgrade your WildFire cluster:

- [Upgrade a Cluster Centrally on Panorama with an Internet Connection](#)
- [Upgrade a Cluster Centrally on Panorama without an Internet Connection](#)
- [Upgrade a Cluster Locally with an Internet Connection](#)
- [Upgrade a Cluster Locally without an Internet Connection](#)

Upgrade a Cluster Locally with an Internet Connection

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

To upgrade a cluster locally, you must individually upgrade each WildFire appliance enrolled in a cluster. When an appliance finishes upgrading, it automatically re-enrolls into the cluster that it was originally assigned to.

STEP 1 | Temporarily suspend sample analysis.

1. Stop firewalls from forwarding any new samples to the WildFire appliance.
 1. Log in to the firewall web interface.
 2. Select **Device > Setup > WildFire** and edit **General Settings**.
 3. Clear the **WildFire Private Cloud** field.
 4. Click **OK** and **Commit**.
2. Confirm that analysis for samples the firewalls already submitted to the appliance is complete:

```
admin@WF-500(passive-controller)> show  
wildfire latest samples
```



If you do not want to wait for the WildFire appliance to finish analyzing recently-submitted samples, you can continue to the next step. However, consider that the WildFire appliance then drops pending samples from the analysis queue.

STEP 2 | Install the latest WildFire appliance content update. This update equips the appliance with the latest threat information to accurately detect malware.



This process can take up to 6 hours or more on older appliances.

1. Verify that you are running the latest content update on your WildFire appliance.

```
admin@WF-500> request wf-content upgrade check
```

2. Download the latest WildFire content update package.

```
admin@WF-500> request  
wf-content upgrade download latest
```

If you do not have direct connectivity to the Palo Alto Networks Update Server, you can download and [Install WildFire Content Updates from an SCP-Enabled Server](#).

3. View the status of the download.

```
admin@WF-500> show jobs all
```

4. After the download is complete, install the update.

```
admin@WF-500> request  
wf-content upgrade install version latest
```

STEP 3 | (Required when upgrading to PAN-OS 10.2.2) Upgrade the VM images on the WildFire appliance.

1. Log in and access the [Palo Alto Networks Customer Support Portal Software Download Page](#). You can also manually navigate to the software download page from the Support homepage by going to **Updates > Software Updates**.
2. From the software updates page, select **WF-500 Guest VM Images** and download the following VM image files:



Palo Alto Networks periodically updates the VM image files; as a result, the specific filename changes based on the version that is available. Be sure to download the latest version, whereby the m-x.x.x in the filename indicates the release number; additionally, there is a release date that can be cross-referenced to help determine the latest version.

- WFWinXpAddon3_m-1.0.1.xpaddon3
 - WFWinXpGf_m-1.0.1.xpgf
 - WFWin7_64Addon1_m-1.0.1.7_64addon1
 - WFWin10Base_m-1.0.1.10base
3. Upload the VM images to the WildFire appliance.
 1. Import the VM image from the SCP server:

```
admin@WF-500>scp import wildfire-vm-image from  
<username@ip_address>/<folder_name>/<vm_image_filename>
```

For example:

```
admin@WF-500>scp import wildfire-vm-image from  
user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
```

2. To check the status of the download, use the following command:

```
admin@WF-500>show jobs all
```

3. Repeat for the remaining VM images.
4. Install the VM image.
 1.

```
admin@WF-500>request system wildfire-vm-image upgrade  
install file <vm_image_filename>
```
 2. Repeat for the remaining VM images.
5. Confirm that the VM images have been properly installed and enabled on the WildFire appliance.
 1. (Optional) View a list of available virtual machines images:

```
admin@WF-500> show wildfire vm-images
```

The output displays the available VM images.

2. Commit the configuration:

```
admin@WF-500# commit
```

3. View the active VM image by running the following command:

```
admin@WF-500> show wildfire status
```

- STEP 4 |** Verify that the WildFire appliance software version you want to install is available.

```
admin@WF-500(passive-controller)> request  
system software check
```

- STEP 5 |** Download the PAN-OS 10.2.2 software version to the WildFire appliance.

You cannot skip any major release version when upgrading the WildFire appliance. For example, if you want to upgrade from PAN-OS 6.1 to PAN-OS 7.1, you must first download and install PAN-OS 7.0. The examples in this procedure demonstrate how to upgrade to PAN-OS 10.2.2. Replace 10.2.2 with the appropriate target release for your upgrade.

Download the 10.2.2 software version.

```
admin@WF-500(passive-controller)> request  
system software download version 10.2.2
```

To check the status of the download, use the following command

```
admin@WF-500(passive-controller)> show  
jobs all
```

- STEP 6 |** Confirm that all services are running.

```
admin@WF-500(passive-controller)> show  
system software status
```

- STEP 7 |** Install the 10.2.2 software version.

```
admin@WF-500(passive-controller)> request  
system software install version 10.2
```

STEP 8 | Complete the software upgrade.

1. Confirm that the upgrade is complete. Run the following command and look for the job type **Install** and status **FIN**:

```
admin@WF-500(passive-controller)> show
jobs all

Enqueued Dequeued ID Type Status Result Completed
-----
14:53:15 14:53:15 5 Install FIN OK 14:53:19
```

2. Gracefully restart the appliance:

```
admin@WF-500(passive-controller)> request
cluster reboot-local-node
```



The upgrade process could take 10 minutes or over an hour, depending on the number of samples stored on the WildFire appliance.

STEP 9 | Repeat steps 1-8 for each WildFire worker node in the cluster.**STEP 10 |** (Optional) View the status of the reboot tasks on the WildFire controller node.

On the WildFire cluster controller, run the following command and look for the job type **Install** and Status **FIN**:

```
admin@WF-500(active-controller)> show
cluster task pending
```

STEP 11 | Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the sw-version field shows the upgraded release version:

```
admin@WF-500(passive-controller)> show
system info | match sw-version
```

2. Confirm that all processes are running:

```
admin@WF-500(passive-controller)> show
system software status
```

3. Confirm that the auto-commit (**AutoCom**) job is complete:

```
admin@WF-500(passive-controller)> show
```

jobs all

- Confirm that data migration has successfully completed. Run `show cluster data-migration-status` to view the progress of the database merge. After the data merge is complete the completion timestamp displays:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```



The duration of a data merge depends on the amount of data stored on the WildFire appliance. Be sure to allot at least several hours for recovery as the data merge can be a lengthy process.

Upgrade a Cluster Locally without an Internet Connection

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

To upgrade a cluster locally, you must individually upgrade each WildFire appliance enrolled in a cluster. When an appliance finishes upgrading, it automatically re-enrolls into the cluster that it was originally assigned to.

STEP 1 | Temporarily suspend sample analysis.

- Stop firewalls from forwarding any new samples to the WildFire appliance.
 - Log in to the firewall web interface.
 - Select **Device > Setup > WildFire** and edit **General Settings**.
 - Clear the **WildFire Private Cloud** field.
 - Click **OK** and **Commit**.
- Confirm that analysis for samples the firewalls already submitted to the appliance is complete:

```
admin@WF-500(passive-controller)> show
wildfire latest samples
```



If you do not want to wait for the WildFire appliance to finish analyzing recently-submitted samples, you can continue to the next step. However, consider that the WildFire appliance then drops pending samples from the analysis queue.

STEP 2 | Retrieve the content update file from the update server.

- Log in to the [Palo Alto Networks Support Portal](#) and click **Dynamic Updates**.
- In the WildFire Appliance section, locate the latest WildFire appliance content update and download it.
- Copy the content update file to an SCP-enabled server and note the file name and directory path.

STEP 3 | Install the content update on the WildFire appliance.

1. Log in to the WildFire appliance and download the content update file from the SCP server:

```
admin@WF-500> scp
import wf-content from username@host:path
```

For example:

```
admin@WF-500> scp
import wf-content from bart@10.10.10.5:c:/updates/panup-all-
wfmeta-2-253.tgz
```



*If your SCP server is running on a non-standard port or if you need to specify the source IP, you can also define those options in the **scp import** command.*

2. Install the update:

```
admin@WF-500> request
wf-content upgrade install file panup-all-wfmeta-2-253.tgz
```

3. View the status of the installation:

```
admin@WF-500> show
jobs all
```

STEP 4 | Verify the content update.

Verify the content version:

```
admin@WF-500> show
system info | match wf-content-version
```

The following output now shows version 2-253:

```
wf-content-version: 2-253
```

STEP 5 | (Required when upgrading to PAN-OS 10.2.2) Upgrade the VM images on the WildFire appliance.

1. Log in and access the [Palo Alto Networks Customer Support Portal Software Download Page](#). You can also manually navigate to the software download page from the Support homepage by going to **Updates > Software Updates**.
2. From the software updates page, select **WF-500 Guest VM Images** and download the following VM image files:



Palo Alto Networks periodically updates the VM image files; as a result, the specific filename changes based on the version that is available. Be sure to download the latest version, whereby the m-x.x.x in the filename indicates the release number; additionally, there is a release date that can be cross-referenced to help determine the latest version.

- WFWinXpAddon3_m-1.0.1.xpaddon3
 - WFWinXpGf_m-1.0.1.xpgf
 - WFWin7_64Addon1_m-1.0.1.7_64addon1
 - WFWin10Base_m-1.0.1.10base
3. Upload the VM images to the WildFire appliance.
 1. Import the VM image from the SCP server:

```
admin@WF-500>scp import wildfire-vm-image from  
<username@ip_address>/<folder_name>/<vm_image_filename>
```

For example:

```
admin@WF-500>scp import wildfire-vm-image from  
user1@10.0.3.4:/tmp/WFWin7_64Addon1_m-1.0.1.7_64addon1
```

2. To check the status of the download, use the following command:

```
admin@WF-500>show jobs all
```

3. Repeat for the remaining VM images.
4. Install the VM image.
 1.

```
admin@WF-500>request system wildfire-vm-image upgrade  
install file <vm_image_filename>
```
 2. Repeat for the remaining VM images.
5. Confirm that the VM images have been properly installed and enabled on the WildFire appliance.
 1. (Optional) View a list of available virtual machines images:

```
admin@WF-500> show wildfire vm-images
```

The output displays the available VM images.

2. Commit the configuration:

```
admin@WF-500# commit
```

3. View the active VM images by running the following command:

```
admin@WF-500> show wildfire status
```

STEP 6 | Verify that the WildFire appliance software version you want to install is available.

```
admin@WF-500(passive-controller)> request  
system software check
```

STEP 7 | Download the PAN-OS 10.2.2 software version to the WildFire appliance.

You cannot skip any major release version when upgrading the WildFire appliance. For example, if you want to upgrade from PAN-OS 6.1 to PAN-OS 7.1, you must first download and install PAN-OS 7.0. The examples in this procedure demonstrate how to upgrade to PAN-OS 10.2.2. Replace 10.2.2 with the appropriate target release for your upgrade.

Download the 10.2.2 software version:

1. Navigate to the [Palo Alto Networks Support](#) site and in the Tools section, click on **Software Updates**.
2. Download the WildFire appliance software image file to be installed to a computer running SCP server software.
3. Import the software image from the SCP server:

```
admin@WF-500> scp import software from  
<username@ip_address>/<folder_name>/<imagefile_name>
```

For example:

```
admin@WF-500> scp import software  
from user1@10.0.3.4:/tmp/WildFire_m-10.2.2
```

4. To check the status of the download, use the following command:

```
admin@WF-500> show jobs all
```

STEP 8 | Confirm that all services are running.

```
admin@WF-500(passive-controller)> show
```

system software status

STEP 9 | Install the 10.2.2 software version.

```
admin@WF-500(passive-controller)> request
system software install version 10.2.2
```

STEP 10 | Complete the software upgrade.

1. Confirm that the upgrade is complete. Run the following command and look for the job type **Install** and status **FIN**:

```
admin@WF-500(passive-controller)> show
jobs all
```

```
Enqueued Dequeued ID Type Status Result Completed
-----
14:53:15 14:53:15 5 Install FIN OK 14:53:19
```

2. Gracefully restart the appliance:

```
admin@WF-500(passive-controller)> request
cluster reboot-local-node
```



The upgrade process could take 10 minutes or over an hour, depending on the number of samples stored on the WildFire appliance.

STEP 11 | Repeat steps 1-10 for each WildFire worker node in the cluster.

STEP 12 | (Optional) View the status of the reboot tasks on the WildFire controller node.

On the WildFire cluster controller, run the following command and look for the job type **Install** and Status **FIN**:

```
admin@WF-500(active-controller)> show
cluster task pending
```

STEP 13 | Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the sw-version field shows the upgraded release version:

```
admin@WF-500(passive-controller)> show
system info | match sw-version
```

2. Confirm that all processes are running:

```
admin@WF-500(passive-controller)> show
```

system software status

3. Confirm that the auto-commit (**AutoCom**) job is complete:

```
admin@WF-500(passive-controller)> show  
jobs all
```

4. Confirm that data migration has successfully completed. Run `show cluster data-migration-status` to view the progress of the database merge. After the data merge is complete, the completion timestamp displays:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```



The duration of a data merge depends on the amount of data stored on the WildFire appliance. Be sure to allot at least several hours for recovery as the data merge can be a lengthy process.

Troubleshoot a WildFire Cluster

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Refer to the following topics to diagnose and troubleshoot WildFire cluster issues:

- [Troubleshoot WildFire Split-Brain Conditions](#)

Troubleshoot WildFire Split-Brain Conditions

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

A WildFire 2-node HA (high availability) cluster experiences a split-brain condition when a node (or both HA peers) believes the other is no longer operational. This occurs when both the HA and cluster connections fail as a result of network connectivity or configuration issues, but allows the appliances to continue processing samples. When this occurs both WildFire appliances assume the role of the active (or primary) controller without a backup, negating the benefits of a HA deployment, such as redundancy and load-balancing. Furthermore, this prevents the WildFire appliances from efficiently utilizing analysis resources. When WildFire clusters experience a minor disruption, it automatically attempts to recover from split-brain conditions. More serious events will require manual intervention.

When a split-brain occurs, the following conditions apply:

- Neither WildFire peer is aware of the state nor the HA role of the other.
- Both WildFire peers become the primary server and will continue to receive samples from firewalls, but operate as independent appliances.
- Cluster-related tasks are suspended when HA is not available.



3-node WildFire appliance clusters should not experience split-brain conditions when properly configured because of the additional redundancy provided by the third server node.

What Causes a Split-Brain Condition?

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

A split-brain condition is a corrective response to a single node failure of 2-node clusters, in which the WildFire high-availability pair is no longer able to communicate with each other, but still provides limited functionality. While high-availability and load-balancing functionality is no longer

available, you can still forward samples to WildFire for analysis. When a split-brain occurs, it is due to one of the following:

- Hardware issues or a power outage.
- Network connectivity issues, such as switch/router failures, network flapping, or a network partition.
- WildFire appliance configuration and connectivity issues.



Palo Alto Networks recommends using a direct cable connection for the HA1 and the cluster interface link.

- Unhealthy WildFire node.

Determine if the WildFire Cluster is in a Split-Brain Condition

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

When the appliances in a WildFire 2-node cluster enter a split-brain condition, the service failure(s) generate warnings in the WildFire CLI and managing Panorama (where available).

STEP 1 | (WildFire appliance CLI only) On a WildFire appliance controller, run:

```
admin@WF-500>show cluster membership
```

The affected WildFire cluster node displays `Cluster:splitbrain` next to `Service Summary`.

The following example shows a node in a 2-node WildFire cluster in a split-brain condition:

```
Service Summary: Cluster:splitbrain
Cluster name:    WF_Cluster_1
Address:         2.2.2.114
Host name:       wf1
Node name:       wfpc-009707000380-internal
Serial number:   009707000380
Node mode:       controller
Server role:     True
HA priority:     secondary
Last changed:    Tue, 24 Oct 2017 15:13:18 -0700
Services:        wfcore signature wfpc infra
Monitor status:
                 Serf Health Status: passing
                 Agent alive and reachable
                 Service 'infra' check: passing
Application status:
                 global-db-service: ReadyLeader
                 wildfire-apps-service: Ready
                 global-queue-service: ReadyLeader
                 wildfire-management-service: Done
                 siggen-db: ReadyMaster
```

```

Work queue status:
    sample analysis queued: 0
    sample analysis running: 0
    sample copy queued: 0
    sample copy running: 0

Diag report:
    2.2.2.114: reported leader '2.2.2.114', age 0.
    2.2.2.114: local node passed sanity check.
    
```

STEP 2 | (Panorama only) On the Panorama appliance that is managing the WildFire cluster:

1. Select **Panorama > Managed WildFire Clusters**.
2. In the **Cluster Status** column, check for the presence of **cluster [splitbrain]**. This indicates that the appliance is in split-brain mode.

APPLIANCE	SOFTWARE VERSION	IP ADDRESS	CONNECTED	CLUSTER NAME	ANALYSIS ENVIRONM...	CONTENT	ROLE	CONFIG STATUS	CLUSTER STATUS	LAST COMMIT STATE	UTILIZATION	FIREWALLS CONNECTED
wfcluster1 (2/3 Nodes Connected)												
qa19	10.0.2-c12		Connected	WF_Cluster1	vm-5	4033-4496	Controller		cluster [splitbrain]		View	View
qa18			Connected		vm-5		Controller Backup					
qa17	10.0.2-c12		Connected		vm-5	4033-4496	Worker					

Recover From a Split-Brain Condition

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

To resolve a split-brain condition, debug your network issues and then restore connectivity between the WildFire HA pair. WildFire appliance clusters automatically attempt to recover from split-brain conditions, but if those measures fail, you must manually initiate the recovery process.

STEP 1 | Verify that your network is operating normally and that the WildFire appliance is transmitting and receiving traffic.

1. Enable the ability to ping on a WildFire appliance interface.
 - Enable ping on a specific appliance interface— `setdeviceconfig system <interface_number> service disable-icmp no`
 - Enable ping on all appliance interfaces— `setdeviceconfig system service disable-icmp no`
2. Generate ping traffic from a WildFire interface to an external device. Verify that the received and transmitted counters increment.

```
ping source <wildfire-interface-ip> host<destination-ip-address>
```

STEP 2 | Determine which WildFire appliance is unhealthy. Refer to [View WildFire Cluster Status Using the CLI](#) or [View WildFire Cluster Status Using Panorama](#) to view the status of the appliance.

STEP 3 | Gracefully restart the *unhealthy* node using the following command:

request cluster reboot-local-node

The WildFire appliance that is rebooted should auto-enroll into the WildFire cluster it was configured for.



The remaining controller node that is in split-brain mode must be in a healthy state.

STEP 4 | Wait for the [Data Migration](#) to complete. Run `show cluster data-migration-status` to view the progress of the database merge. After the data merge is complete the completion timestamp displays:

```
100% completed on Mon Sep 9 21:44:48 PDT 2019
```



The duration of a data merge depends on the amount of data stored on the WildFire appliance. Be sure to allot at least several hours for recovery as the data merge can be a lengthy process.

STEP 5 | [Verify the status of the cluster](#) on Panorama or through the WildFire appliance CLI.

Use the WildFire Appliance CLI

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ▣ WildFire License

The following topics describe the CLI commands that are specific to the WildFire™ appliance software. All other commands, such as configuring interfaces, committing the configuration, and setting system information are identical to PAN-OS and are also shown in the hierarchy. For information on the PAN-OS commands, refer to the [PAN-OS CLI Quick Start](#).

- [WildFire Appliance Software CLI Concepts](#)
- [WildFire CLI Command Modes](#)
- [Access the WildFire Appliance CLI](#)
- [WildFire Appliance CLI Operations](#)
- [WildFire Appliance Configuration Mode Command Reference](#)
- [WildFire Appliance Operational Mode Command Reference](#)

WildFire Appliance Software CLI Concepts

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

This section introduces and describes how to use the WildFire appliance software command line interface (CLI):

- [WildFire Appliance Software CLI Structure](#)
- [WildFire Appliance Software CLI Command Conventions](#)
- [WildFire Appliance CLI Command Messages](#)
- [WildFire Appliance Command Option Symbols](#)
- [WildFire Appliance Privilege Levels](#)

WildFire Appliance Software CLI Structure

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The WildFire appliance software CLI is used to manage the appliance. The CLI is the only interface to the appliance. Use it to view status and configuration information and modify the appliance configuration. Access the WildFire appliance software CLI over SSH or by direct console access using the console port.

The WildFire appliance software CLI operates in two modes:

- **Operational mode**—View the state of the system, navigate the WildFire appliance software CLI, and enter configuration mode.
- **Configuration mode**—View and modify the configuration hierarchy.

WildFire Appliance Software CLI Command Conventions

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The basic command prompt incorporates the user name and hostname of the appliance:

```
username@hostname>
```

Example:

```
admin@WF-500>
```

When entering Configuration mode, the prompt changes from > to #:

```
username@hostname> (Operational mode)
username@hostname> configure
Entering configuration mode
[edit]
username@hostname# (Configuration mode)
```

In Configuration mode, the current hierarchy context is shown by the [edit...] banner presented in square brackets when a command is issued.

WildFire Appliance CLI Command Messages

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<input type="checkbox"/> WildFire License

Messages may be displayed when issuing a command. The messages provide context information and can help in correcting invalid commands. In the following examples, the message is shown in bold.

Example: Unknown command

```
username@hostname# application-group
Unknown command: application-group
[edit network]
username@hostname#
```

Example: Changing modes

```
username@hostname# exit
Exiting configuration mode
username@hostname>
```

Example: Invalid syntax

```
username@hostname> debug 17
Unrecognized command
Invalid syntax.
username@hostname>
```


The CLI checks the syntax of each command. If the syntax is correct, it executes the command and the candidate hierarchy changes are recorded. If the syntax is incorrect, an invalid syntax message is presented, as in the following example:

```
username@hostname# set deviceconfig setting wildfire cloud-
intelligence submit-sample yes
Unrecognized command
Invalid syntax.
[edit]
username@hostname#
```

WildFire Appliance Command Option Symbols

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The symbol preceding an option can provide additional information about command syntax.

Symbol	Description
*	This option is required.
>	There are additional nested options for this command.
+	There are additional command options for this command at this level.
	There is an option to specify an “except value” or a “match value” to restrict the command.
“ “	<p>Although the double quote is not a command option symbol, it must be used when entering multi-word phrases in CLI commands. For example, to create an address group named Test Group and to add the user named user1 to this group, you must surround the group name with double quotes as follows:</p> <pre>set address-group “Test Group” user1.</pre> <p>If you do not put a double quote surrounding the group name, the CLI would interpret the word Test as the group name and Group as the username and the following error would be displayed: testis not a valid name.</p> <p> <i>A single quote would also be invalid in this example.</i></p>

The following examples show how these symbols are used.

Example: In the following command, the keyword `from` is required:

```
username@hostname> scp import configuration ?
```

```

+ remote-port    SSH port number on remote host
* from          Source (username@host:path)
username@hostname> scp import configuration
Example: This command output shows options designated with + and >.
username@hostname# set rulebase security rules rule1 ?
+ action        action
+ application   application
+ destination   destination
+ disabled      disabled
+ from          from
+ log-end       log-end
+ log-setting   log-setting
+ log-start     log-start
+ negate-destination negate-destination
+ negate-source negate-source
+ schedule      schedule
+ service       service
+ source        source
+ to            to
> profiles      profiles
<Enter>        Finish input
[edit]
username@hostname# set rulebase security rules rule1

```

Each option listed with + can be added to the command.

The profiles keyword (with >) has additional options:

```

username@hostname# set rulebase security rules rule1 profiles ?
+ virus         Help string for virus
+ spyware       Help string for spyware
+ vulnerability Help string for vulnerability
+ group         Help string for group
<Enter>        Finish input
[edit]
username@hostname# set rulebase security rules rule1 profiles

```

WildFire Appliance Privilege Levels

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

Privilege levels determine which commands the user is permitted to execute and the information the user is permitted to view.

Level	Description
superreader	Has complete read-only access to the appliance.

Level	Description
superuser	Has complete read-write access to the appliance.

WildFire CLI Command Modes

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

The following topics describe the modes used to interact with the WildFire appliance software CLI:

- [WildFire Appliance CLI Configuration Mode](#)
- [WildFire Appliance CLI Operational Mode](#)

WildFire Appliance CLI Configuration Mode

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Entering commands in configuration mode modifies the candidate configuration. The modified candidate configuration is stored in the appliance memory and maintained while the appliance is running.

Each configuration command involves an action, and may also include keywords, options, and values.

This section describes Configuration mode and the configuration hierarchy:

- [Configuration Mode Command Usage](#)
- [Configuration Hierarchy](#)
- [Hierarchy Paths](#)
- [Navigate the Hierarchy](#)

Configuration Mode Command Usage

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

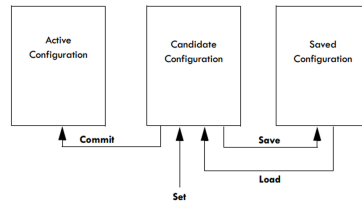
Use the following commands to store and apply configuration changes:

- **save**—Saves the candidate configuration in the non-volatile storage on the appliance. The saved configuration is retained until overwritten by subsequent **save** commands. Note that this command does not make the configuration active.
- **commit**—Applies the candidate configuration to the appliance. A committed configuration becomes the active configuration for the device.

- **set**—Changes a value in the candidate configuration.
- **load**—Assigns the last saved configuration or a specified configuration to be the candidate configuration.



When exiting configuration mode without issuing the **save** or **commit** command, the configuration changes could be lost if the appliance loses power.



Maintaining a candidate configuration and separating the save and commit steps confers important advantages when compared with traditional CLI architectures:

- Distinguishing between the save and commit concepts allows multiple changes to be made at the same time and reduces system vulnerability.
- Commands can easily be adapted for similar functions. For example, when configuring two Ethernet interfaces, each with a different IP address, you can edit the configuration for the first interface, copy the command, modify only the interface and IP address, and then apply the change to the second interface.
- The command structure is always consistent.

Because the candidate configuration is always unique, all authorized changes to the candidate configuration are consistent with each other.

Configuration Hierarchy

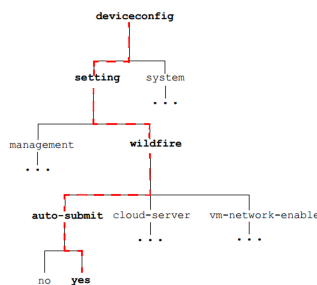
Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ❑ WildFire License

The configuration for the appliance is organized in a hierarchical structure. To display a segment of the current hierarchy level, use the `show` command. Entering `show` displays the complete hierarchy, while entering `show` with keywords displays a segment of the hierarchy. For example, when running the command `show` from the top level of configuration mode, the entire configuration is displayed. When running the command `edit mgt-config` and you enter `show`, or by running **`showmgt-config`**, only the `mgt-config` part of the hierarchy displays.

Hierarchy Paths

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ❑ WildFire License

When entering commands, the path is traced through the hierarchy as follows:

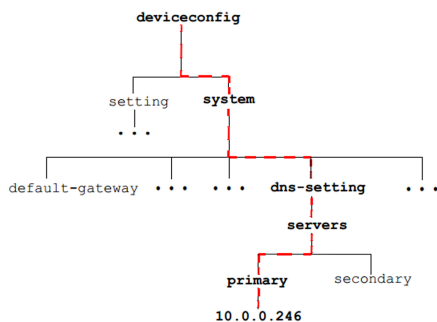


For example, the following command assigns the primary DNS server 10.0.0.246 for the appliance:

```
[edit]
username@hostname# set deviceconfig system dns-setting servers
primary 10.0.0.246
```

This command generates a new element in the hierarchy and in the output of the following show command:

```
[edit]
username@hostname# show deviceconfig system dns-settings
dns-setting {
  servers {
    primary 10.0.0.246
  }
}
[edit]
username@hostname#
```



Navigate the Hierarchy

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> ☐ WildFire License

The [edit...] banner presented below the Configure mode command prompt line shows the current hierarchy context.

```
[edit]
```

indicates that the relative context is the top level of the hierarchy, whereas

```
[edit deviceconfig]
```

indicates that the relative context is at the deviceconfig level.

Use the commands listed in to navigate through the configuration hierarchy.

Level	Description
edit	Sets the context for configuration within the command hierarchy.
up	Changes the context to the next higher level in the hierarchy.
top	Changes the context to the highest level in the hierarchy.



The **set** command issued after using the **up** and **top** commands starts from the new context.

WildFire Appliance CLI Operational Mode

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

At the initial login to the device, the WildFire appliance software CLI opens in Operational mode. Operational mode commands involve actions that are executed immediately. They do not involve changes to the configuration, and do not need to be saved or committed.

Operational mode commands are of several types:

- **Network access**—Open a window to another host. SSH is supported.
- **Monitoring and troubleshooting**—Perform diagnosis and analysis. Includes debug and ping commands.
- **Display commands**—Display or clear current information. Includes clear and show commands.
- **WildFire appliance software CLI navigation commands**—Enter Configure mode or exit the WildFire appliance software CLI. Includes configure, exit, and quit commands.
- **System commands**—Make system-level requests or restart. Includes set and request commands.

Access the WildFire Appliance CLI

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

This section describes how to access WildFire appliance software CLI:

- [Establish a Direct Console Connection](#)
- [Establish an SSH Connection](#)

Establish a Direct Console Connection

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Use the following settings for direct console connection:

- Data rate: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: None

Establish an SSH Connection

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

To access the WildFire appliance software CLI:

- STEP 1** | Use terminal emulation software to establish an SSH console connection with the WildFire appliance.
- STEP 2** | Enter the administrative user name. The default is admin.
- STEP 3** | Enter the administrative password. The default is admin.

The WildFire appliance software CLI opens in Operational mode, and the CLI prompt is displayed:

```
username@hostname>
```

WildFire Appliance CLI Operations

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

- [Access WildFire Appliance Operational and Configuration Modes](#)
- [Display WildFire Appliance Software CLI Command Options](#)
- [Restrict WildFire Appliance CLI Command Output](#)
- [Set the Output Format for WildFire Appliance Configuration Commands](#)

Access WildFire Appliance Operational and Configuration Modes

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

When logging in, the WildFire appliance software CLI opens in Operational mode. You can navigate between Operational and Configuration modes at any time.

- To enter Configuration mode from Operational mode, use the **configure** command:

```
username@hostname> configure
Entering configuration mode
[edit]
username@hostname#
```

- To leave Configuration mode and return to Operational mode, use the **quit** or **exit** command:

```
username@hostname# quit
Exiting configuration mode
username@hostname>
```

To enter an Operational mode command while in Configuration mode, use the **run** command. For example, to show system resources from configure mode, use **run show system resources**.

Display WildFire Appliance Software CLI Command Options

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

Use **?** (or Meta-H) to display a list of command options, based on context:

- To display a list of operational commands, enter ? at the command prompt.

```
username@hostname> ?
clear          Clear runtime parameters
  configure    Manipulate software configuration information
  create       create commands
  debug        Debug and diagnose
  delete        Remove files from hard disk
  disable       disable commands
  edit          edit commands
  exit          Exit this session
  find          Find CLI commands with keyword
  grep          Searches file for lines containing a pattern match
  less          Examine debug file content
  ping          Ping hosts and networks
  quit          Exit this session
  request       Make system-level requests
  scp           Use scp to import / export files
  set           Set operational parameters
  show          Show operational parameters
  ssh           Start a secure shell to another host
  submit        submit commands
  tail          Print the last 10 lines of debug file content
  telnet        Start a telnet session to another host
  test          verify system settings with test cases
  tftp          Use tftp to import / export files
  traceroute    Print the route packets take to network host
username@hostname>
```

- To display the available options for a specified command, enter the command followed by ?.

Example:

```
username@hostname> ping ?
+ bypass-routing  Bypass routing table, use specified interface
+ count           Number of requests to send (1..2000000000
  packets)
+ do-not-fragment Don't fragment echo request packets (IPv4)
+ interval         Delay between requests (seconds)
+ no-resolve       Don't attempt to print addresses symbolically
+ pattern          Hexadecimal fill pattern
+ size             Size of request packets (0..65468 bytes)
+ source           Source address of echo request
+ tos              IP type-of-service value (0..255)
+ ttl              IP time-to-live value (IPv6 hop-limit value)
  (0..255 hops)
+ verbose          Display detailed output
* host             Hostname or IP address of remote host
```

Restrict WildFire Appliance CLI Command Output

Some operational commands include an option to restrict the displayed output. To restrict the output, enter a pipe symbol followed by **except** or **match** and the value that is to be excluded or included:

Example:

The following sample output is for the show system info command:

```
username@hostname> show system info
hostname: WildFire
ip-address: 192.168.2.20
netmask: 255.255.255.0
default-gateway: 192.168.2.1
mac-address: 00:25:90:95:84:76
vm-interface-ip-address: 10.16.0.20
vm-interface-netmask: 255.255.252.0
vm-interface-default-gateway: 10.16.0.1
vm-interface-dns-server: 10.0.0.247
time: Mon Apr 15 13:31:39 2013
uptime: 0 days, 0:02:35
family: m
model: WF-500
serial: 009707000118
sw-version: 8.0.1
wf-content-version: 702-283
wf-content-release-date: unknown
logdb-version: 8.0.15
platform-family: m
operational-mode: normal
```

```
username@hostname>
```

The following sample displays only the system model information:

```
username@hostname> show system info | match model
model: WF-500
```

```
username@hostname>
```

Set the Output Format for WildFire Appliance Configuration Commands

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> WildFire Appliance 	<ul style="list-style-type: none"> WildFire License

Change the output format for the configuration commands by using the **set cli config-output-format** command in Operational mode. Options include the default format, JSON (JavaScript Object Notation), set format, and XML format. The default format is a hierarchal format where configuration sections are indented and enclosed in curly brackets.

WildFire Appliance Configuration Mode Command Reference

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none"> • WildFire Appliance 	<ul style="list-style-type: none"> □ WildFire License

This section contains command reference information for the following Configuration mode commands that are specific to the WildFire appliance software. All other commands that are part of the WildFire appliance software are identical to PAN-OS as described in the [PAN-OS 11.0 CLI Quick Start](#).

- [set deviceconfig cluster](#)
- [set deviceconfig high-availability](#)
- [set deviceconfig setting management](#)
- [set deviceconfig setting wildfire](#)
- [set deviceconfig system eth2](#)
- [set deviceconfig system eth3](#)
- [set deviceconfig system panorama local-panorama panorama-server](#)
- [set deviceconfig system panorama local-panorama panorama-server-2](#)
- [set deviceconfig system update-schedule](#)
- [set deviceconfig system vm-interface](#)

set deviceconfig cluster

Description

Configure Wildfire appliance cluster settings on the WildFire appliance. You can configure the cluster name, the interface used for cluster communication, and the mode (role) of the appliance in the cluster—controller or worker. On WildFire appliances that you configure as cluster controllers, you can add WildFire appliances to the cluster and set whether the controller provides DNS service on its management interface.

Hierarchy Location

```
set deviceconfig
```

Syntax

```
cluster {
  cluster-name <name>;
  interface {eth2 | eth3};
  mode {
```

```
controller {
  service-advertisement dns-service enabled {no | yes};
  worker-list {ip-address}
}
worker;
}
```

Options

+ `cluster-name` – Name the cluster. The name must be a valid domain name section.

+ `interface` – Configure the interface to use for cluster communication. The cluster communication interface must be the same on all cluster members.

> `mode` – Configure whether the WildFire appliance is a controller node or a worker node. For controller nodes, configure whether the controller provides DNS service on the management interface (`service-advertisement`) and add worker nodes to the cluster (`worker-list`). Each WildFire appliance cluster should have two controller nodes to provide high availability. You can add two controllers and up to 18 worker nodes to a cluster, for a maximum total of 20 nodes.

Sample Output

```
admin@wf-500(active-controller)# show deviceconfig cluster
cluster {
  cluster-name sid-6;
  interface eth2;
  mode {
    controller {
      worker-list {
        2.2.2.115;
      }
    }
  }
}
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig high-availability

Description

Configure Wildfire appliance cluster high-availability (HA) settings.

Hierarchy Location

```
set deviceconfig
```

Syntax

```

high-availability {
  enabled {no | yes};
  election-option {
    preemptive {no | yes};
    priority {primary | secondary};
    timers {
      advanced {heartbeat interval <value> | hello-interval <value> |
      preemption-hold-time <value> | promotion-hold-time <value>}
      aggressive;
      recommended;
    }
  }
}
interface {
  ha1 {
    peer-ip-address <ip-address>;
    port {eth2 | eth3 | management};
    encryption enabled {no | yes};
  }
  ha1-backup {
    peer-ip-address <ip-address>;
    port {eth2 | eth3 | management};
  }
}
}

```

Options

+ **enabled** – Enable HA on both controller nodes to provide fault tolerance for the cluster. Each WildFire appliance cluster should have two controller nodes configured as an HA pair.

> **election-option** – Configure the preemptive, priority, and timer HA option values.

+ **preemptive** – Election option to enable the passive HA peer (the controller backup node) to preempt the active HA peer (the primary controller node) based on the HA priority setting. For example, if the primary controller node goes down, the secondary (passive) controller node takes over cluster control. When the primary controller node comes back up, if you do not configure preemption, the secondary controller continues to control the cluster and the primary controller acts as the controller backup node. However, if you configure preemption on both HA peers, then when the primary controller comes back up, it preempts the secondary controller by taking back control of the cluster. The secondary controller resumes its former role as the controller backup node. You must configure the preemptive setting on both of the HA peers for preemption to work.

+ **priority** – Election option to configure the preemption priority of each controller in the HA pair. Configure preemption on both members of the HA controller pair.

> **timers** – Configure the timers for HA election options. The WildFire appliance provides two pre-configured timer options (**aggressive** and **recommended** settings), or you can configure each timer individually. The **Advanced** timers enable you to configure values individually:

- The **heartbeat-interval** sets the time in milliseconds to send heartbeat pings. The range of values is 1000-60,000 ms, with a default value of 2000 ms.

- The `hello-interval` sets the time in milliseconds to send Hello messages. The range of values is 8000-60,000 ms, with a default value of 8000 ms.
- The `preemption-hold-time` sets the time in minutes to remain in passive (controller backup) mode before preempting the active (primary) controller node. The range of values is 1-60 minutes, with a default value of 1 minute.
- The `promption-hold-time` sets the time in milliseconds to change state from passive (controller backup) to active (primary) state. The range of values is 0-60,000 ms, with a default value of 2000 ms.

> `interface` – Configure HA interface settings for the primary (`ha1`) and backup (`ha1-backup`) control link interfaces. The control link interfaces enable the HA controller pair to remain synchronized and prepared to failover in case the primary controller node goes down. Configuring both the `ha1` interface and the `ha1-backup` interface provides redundant connectivity between controllers in case of a link failure. Set:

- The `peer-ip-address`. For each interface, configure the IP address of the HA peer. The `ha1` interface peer is the `ha1` interface IP address on the other controller node in the HA pair. The `ha1-backup` interface peer is the `ha1-backup` interface IP address on the other controller node in the HA pair.
- The `port`. On each controller node, configure the port to use for the `ha1` interface and the port to use for the `ha-backup` interface. You can use `eth2`, `eth3`, or the management port (`eth0`) for the HA control link interfaces. You cannot use the Analysis Environment Network interface (`eth1`) as an `ha1` or `ha1-backup` control link interface. Use the same interface on both HA peers as the `ha1` interface, and use the same interface (but not the `ha1` interface) on both HA peers as the `ha1-backup` interface. For example, configure `eth3` as the `ha1` interface on both controller nodes and configure the management interface as the `ha1-backup` interface on both controller nodes.

Sample Output

```
admin@wf-500(active-controller)# show deviceconfig high-availability
high-availability {
election-option {
priority primary;
}
enabled no;
interface {
ha1 {
peer-ip-address 10.10.10.150;
port eth2
}
ha1-backup {
peer-ip-address 10.10.10.160;
port management
}
}
}
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig setting management

Description

Configure administrative management session settings on the WildFire appliance. You can configure timeouts to end administrative sessions if they are idle too long and how many login retries (failed login attempts) it takes to lock out an administrator.

Hierarchy Location

```
set deviceconfig setting
```

Syntax

```
management {  
  idle-timeout {0 | <value>}  
  admin-lockout {  
    failed-attempts <value>  
    lockout-time <value>  
  }  
}
```

Options

- + `idle-timeout` – Default administrative session idle timeout in minutes. Configure an idle timeout from 1-1440 minutes, or set the timeout value to 0 (zero) to never timeout the session.
- > `admin-lockout` – Configure the number of `failed-attempts` to login to the appliance before the administrator is locked out of the system (0-10), and the `lockout-time` in minutes (0-60) to lock out an administrator if the administrator crosses the `failed-attempts` threshold.

Sample Output

```
management {  
  idle-timeout 0;  
  admin-lockout {  
    failed-attempts 3;  
    lockout-time 5;  
  }  
}
```

set deviceconfig setting wildfire

Description

Configure Wildfire settings on the WildFire appliance. You can configure forwarding of malicious files, define the cloud server that receives malware infected files, and enable or disable the vm-interface.

Hierarchy Location

```
set deviceconfig setting
```

Syntax

```
wildfire {
  active-vm {vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | <value>};
  cloud-server <value>;
  custom-dns-name <value>;
  preferred-analysis-environment {Documents | Executables | default};
  vm-network-enable {no | yes};
  vm-network-use-tor {enable
  | disable};
  cloud-intelligence {
  cloud-query {no | yes};submit-diagnostics {no | yes};
  submit-report {no | yes};
  submit-sample {no | yes};
  }
  file-retention {
  malicious {indefinite | <1-2000>};
  non-malicious <1-90>
  }
  signature-generation {
  av {no | yes};
  dns {no | yes};
  url {no | yes};
  }
}
```

Options

- + **active-vm** – Select the virtual machine environment that WildFire will use for sample analysis. Each vm has a different configuration, such as Windows XP, a specific versions of Flash, Adobe reader, etc. To view which VM is selected, run the following command: **show wildfire status** and view the Selected VM field. To view the VM environment information, run the following command : **show wildfire vm-images**.
- + **cloud-server** – Hostname for the cloud server that the appliance will forward malicious samples/reports to for a re-analysis. The default cloud server is wildfire-public-cloud. To configure forwarding, use the following command: **set deviceconfig setting wildfire cloud-intelligence**.
- + **custom-dns-name** – Configure a custom DNS name to use in server certificates and the WildFire server list instead of the default DNS name wfpc.sevice.<clustername>.<domain>.
- + **preferred-analysis-environment** – Allocate the majority of the resources to document analysis or to executable analysis, depending on the type of samples most often analyzed in your environment. The default allocation balances resources between document and executable samples. For example, to allocate the majority of the analysis resources to documents: **set deviceconfig setting wildfire preferred-analysis-environment Documents**.

+ `vm-network-enable` – Enable or disable the vm-network. When enabled, sample files running in the virtual machine sandbox can access the Internet. This helps WildFire better analyze the behavior of the malware to look for things like phone home activity.

+ `vm-network-use-tor` – Enable or disable the Tor network for the vm-interface. When this option is enabled, any malicious traffic coming from the sandbox systems on the WildFire appliance during sample analysis is sent through the Tor network. The Tor network will mask your public facing IP address, so the owners of the malicious site cannot determine the source of the traffic.

> `cloud-intelligence` – Configure the appliance to submit WildFire diagnostics, reports or samples to the Palo Alto Networks WildFire cloud, or to automatically query the public WildFire cloud before performing local analysis to conserve WildFire appliance resources. The `submit-report` option sends reports for malicious samples to the cloud for statistical gathering. The `submit-sample` option sends malicious samples to the cloud. If `submit-sample` enabled, you don't need to enable `submit-report` because the cloud re-analyzes the sample and a new report and signature is generated if the sample is malicious.

> `file-retention` – Configure how long to save malicious (malware and phishing) samples and non-malicious (grayware and benign) samples. The default for malicious samples is indefinite (never delete). The default for non-malicious samples is 14 days. For example, to retain non-malicious samples for 30 days: **`set deviceconfig setting wildfire file-retention non-malicious 30`**.

> `signature-generation` – Enable the appliance to generate signatures locally, eliminating the need to send any data to the public cloud in order to block malicious content. The WildFire appliance will analyze files forwarded to it from Palo Alto Networks firewalls or from the WildFire API and generate antivirus and DNS signatures that block both the malicious files as well as associated command and control traffic. When the appliance detects a malicious URL, it sends the URL to PAN-DB and PAN-DB assigns it the malware category.

Sample Output

The following shows an example output of the WildFire settings.

```
admin@WF-500# show deviceconfig setting wildfire
wildfire {
signature-generation {
    av yes;
    dns yes;
    url yes;
}
cloud-intelligence {
submit-report no;
submit-sample yes;
submit-diagnostics yes;
cloud-query yes;
}
file-retention {
non-malicious 30;
malicious 1000;
{
active-vm vm-5;
cloud-server wildfire-public-cloud;
```

```
vm-network-enable yes;  
}
```

set deviceconfig system eth2

Description

Configure the eth2 interface.

Hierarchy Location

```
set deviceconfig system
```

Syntax

```
eth2 {  
  default-gateway <ip-address>;  
  ip-address <ip-address>;  
  mtu <value>;  
  netmask <ip-netmask>;  
  speed-duplex {100Mbps-full-duplex | 100Mbps-half-duplex | 10Mbps-  
  full-duplex | 10Mbps-half-duplex | 1Gbps-full-duplex | 1Gbps-half-  
  duplex | auto-negotiate};  
  permitted-ip <ip-address/netmask>;  
  service disable-icmp {no | yes};  
}
```

Options

- + `default-gateway` – IP address of the default gateway for the eth2 interface.
- + `ip-address` – IP address for the eth2 interface.
- + `mtu` – Maximum Transmission Unit (MTU) for the eth2 interface.
- + `netmask` – Netmask for the eth2 interface.
- + `speed-duplex` – Interface speed (10Mbps, 100Mbps, 1Gbps, or autonegotiate) and duplex mode (full or half) for the eth2 interface.
- > `permitted-ip` – IP addresses allowed to access the eth2 interface. If you specify a netmask with the IP address, the netmask must be in slash notation. For example, to specify a Class C address, enter: 10.10.10.100/24 (not 10.10.10.100 255.255.255.0).
- > `service-disable` – Disable ICMP for the eth2 interface.

Sample Output

```
admin@wf-500(active-controller)# show deviceconfig system eth2  
eth2 {  
  ip-address 10.10.10.120;  
  netmask 255.255.255.0;
```



```
service {
  disable-icmp no;
}
speed-duplex auto-negotiate;
mtu 1500;
}
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system eth3

Description

Configure the eth3 interface.

Hierarchy Location

```
set deviceconfig system
```

Syntax

```
eth3 {
  default-gateway <ip-address>;
  ip-address <ip-address>;
  mtu <value>;
  netmask <ip-netmask>;
  speed-duplex {100Mbps-full-duplex | 100Mbps-half-duplex | 10Mbps-
  full-duplex | 10Mbps-half-duplex | 1Gbps-full-duplex | 1Gbps-half-
  duplex | auto-negotiate};
  permitted-ip <ip-address/netmask>;
  service disable-icmp {no | yes};
}
```

Options

- + `default-gateway` – IP address of the default gateway for the eth3 interface.
- + `ip-address` – IP address for the eth3 interface.
- + `mtu` – Maximum Transmission Unit (MTU) for the eth3 interface.
- + `netmask` – Netmask for the eth3 interface.
- + `speed-duplex` – Interface speed (10Mbps, 100Mbps, 1Gbps, or autonegotiate) and duplex mode (full or half) for the eth3 interface.
- > `permitted-ip` – IP addresses allowed to access the eth3 interface. If you specify a netmask with the IP address, the netmask must be in slash notation. For example, to specify a Class C address, enter: 10.10.10.100/24 (not 10.10.10.100 255.255.255.0).
- > `service-disable` – Disable ICMP for the eth3 interface.

Sample Output

```
admin@wf-500(active-controller)# show deviceconfig system eth3
eth3 {
  ip-address 10.10.20.120;
  netmask 255.255.255.0;
  service {
    disable-icmp no;
  }
  speed-duplex auto-negotiate;
  mtu 1500;
}
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server

Description

Configure the primary Panorama server for managing the WildFire appliance or appliance cluster.

Hierarchy Location

```
set deviceconfig system panorama local-panorama
```

Syntax

```
panorama-server {IP address | FQDN};
```

Options

+ panorama-server – Configure the IP address or the fully qualified domain name (FQDN) of the primary Panorama server you will use to manage the WildFire appliance or appliance cluster.

Sample Output

The output is truncated to show only the output stanza that displays the Panorama server settings.

```
admin@wf-500(active-controller)# show deviceconfig system
system {
  panorama-server 10.10.10.100;
  panorama-server-2 10.10.10.110
  hostname myhost;
  ip-address 10.10.20.120;
  netmask 255.255.255.0;
  default-gateway 10.10.10.1;
```

```
update-server updates.paloaltonetworks.com;
service {
  disable-icmp no;
  disable-ssh no;
  disable-snmp yes;
}
...
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system panorama local-panorama panorama-server-2

Description

Configure the backup Panorama server for managing the WildFire appliance or appliance cluster. Configuring a backup Panorama server provides high availability for cluster or individual appliance management.

Hierarchy Location

```
set deviceconfig system panorama local-panorama
```

Syntax

```
panorama-server-2 {IP address | FQDN};
```

Options

+ panorama-server-2 – Configure the IP address or the fully qualified domain name (FQDN) of the backup Panorama server you will use to manage the WildFire appliance or appliance cluster.

Sample Output

The output is truncated to show only the output stanza that displays the Panorama server settings.

```
admin@wf-500(active-controller)# show deviceconfig system
system {
  panorama-server 10.10.10.100;
  panorama-server-2 10.10.10.110
  hostname myhost;
  ip-address 10.10.20.120;
  netmask 255.255.255.0;
  default-gateway 10.10.10.1;
  update-server updates.paloaltonetworks.com;
  service {
```

```
disable-icmp no;  
disable-ssh no;  
disable-snmp yes;  
}  
...
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system update-schedule

Description

Schedule content updates on a WildFire appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign.

Hierarchy Location

```
set deviceconfig system update-schedule
```

Syntax

```
wf-content recurring {  
  daily at <value> action {download-and-install | download-only};  
  weekly {  
    action {download-and-install | download-only};  
    at <value>;  
    day-of-week {friday | monday | saturday | sunday | thursday | tuesday  
    | wednesday};  
  }  
}
```

Options

- > wf-content – WildFire content updates.
- > daily – Schedule update every day.
- + action – Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
- + at – Time specification hh:mm (for example, 20:10).
- > hourly – Schedule update every hour.
- + action – Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
- + at – Minutes past the hour.
- > weekly – Schedule update once a week.

- + **action** – Specify the action to take. You can schedule the appliance to download and install the update or download only and then you install manually.
- + **at** – Time specification hh:mm (for example, 20:10).
- + **day-of-week** – Day of the week (Friday, Monday, Saturday, Sunday, Thursday, Tuesday, Wednesday).

Sample Output

```
admin@WF-500# show
update-schedule {
  wf-content {
    recurring {
      weekly {
        at 19:00;
        action download-and-install;
        day-of-week friday;
      }
    }
  }
}
```

Required Privilege Level

superuser, deviceadmin

set deviceconfig system vm-interface

Description

The vm-interface is used by malware running on the WildFire appliance virtual machine sandbox to access the Internet. Activating this port is recommended and will help WildFire better identify malicious activity if the malware accesses the Internet for phone-home or other activity. It is important that this interface has an isolated connection to the Internet. If your WildFire appliance is operating in FIPS/CC mode, the vm-interface is disabled. For more information, see [Set Up the WildFire Appliance VM Interface](#).

After configuring the vm-interface, enable it by running the following command:

```
set
deviceconfig setting wildfire vm-network-enable yes
```

Hierarchy Location

```
set deviceconfig system
```

Syntax

```
set vm-interface {
```

```
default-gateway <ip_address>;  
dns-server <ip_address>;  
ip-address <ip_address>;  
link-state;  
mtu;  
netmask <ip_address>;  
speed-duplex;  
{
```

Options

- + `default-gateway` – Default gateway for the VM interface.
- + `dns-server` – dns server for the VM interface.
- + `ip-address` – IP address for VM interface.
- + `link-state` – Set the link state to up or down.
- + `mtu` – Maximum Transmission Unit for the VM interface.
- + `netmask` – IP netmask for the VM interface.
- + `speed-duplex` – Speed and duplex for the VM interface.

Sample Output

The following shows a configured vm-interface.

```
vm-interface {  
ip-address 10.16.0.20;  
netmask 255.255.252.0;  
default-gateway 10.16.0.1;  
dns-server 10.0.0.246;  
}
```

Required Privilege Level

superuser, deviceadmin

WildFire Appliance Operational Mode Command Reference

Where Can I Use This?	What Do I Need?
<ul style="list-style-type: none">• WildFire Appliance	<ul style="list-style-type: none">□ WildFire License

This section contains command reference information for the following Operational mode commands that are specific to the WildFire appliance software. All other commands that are part of the WildFire appliance software are identical to PAN-OS; refer to the [PAN-OS 11.0 CLI Quick Start](#) for information on those commands.

- [clear high-availability](#)
- [create wildfire api-key](#)
- [delete high-availability-key](#)
- [delete wildfire api-key](#)
- [delete wildfire-metadata](#)
- [disable wildfire](#)
- [edit wildfire api-key](#)
- [load wildfire api-key](#)
- [request cluster decommission](#)
- [request cluster reboot-local-node](#)
- [request high-availability state](#)
- [request high-availability sync-to-remote](#)
- [request system raid](#)
- [request wildfire sample redistribution](#)
- [request system wildfire-vm-image](#)
- [request wf-content](#)
- [save wildfire api-key](#)
- [set wildfire portal-admin](#)
- [show cluster all-peers](#)
- [show cluster controller](#)
- [show cluster membership](#)
- [show cluster task](#)
- [show cluster data migration status](#)
- [show high-availability all](#)
- [show high-availability control-link](#)

- [show high-availability state](#)
- [show high-availability transitions](#)
- [show system raid](#)
- [show wildfire](#)
- [show wildfire global](#)
- [show wildfire local](#)
- [submit wildfire local-verdict-change](#)
- [test wildfire registration](#)

clear high-availability

Description

Clear high-availability (HA) control link statistics information and transitions statistics on the controller node of a WildFire appliance cluster.

Syntax

```
create {
  high-availability {
    control-link {
      statistics;
    }
    transitions;
  }
}
```

Options

> `control-link`> – Clear HA control-link statistics.

> `transitions`> – Clear HA transitions statistics (events that occur during HA switchovers).

Sample Output

After you clear control-link or transition statistics, the WildFire cluster resets all values to zero (0).

```
admin@wf-500(active-controller)> show high-availability control-link
statistics
High-Availability:
  Control Link Statistics:
    HA1:
      Messages-TX           : 0
      Messages-RX           : 0
      Capability-Msg-TX     : 0
      Capability-Msg-RX     : 0
      Error-Msg-TX          : 0
      Error-Msg-RX          : 0
      Preempt-Msg-TX        : 0
      Preempt-Msg-RX        : 0
```



```

Preempt-Ack-Msg-TX      : 0
Preempt-Ack-Msg-RX     : 0
Primary-Msg-TX         : 0
Primary-Msg-RX         : 0
Primary-Ack-Msg-TX     : 0
Primary-Ack-Msg-RX     : 0
Hello-Msg-TX           : 0
Hello-Msg-RX           : 0
Hello-Timeouts         : 0
Hello-Failures         : 0
MasterKey-Msg-TX       : 0
MasterKey-Msg-RX       : 0
MasterKey-Ack-Msg-TX   : 0
MasterKey-Ack-Msg-RX   : 0
Connection-Failures    : 0
Connection-Tries-Failures : 0
Connection-Listener-Tries : 0
Connection-Active-Tries : 0
Ping-TX                : 0
Ping-Fail-TX           : 0
Ping-RX                : 0
Ping-Timeouts          : 0
Ping-Failures          : 0
Ping-Error-Msgs       : 0
Ping-Other-Msgs       : 0
Ping-Last-Rsp         : 0

```

```
admin@wf-500(active-controller)> show high-availability transitions
```

```
High-Availability:
```

```
Transition Statistics:
```

```

Unknown      : 0
Suspended    : 0
Initial      : 0
Non-Functional : 0
Passive      : 0
Active       : 0

```

Required Privilege Level

superuser, deviceadmin

create wildfire api-key

Description

Generate API keys on a WildFire appliance that you will use on an external system to submit samples to the appliance, query reports, or retrieve samples and Packet Captures (PCAPS) from the appliance.

Syntax

```

create {
wildfire {
api-key {

```

```
key <value>;
name <value>;
{
}
{
}
```

Options

- + **key** – Create an API key by manually entering a key value. The value must be 64 alpha characters (a-z) or numbers (0-9). If you do not specify the key option, the appliance generates a key automatically.
- + **name** – Optionally enter a name for the API key. An API key name is simply used to label the keys to make it easier to identify keys assigned for specific uses and has no impact on the functionality of the key.

Sample Output

The following output shows that the appliance has three API keys and one key is named my-api-key.

```
admin@WF-500> show
wildfire global api-keys all
+-----+-----+-----+
|                                     |           |           |
|                                     |           |           |
|                                     |           |           |
|                                     |           |           |
|                                     |           |           |
+-----+-----+-----+
| Status | Create Time | Last Used Time |
+-----+-----+-----+
| Enabled | 2017-03-02 19:14:36 | 2017-03-02 19:14:36 |
| Enabled | 2016-02-06 12:13:22 | 2017-03-01 12:10:20 |
| Enabled | 2014-08-04 17:00:42 | 2017-03-01 11:12:52 |
+-----+-----+-----+
```

Required Privilege Level

superuser, deviceadmin

delete high-availability-key

Description

Delete the peer encryption key used for high-availability (HA) on the cluster control links of a WildFire appliance cluster's controller node.

Syntax

```
delete {
```

```
high-availability-key;  
}
```

Options

No additional options.

Sample Output

The highlighted line in the output shows that encryption isn't enabled on the HA control links.

```
admin@wf-500(active-controller)> show high-availability state  
High-Availability:  
  Local Information:  
    Version: 1  
    State: active-controller (last 1 days)  
  Device Information:  
    Management IPv4 Address: 10.10.10.14/24  
    Management IPv6 Address:  
  HA1 Control Links Joint Configuration:  
    Encryption Enabled: no  
  Election Option Information:  
    Priority: primary  
    Preemptive: no  
  Version Compatibility:  
    Software Version: Match  
    Application Content Compatibility: Match  
    Anti-Virus Compatibility: Match  
  Peer Information:  
    Connection status: up  
    Version: 1  
    State: passive-controller (last 1 days)  
    Device Information:  
      Management IPv4 Address: 10.10.20.112/24  
      Management IPv6 Address:  
      Connection up; Primary HA1 link  
    Election Option Information:  
      Priority: secondary  
      Preemptive: no  
  Configuration Synchronization:  
    Enabled: yes  
    Running Configuration: synchronized
```

Required Privilege Level

superuser, deviceadmin

delete wildfire api-key

Description

Delete an API key from the WildFire appliance. Systems configured to use the API to perform API functions on the appliance will no longer be able to access the appliance after you delete the key.

Syntax

```
delete {
wildfire {
api-key {
key <value>;
}
}
}
```

Options

+ key <value> – The key value for the key that you want to delete. To view a list of API keys, run the following command:

```
admin@WF-500> show
wildfire global api-keys all
```

Sample Output

```
admin@WF-500> delete
wildfire api-key key <API KEY>
APIKey <API Key> deleted
```

Required Privilege Level

superuser, deviceadmin

delete wildfire-metadata

Description

Delete content updates on the WildFire appliance. For more information on content updates and how to install them, see [request wf-content](#).

Syntax

```
delete {
wildfire-metadata update <value>;
}
```

Options

+ update <value> – Define the content update that you want to delete.

Sample Output

The output that follows shows the deletion of an update named:

```
panup-all-wfmeta-2-181.candidate.tgz.  
admin@WF-500> delete wildfire-metadata update panup-all-  
wfmeta-2-181.candidate.tgz  
successfully removed panup-all-wfmeta-2-181.candidate.tgz
```

Required Privilege Level

superuser, deviceadmin

disable wildfire

Description

Disables the domain signature or sample signature so that it is excluded from the next WildFire content package release.

Syntax

```
disable wildfire {  
  domain-signature {  
    domain <value>;  
  }  
  OR...  
  sample-signature {  
    sha256 {  
      equal <value>;  
    }  
  }  
}
```

Options

> **domain-signature**—Sets the status of the domain signature to disabled so that it is excluded from the next WildFire content release.

> **sample-signature**—Sets the status of the sample signature to disabled so that it is excluded from the next WildFire content release.

Sample Output

A successfully disabled sample or domain does not display any output.

```
admin@WF-500> disable wildfire sample-signature sha256 equal  
d1378bda0672de58d95f3bff3cb42385f2d806a4a15b89cdecfedbdbl1ec08228
```

Required Privilege Level

superuser, deviceadmin

edit wildfire api-key

Description

Modify an API key name or the key status (enabled/disabled) on a WildFire appliance.

Syntax

```
edit {
wildfire {
api-key [name | status] key <value>;
{
{
```

Options

- + name—Change the name of an API key.
- + status—Enable or disable an API key.
- * key—Specify the key to modify.

Sample Output

The key value in this command is required. For example, to change the name of a key named `stu` to `stu-key1`, enter the following command:



In the following command, you do not need to enter the old key name; only enter the new key name.

```
admin@WF-500> edit
wildfire api-key name stu-key1 key <API KEY>
To change the status of stu-key1 to disabled, enter the following
command:
admin@WF-500> edit wildfire api-key status disable key
<API KEY>
Example output that shows that stu-key1 is disabled:
admin@WF-500> show wildfire global api-keys all
+-----+-----+-----+-----+
|                                     |           |           |
|                                     |           |           |
|                                     |           |           |
|                                     |           |           |
+-----+-----+-----+-----+
| Status | Create Time | Last Used Time |
+-----+-----+-----+-----+
| Disabled | 2017-03-02 19:14:36 | 2017-03-02 19:14:36 |
+-----+-----+-----+-----+
```

Required Privilege Level

superuser, deviceadmin

load wildfire api-key

Description

After importing API keys to the WildFire appliance, you must use the load command to make the keys available for use. Use this command to replace all existing API keys, or you can merge the keys in the import file with the existing key database.

Syntax

```
load {
wildfire {
from <value> mode [merge | replace];
{
{
```

Options

* **from** – Specify the API key filename that you want to import. The key files use the .keys file extension. For example, my-api-keys.keys. To view a list of keys that are available for import, enter the following command:

```
admin@WF-500> load wildfire api-key from ?
```

+ **mode** – Optionally enter the mode for the import (merge/replace). For example, to replace the key database on the appliance with the contents of the contents of the new key file, enter the following command:

```
admin@WF-500> load wildfire api-key mode replace from my-api-
keys.keys
```

If you do not specify the **mode** option, the default action will merge the keys.

Required Privilege Level

superuser, deviceadmin

request cluster decommission

Description

Remove a WildFire appliance cluster node from a cluster that has three or more member nodes. Do not use this command to remove a node from a two-node cluster. Instead, [Remove a Node from a Cluster Locally](#) using the delete deviceconfig high-availability and delete deviceconfig cluster commands.

Hierarchy Location

request cluster

Syntax

```
request {
  cluster {
    decommission {
      show;
      start;
      stop;
    }
  }
}
```

Options

show—Display the status of the node decommission job.

start—Begin the node decommission job.

stop—Abort the node decommission job.

Sample Output

The Node mode field confirms that the cluster node decommission worked because the mode is stand_alone instead of controller or worker.

```
admin@wf-500> show cluster membership
Service Summary: wfpc signature
Cluster name:
Address:          10.10.10.86
Host name:        wf-500
Node name:        wfpc-009707000xxx-internal
Serial number:    009707000xxx
Node mode:     stand_alone
Server role:      True
HA priority:
Last changed:     Wed, 15 Feb 2017 00:05:11 -0800
Services:         wfcore signature wfpc infra
Monitor status:
                  Serf Health Status: passing
                  Agent alive and reachable
Application status:
wildfire-apps-service: Ready
global-db-service: ReadyStandalone
global-queue-service: ReadyStandalone
local-db-service: ReadyMaster
```

Required Privilege Level

superuser, deviceadmin

request cluster reboot-local-node

Description

Gracefully reboot the local WildFire cluster node.

Hierarchy Location

```
request cluster
```

Syntax

```
request {  
  cluster {  
    reboot-local-node;  
  }  
}
```

Options

No additional options.

Sample Output

You can verify that the local cluster node has rebooted or is in the process of rebooting in several ways:

- `show cluster task local`—display tasks requested on the local node.
- `show cluster task current`—display currently running tasks on the local node or the last completed task (**controller nodes only**).
- `show cluster task pending`—display tasks that are queued but have not run yet on the local node (**controller nodes only**).
- `show cluster task history`—display tasks that have been run on the local node (**controller nodes only**).

For example, the following command shows that two cluster node reboot tasks have completed successfully:

```
admin@qa15(passive-controller)> show cluster task history  
  
Request:          reboot from qa16 (009701000044/35533) at 2017-02-17  
                  19:21:53 UTC  
Response:         Reboot requested by admin  
                  permit by qa15 at 2017-02-17 22:11:31 UTC  
                  request not affecting healthy core server.  
Progress:         Wait for kv store ready for query...  
                  KV store is ready, wait for cluster leader  
                  available...  
                  Cluster leader is 2.2.2.16...  
                  Checking is sysd and clusterd are alive...
```

```

Checking if cluster-mgr is ready...
Checking global-db-cluster readiness...
Stopping global-queue server and leaving cluster...
Stopping global-db servers and doing failover...
rebooting...
Finished: success at 2017-02-17 22:17:56 UTC

Request: reboot from qa16 (009701000044/35535) at 2017-02-17
22:45:50 UTC

Response: Reboot requested by admin
permit by qa15 at 2017-02-17 23:06:44 UTC
request not affecting healthy core server.

Progress: Wait for kv store ready for query...
KV store is ready, wait for cluster leader
available...

Cluster leader is 2.2.2.15...
Checking if sysd and clusterd are alive...
Checking if cluster-mgr is ready...
Checking global-db-cluster readiness...
Stopping global-queue server and leaving cluster...
Stopping global-db servers and doing failover...
rebooting...
Finished: success at 2017-02-17 23:12:53 UTC

```

Required Privilege Level

superuser, deviceadmin

request high-availability state

Description

On a WildFire appliance cluster, make the high-availability (HA) state of the local controller node or of the peer controller node functional.

Hierarchy Location

```
request high-availability
```

Syntax

```

request {
  high-availability {
    state {
      functional;
    }
  }
  peer {
    functional;
  }
}

```

Options

- > `functional`—Make the HA state of the local controller node functional.
- > `peer`—Make the HA state of the peer controller node functional.

Sample Output

The highlighted lines in the output show that the HA state of the local controller node is functional in the active (primary) controller role and that the HA state of the peer controller node is functional in the passive (backup) controller role.

```
admin@wf-500(active-controller)> show high-availability state
High-Availability:
  Local Information:
    Version: 1
    State: active-controller (last 1 days)
    Device Information:
      Management IPv4 Address: 10.10.10.14/24
      Management IPv6 Address:
    HA1 Control Links Joint Configuration:
      Encryption Enabled: no
    Election Option Information:
      Priority: primary
      Preemptive: no
    Version Compatibility:
      Software Version: Match
      Application Content Compatibility: Match
      Anti-Virus Compatibility: Match
  Peer Information:
    Connection status: up
    Version: 1
    State: passive-controller (last 1 days)
    Device Information:
      Management IPv4 Address: 10.10.20.112/24
      Management IPv6 Address:
      Connection up; Primary HA1 link
    Election Option Information:
      Priority: secondary
      Preemptive: no
  Configuration Synchronization:
    Enabled: yes
    Running Configuration: synchronized
```

Required Privilege Level

superuser, deviceadmin

request high-availability sync-to-remote

Description

On a WildFire appliance cluster, synchronize the local controller node's candidate configuration or running configuration, or the local controller node's clock (time and date) to the remote high-availability (HA) peer controller node.

Hierarchy Location

request high-availability

Syntax

```
request {
  high-availability {
    sync-to-remote {
      candidate-config;
      clock;
      running-config;
    }
  }
}
```

Options

- > **candidate-config**—Synchronize the candidate configuration on the local peer controller node to the remote HA peer controller node.
- > **clock**—Synchronize the clock (time and date) on the local peer controller node to the remote HA peer controller node.
- > **running-config**—Synchronize the running configuration on the local peer controller node to the remote HA peer controller node.

Sample Output

The highlighted line in the output shows that the HA configuration state is synchronized on the HA peer controller node.

```
admin@wf-500(active-controller)> show high-availability state
High-Availability:
  Local Information:
    Version: 1
    State: active-controller (last 1 days)
  Device Information:
    Management IPv4 Address: 10.10.10.14/24
    Management IPv6 Address:
  HA1 Control Links Joint Configuration:
    Encryption Enabled: no
  Election Option Information:
    Priority: primary
    Preemptive: no
```

```

Version Compatibility:
  Software Version: Match
  Application Content Compatibility: Match
  Anti-Virus Compatibility: Match
Peer Information:
  Connection status: up
  Version: 1
  State: passive-controller (last 1 days)
Device Information:
  Management IPv4 Address: 10.10.20.112/24
  Management IPv6 Address:
  Connection up; Primary HA1 link
Election Option Information:
  Priority: secondary
  Preemptive: no
Configuration Synchronization:
  Enabled: yes
Running Configuration: synchronized

```

Required Privilege Level

superuser, deviceadmin

request system raid

Description

Use this option to manage the RAID pairs installed in the WildFire appliance. The WF-500 appliance ships with four drives in the first four drive bays (A1, A2, B1, B2). Drives A1 and A2 are a RAID 1 pair and drives B1 and B2 are a second RAID 1 pair.

Hierarchy Location

request system

Syntax

```

raid {
  remove <value>;
  OR...
  copy {
    from <value>;
    to <value>;
  }
  OR...
  add {

```

Options

- > add—Add a drive into the corresponding RAID Disk Pair
- > copy—Copy and migrate from one drive to other drive in the bay
- > remove—Drive to remove from RAID Disk Pair

Sample Output

The following output shows a WF-500 appliance with a correctly configured RAID.

```
admin@WF-500> show system raid
Disk Pair A                               Available
  Disk id A1                               Present
  Disk id A2                               Present
Disk Pair B                               Available
  Disk id B1                               Present
  Disk id B2                               Present
```

Required Privilege Level

superuser, deviceadmin

request wildfire sample redistribution

Description

Redistribute samples from the local WildFire appliance cluster node to another cluster node while optionally retaining samples on the local node.

Hierarchy Location

```
request system
```

Syntax

```
request {
wildfire {
sample {
redistribution {
  keep-local-copy {no | yes};
  serial-number <value>;
}
}
}
}
```

Options

- * `keep-local-copy`—Keep or do not keep a copy of the redistributed samples on the local WildFire appliance node.
- * `serial-number`—Serial number of the node to which you redistribute samples.

Sample Output

`Storage Nodes` displays the other node to which the local node redistributes samples. If the local node is not redistributing samples, only one storage node location displays. If the local node

is redistributing samples, Storage Nodes shows two storage node locations. The highlighted output shows the two storage nodes that store samples (the local node and the node to which the local node redistributes samples) and verifies that sample redistribution is occurring.

```

admin@WF-500> show wildfire global sample-analysis
Last Created 100 Malicious Samples
+-----+
+
+   SHA256      |   Finish Date   |   Create Date   |
+   Malicious  |                 |                  |
+-----+
+
+ <HASH VALUE> | 2017-03-24 17:27:40 | 2017-03-24 15:41:47 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:26:46 | 2017-03-24 15:41:45 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:26:54 | 2017-03-24 15:41:45 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:25:12 | 2017-03-24 15:41:44 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:24:28 | 2017-03-24 15:41:44 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:23:58 | 2017-03-24 15:41:44 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:26:52 | 2017-03-24 14:55:23 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:23:32 | 2017-03-24 14:55:23 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:24:58 | 2017-03-24 14:55:23 | Yes
+ |             |                   |                   |
+ <HASH VALUE> | 2017-03-24 17:22:02 | 2017-03-24 14:55:23 | Yes
+ |             |                   |                   |
+-----+
+
+-----+
+
+   Storage Nodes   | Analysis Nodes |   Status   |   File Type
+-----+
+
+ 0907:ld2_2,065:ld2_2 |   qa116   | Notify Finish | Java JAR
+ |
+ 0097:ld2_2,004:ld2_2 |   qa117   | Notify Finish | Java Class
+ |
+ 0524:ld2_2,006:ld2_2 |   qa117   | Notify Finish | Java Class
+ |
+ 0656:ld2_2,524:ld2_2 |   qa117   | Notify Finish | Java Class
+ |
+ 0024:ld2_2,056:ld2_2 |   qa117   | Notify Finish |   DLL
+ |
+ 0324:ld2_2,006:ld2_2 |   qa117   | Notify Finish | Java JAR
+ |
+ 0682:ld2_2,006:ld2_2 |   qa116   | Notify Finish | Java JAR
+ |

```

```

| 0092:ld2_2,016:ld2_2 | qa116 | Notify Finish | DLL
| 0682:ld2_2,002:ld2_2 | qa116 | Notify Finish | DLL
| 0056:ld2_2,824:ld2_2 | qa117 | Notify Finish | DLL
+-----+
*
lines 1-10

```

Required Privilege Level

superuser, deviceadmin

request system wildfire-vm-image

Perform upgrades on the WildFire appliance virtual machine (VM) sandbox images used to analyze files. To retrieve new VM images from the Palo Alto Networks Update Server, you must first download the image manually, host it on an SCP enabled server, and then retrieve the image from the appliance using the SCP client. After downloading the image to the appliance, you can then install it using this command.

Hierarchy Location

request system

Syntax

```

request {
  system {
    wildfire-vm-image {
      upgrade install file <value>;
    }
  }
}

```

Options

> wildfire-vm-image—Install Virtual Machine (VM) images.

+ upgrade install file—Perform an upgrade to the VM image. After the file option, type ? to view a list of available VM images. For example, run the following command to list available images:

```
admin@WF-500> request system wildfire-vm-image upgrade install file ?
```

Sample Output

To list available VM images, run the following command:

```
admin@WF-500> request system wildfire-vm-image upgrade install
file ?
```



```
To install a VM image (Windows 7 64-bit in this example), run the
following command:
admin@WF-500> request system wildfire-vm-image upgrade install file
WFWin7_64Base_m-1.0.0_64base
```

Required Privilege Level

superuser, deviceadmin

request wf-content

Perform content updates on a WildFire appliance. These content updates equip the appliance with the most up-to-date threat information for accurate malware detection and improve the appliance's ability to differentiate the malicious from the benign. To schedule content updates to install automatically, see [set deviceconfig system update-schedule](#) and to delete content updates on the WildFire appliance, see [delete wildfire-metadata](#).

Hierarchy Location

```
request
```

Syntax

```
request wf-content
{
  downgrade install {previous | <value>};
  upgrade
  {
    check
    download latest
    info
    install {
      file <filename>
      version latest;
    }
  }
}
```

Options

- > **downgrade** – Installs a previous content version. Use the previous option to install the previously installed content package or enter a value to downgrade to a specific content package number.
- > **upgrade** – Performs content upgrade functions
- > **check** – Obtain information on available content packages from the Palo Alto Networks Update Server
- > **download** – Download a content package
- > **info** – Show information about available content packages

- > `install` – Install a content package
- > `file` – Specify the name of the file containing the content package
- > `version` – Download or upgrade based on the version number of the content package

Sample Output

To list available content updates, run the following command:

```
admin@WF-500> request wf-content upgrade check
```

Version Installed	Size	Released on	Downloaded
2-217 current	58MB	2014/07/29 13:04:55 PDT	yes
2-188 previous	58MB	2014/07/01 13:04:48 PDT	yes
2-221 no	59MB	2014/08/02 13:04:55 PDT	no

Required Privilege Level

superuser, deviceadmin

save wildfire api-key

Description

Use the `save` command to save all API keys on the WildFire appliance to a file. You can then export the key file for backup purposes or to modify the keys in bulk. For details on using the WildFire API on a WildFire appliance, see the [WildFire API Reference](#).

Hierarchy Location

```
save
```

Syntax

```
save {  
  wildfire {  
    api-key to <value>;  
  }  
}
```

Options

* `to` – Enter the filename for key export. For example, to export all of the API keys on the WildFire appliance to a file named `my-wf-keys`, enter the following command:

```
admin@WF-500> save wildfire api-key to my-wf-keys
```

Required Privilege Level

superuser, deviceadmin

set wildfire portal-admin

Description

Sets the portal admin account password that an administrator will use to view WildFire analysis reports generated by a WildFire appliance. The account name (admin) and password is required when viewing the report on the firewall or from Panorama in **Monitor > WildFire Submissions > View WildFire Report**. The default username and password is admin/admin.



The portal admin account is the only account that you configure on the appliance to view reports from the firewall or Panorama. You cannot create new accounts or change the account name. This is not the same admin account used to manage the appliance.

Hierarchy Location

```
set wildfire
```

Syntax

```
set {
  wildfire {
    portal-admin {
      password <value>;
    }
  }
}
```

Sample Output

The following shows the output of this command.

```
admin@WF-500> set wildfire portal-admin password
Enter password:
Confirm password:
```

Required Privilege Level

superuser, deviceadmin

show cluster all-peers

Description

On a WildFire appliance cluster controller node, display the status of all WildFire appliance cluster members, including the WildFire appliance mode (controller or worker), connection status, and application service status.

Hierarchy Location

```
show cluster
```

Syntax

```
all-peers;
```

Options

No additional options.

Sample Output

```
admin@thing1(active-controller)> show cluster all-peers
Address          Mode          Server Node Name
-----
10.10.10.14     controller Self   True   thing1
  wfcore wfpc
  role applied
  09:12:01 -0800
  service: Ready
  JoinedCluster
  service: JoinedCluster
  ReadyMaster
  Service: infra signature
  Status: Connected, Server
  Changed: Wed, 15 Feb 2017
  WF App:
  wildfire-apps-
  global-db-service:
  global-queue-
  siggen-db:
10.10.10.112    controller Peer   True   thing2
  wfcore wfpc
  role applied
  09:13:00 -0800
  service: Ready
  Service: infra signature
  Status: Connected, Server
  Changed: Wed, 15 Feb 2017
  WF App:
  wildfire-apps-
```

```

ReadyLeader
service: ReadyLeader
ReadySlave
Diag report:
10.10.10.112: reported leader '10.10.10.112', age 0.
10.10.10.14: local node passed sanity check.
global-db-service:
global-queue-
siggen-db:

```

Required Privilege Level

superuser, deviceadmin

show cluster controller

Description

On a WildFire appliance cluster controller node, display the status of the WildFire appliance cluster controllers, including the cluster name and the role of the local controller node (if the Active Controller field displays True, the local controller is the primary controller, if the Active Controller field displays False, the local controller is the backup controller).

Hierarchy Location

```
show cluster
```

Syntax

```
controller;
```

Options

No additional options.

Sample Output

```

admin@thing1(active-controller)> show cluster controller
Cluster name:          satriani1
K/V API online:       True
Task processing:      on
Active Controller:    True
DNS Advertisement:
App Service DNS Name:
App Service Avail:    10.10.10.112, 10.10.10.14
Core Servers:
    009707000742:     10.10.10.112
    009701000043:     10.10.10.14
Good Core Servers:    2
Suspended Nodes:

```

```
Current Task:  
no tasks found
```

Required Privilege Level

superuser, deviceadmin

show cluster data migration status

Description

Use this command from a WildFire appliance cluster controller node to display the current data migration status. The command displays when data migration was initiated and it's progress. When data migration finishes the command displays the completion time stamp. If the data migration fails, the status will display 0% completed.

Hierarchy Location

```
show cluster
```

Syntax

```
data-migration-status;
```

Options

No additional options.

Sample Output

```
adminWF-500(active-controller)>  
  show  
  cluster data-migration-status  
  100% completed on Mon Sep 9 21:44:48 PDT 2019
```

Required Privilege Level

superuser, deviceadmin

show cluster membership

Description

Show WildFire appliance cluster membership information for the cluster node or standalone WildFire appliance, including the IP address, host name, WildFire appliance serial number, the appliance's role (Node mode), high-availability priority, and application status.

Hierarchy Location

```
show cluster
```

Syntax

```
membership;
```

Options

No additional options.

Sample Output

You can display cluster membership information for WildFire appliance cluster node members (controller and worker nodes) and standalone WildFire appliances to check whether they belong to a cluster, their application status, and other local host information. The output differs slightly depending on the WildFire appliance's role. The differences are:

- The prompt indicates the active (primary) controller node and the passive (backup) controller node, but does not indicate a worker node or standalone role.
- The `Node mode` indicates if the WildFire appliance is a `controller node`, a `worker node`, or a `stand_alone` WildFire appliance.
- `HA priority` displays `primary` for the active controller node, `secondary` for the passive (backup) controller node, and the field is blank for worker nodes and standalone WildFire appliances.
- `Application status` fields display different values in some fields. For `global-db-service` and `global-queue-service`, cluster members display `ReadyLeader` or `JoinedCluster`, and standalone appliances display `ReadyStandalone`.

For `siggen-db`, the primary controller node of the WildFire appliance cluster displays `ReadyMaster`, the secondary controller node of the WildFire appliance cluster displays `ReadySlave`, WildFire appliance cluster work nodes display `Ready`, and standalone WildFire appliances display `ReadyMaster`.



The last four digits of each WildFire appliance serial number is changed to "xxxx" in the displays to avoid revealing real serial numbers.

Output on the primary controller node in a WildFire appliance cluster:

```
admin@thing1(active-controller)> show cluster membership
Service Summary: wfpc signature
Cluster name:    satrian1
Address:        10.10.10.14
Host name:      thing1
Node name:      wfpc-00970100xxxx-internal
Serial number:  00970100xxxx
Node mode:      controller
Server role:    True
HA priority:    primary
```

```
Last changed: Wed, 15 Feb 2017 09:12:01 -0800
Services: wfcore signature wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable
Application status:
                wildfire-apps-service: Ready
                global-db-service: JoinedCluster
                global-queue-service: JoinedCluster
                siggen-db: ReadyMaster
```

Output on the controller backup node in a WildFire appliance cluster:

```
admin@thing2(passive-controller)> show cluster membership
Service Summary: wfpc signature
Cluster name: satrianil
Address: 10.10.10.112
Host name: thing2
Node name: wfpc-00970700xxxx-internal
Serial number: 009707000xxxx
Node mode: controller
Server role: True
HA priority: secondary
Last changed: Wed, 15 Feb 2017 09:13:10 -0800
Services: wfcore signature wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable
Application status:
                wildfire-apps-service: Ready
                global-db-service: ReadyLeader
                global-queue-service: ReadyLeader
                siggen-db: ReadySlave
```

Output on a worker node in a WildFire appliance cluster:

```
admin@grinch> show cluster membership
Service Summary: wfpc
Cluster name: satrianil
Address: 10.10.10.19
Host name: grinch
Node name: wfpc-00970100xxxx-internal
Serial number: 00970100xxxx
Node mode: worker
Server role: True
HA priority:
Last changed: Thu, 09 Feb 2017 15:55:55 -0800
Services: wfcore wfpc infra
Monitor status:
                Serf Health Status: passing
                Agent alive and reachable
Application status:
                wildfire-apps-service: Ready
                global-db-service: JoinedCluster
```



```
global-queue-service: JoinedCluster  
siggen-db: Ready
```

Output on a standalone WildFire appliance (not a WildFire appliance cluster member):

```
admin@max> show cluster membership  
Service Summary: wfpc signature  
Cluster name:  
Address: 10.10.10.90  
Host name: max  
Node name: wfpc-00970700xxxx-internal  
Serial number: 00970700xxxx  
Node mode: stand_alone  
Server role: True  
HA priority:  
Last changed: Mon, 13 Feb 2017 02:54:52 -0800  
Services: wfcore signature wfpc infra  
Monitor status:  
    Serf Health Status: passing  
    Agent alive and reachable  
Application status:  
wildfire-apps-service: Ready  
global-db-service: ReadyStandalone  
global-queue-service: ReadyStandalone  
siggen-db: ReadyMaster
```

Required Privilege Level

superuser, deviceadmin

show cluster task

Description

Show WildFire appliance cluster task information for the local cluster node or for all cluster nodes, or display the completed cluster task history or pending cluster tasks.

Hierarchy Location

```
show cluster
```

Syntax

```
task {  
current;  
history;  
local;  
pending;  
}
```

Options

- > **current**—Display tasks currently allowed on the WildFire appliance cluster. Available only on cluster controller nodes.
- > **history**—Display completed cluster tasks. Available only on cluster controller nodes.
- > **local**—Display pending tasks on the local WildFire appliance cluster node.
- > **pending**—Display pending tasks for the entire WildFire appliance cluster. Available only on cluster controller nodes.

Sample Output

```
admin@WF-500(active-controller)> show cluster task local
Request:      reboot from WF-500 (009701000034/74702) at 2017-02-21
03:06:45 UTC
Queued:       Reboot requested by admin
              by WF-500
              2/3 core servers available. reboot not allowed to
              maintain quorum

Request:      reboot from WF-500 (009701000034/74704) at 2017-02-21
03:10:27 UTC
Queued:       Reboot requested by admin
              by WF-500
              2/3 core servers available. reboot not allowed to
              maintain quorum

admin@WF-500(active-controller)> show cluster task current
no tasks found

admin@WF-500(active-controller)> show cluster task pending
Request:      reboot from WF-500 (009701000034/74702) at 2017-02-21
03:06:45 UTC
Queued:       Reboot requested by admin
              by WF-500
              2/3 core servers available. reboot not allowed to
              maintain quorum

Request:      reboot from WF-500 (009701000034/74704) at 2017-02-21
03:10:27 UTC
Queued:       Reboot requested by admin
              by WF-500
              2/3 core servers available. reboot not allowed to
              maintain quorum

admin@WF-500B(passive-controller)> show cluster task history
Request:      reboot from WF-500 (009701000044/35533) at 2017-02-17
19:21:53 UTC
Response:     Reboot requested by admin
              permit by WF-500B at 2017-02-17 22:11:31 UTC
              request not affecting healthy core server.
Progress:     Wait for kv store ready for query...
              KV store is ready, wait for cluster leader
              available...
```

```
Cluster leader is 10.10.10.100...
Checking is sysd and clusterd are alive...
Checking if cluster-mgr is ready...
Checking global-db-cluster readiness...
Stopping global-queue server and leaving cluster...
Stopping global-db servers and doing failover...
rebooting...
Finished:      success at 2017-02-17 22:17:56 UTC
```

Required Privilege Level

superuser, deviceadmin

show high-availability all

Description

Show all WildFire appliance cluster high-availability (HA) information, including HA control link, HA state, and HA transition information, peer software, content update, and antivirus compatibility information, and peer connection and role information.

Hierarchy Location

```
show high-availability
```

Syntax

```
all;
```

Options

No additional options.

Sample Output

```
admin@thing1(active-controller)> show high-availability all
High-Availability:
  Local Information:
    Version: 1
    State: active-controller (last 1 days)
  Device Information:
    Management IPv4 Address: 10.10.10.14/24
    Management IPv6 Address:
  HA1 Control Links Joint Configuration:
    Link Monitor Interval: 3000 ms
    Encryption Enabled: no
  HA1 Control Link Information:
    IP Address: 10.10.10.140/24
    MAC Address: 00:00:5e:00:53:ff
    Interface: eth3
    Link State: Up; Setting: 1Gb/s-full
```

```
Key Imported : no
Election Option Information:
  Priority: primary
  Preemptive: no
  Promotion Hold Interval: 2000 ms
  Hello Message Interval: 8000 ms
  Heartbeat Ping Interval: 2000 ms
  Preemption Hold Interval: 1 min
  Monitor Fail Hold Up Interval: 0 ms
  Addon Master Hold Up Interval: 500 ms
Version Information:
  Build Release: 8.0.1-c31
  URL Database: Not Installed
  Application Content: 497-2688
  Anti-Virus: 0
Version Compatibility:
  Software Version: Match
  Application Content Compatibility: Match
  Anti-Virus Compatibility: Match
Peer Information:
  Connection status: up
  Version: 1
  State: passive-controller (last 1 days)
  Device Information:
    Management IPv4 Address: 10.10.10.30/24
    Management IPv6 Address:
  HA1 Control Link Information:
    IP Address: 10.10.10.130
    MAC Address: 00:00:5e:00:53:00
    Connection up; Primary HA1 link
  Election Option Information:
    Priority: secondary
    Preemptive: no
  Version Information:
    Build Release: 8.0.1-c31
    URL Database: Not Installed
    Application Content: 497-2688
    Anti-Virus: 0
Initial Monitor Hold inactive; Allow Network/Links to Settle:
  Link and path monitoring failures honored
Configuration Synchronization:
  Enabled: yes
  Running Configuration: synchronized
```

Required Privilege Level

superuser, deviceadmin

show high-availability control-link

Description

Show WildFire appliance cluster high-availability (HA) statistics for the HA control link between the primary and backup controller nodes, including the number of different types of messages transmitted and received on the HA control link, connection failures, and ping activity.

Hierarchy Location

```
show high-availability
```

Syntax

```
control-link {  
  statistics;  
}
```

Options

> **statistics**—Display WildFire appliance cluster controller node HA control-link statistics.

Sample Output

```
admin@thing1(active-controller)> show high-availability control-link  
statistics  
High-Availability:  
  Control Link Statistics:  
    HA1:  
      Messages-TX           : 13408  
      Messages-RX           : 13408  
      Capability-Msg-TX      : 2  
      Capability-Msg-RX      : 2  
      Error-Msg-TX           : 0  
      Error-Msg-RX           : 0  
      Preempt-Msg-TX         : 0  
      Preempt-Msg-RX         : 0  
      Preempt-Ack-Msg-TX     : 0  
      Preempt-Ack-Msg-RX     : 0  
      Primary-Msg-TX         : 1  
      Primary-Msg-RX         : 1  
      Primary-Ack-Msg-TX     : 1  
      Primary-Ack-Msg-RX     : 1  
      Hello-Msg-TX           : 13402  
      Hello-Msg-RX           : 13402  
      Hello-Timeouts         : 0  
      Hello-Failures         : 0  
      MasterKey-Msg-TX       : 1  
      MasterKey-Msg-RX       : 1  
      MasterKey-Ack-Msg-TX   : 1  
      MasterKey-Ack-Msg-RX   : 1  
      Connection-Failures    : 0  
      Connection-Tries-Failures : 12  
      Connection-Listener-Tries : 1  
      Connection-Active-Tries : 12  
      Ping-TX                : 53614  
      Ping-Fail-TX           : 0  
      Ping-RX                : 53613  
      Ping-Timeouts          : 0  
      Ping-Failures          : 0  
      Ping-Error-Msgs        : 0
```

```
Ping-Other-Msgs      : 0
Ping-Last-Rsp       : 1
```

Required Privilege Level

superuser, deviceadmin

show high-availability state

Description

Show WildFire appliance cluster high-availability (HA) state information for the local and peer cluster controller nodes, including whether the controller node is active (primary) or passive (backup) and how long the controller node has been in that state, the HA configuration, whether the local and peer controller node configurations are synchronized, and software, content update, and antivirus version compatibility between controller node peers.

Hierarchy Location

```
show high-availability
```

Syntax

```
state;
```

Options

No additional options.

Sample Output

```
admin@thing1(active-controller)> show high-availability state
High-Availability:
  Local Information:
    Version: 1
    State: active-controller (last 1 days)
  Device Information:
    Management IPv4 Address: 10.10.10.14/24
    Management IPv6 Address:
  HA1 Control Links Joint Configuration:
    Encryption Enabled: no
  Election Option Information:
    Priority: primary
    Preemptive: no
  Version Compatibility:
    Software Version: Match
    Application Content Compatibility: Match
    Anti-Virus Compatibility: Match
  Peer Information:
    Connection status: up
    Version: 1
```

```
State: passive-controller (last 1 days)
Device Information:
  Management IPv4 Address: 10.10.10.30/24
  Management IPv6 Address:
  Connection up; Primary HA1 link
Election Option Information:
  Priority: secondary
  Preemptive: no
Configuration Synchronization:
  Enabled: yes
  Running Configuration: synchronized
```

Required Privilege Level

superuser, deviceadmin

show high-availability transitions

Description

Show WildFire appliance cluster high-availability (HA) transition information about events that occur during HA switchovers for the cluster controller nodes.

Hierarchy Location

```
show high-availability
```

Syntax

```
transitions;
```

Options

No additional options.

Sample Output

```
admin@thing1(active-controller)> show high-availability transitions
High-Availability:
  Transition Statistics:
    Unknown           : 1
    Suspended         : 0
    Initial           : 0
    Non-Functional    : 0
    Passive           : 0
    Active            : 3
```

Required Privilege Level

superuser, deviceadmin

show system raid

Description

Show the RAID configuration of the WildFire appliance. The WF-500 appliance ships with four drives in the first four drive bays (A1, A2, B1, B2). Drives A1 and A2 are a RAID 1 pair and drives B1 and B2 are a second RAID 1 pair.

Hierarchy Location

```
show system
```

Syntax

```
raid {  
    detail;  
}
```

Options

No additional options.

Sample Output

The following shows the RAID configuration on a functioning WF-500 appliance.

```
admin@WF-500> show system raid detail  
Disk Pair A                               Available  
Status                                   clean  
Disk id A1                               Present  
  model      : ST91000640NS  
  size       : 953869 MB  
  partition_1 : active sync  
  partition_2 : active sync  
Disk id A2                               Present  
  model      : ST91000640NS  
  size       : 953869 MB  
  partition_1 : active sync  
  partition_2 : active sync  
Disk Pair B                               Available  
Status                                   clean  
Disk id B1                               Present  
  model      : ST91000640NS  
  size       : 953869 MB  
  partition_1 : active sync  
  partition_2 : active sync  
Disk id B2                               Present  
  model      : ST91000640NS  
  size       : 953869 MB  
  partition_1 : active sync  
  partition_2 : active sync
```


Required Privilege Level

superuser, superreader

submit wildfire local-verdict-change

Description

Changes locally generated WildFire verdicts for samples submitted from the Firewall. Verdict changes apply only to those samples submitted to the WildFire appliance, and the verdict for the same sample remains unchanged in the WildFire public cloud. You can view samples with changed verdicts using the [show wildfire global](#) command.

The [WildFire private cloud content package](#) is updated to reflect any verdict changes that you make (on the firewall, select **Device > Dynamic Updates > WF-Private** to enable WildFire private cloud content updates). When you change a sample verdict to malicious, the WildFire appliance generates a new signature to detect the malware and adds that signature to the WildFire private cloud content package. When you change a sample verdict to benign, the WildFire appliance removes the signature from the WildFire private cloud content package.

There is also an API call which can be used to change the verdicts of local samples. Refer to the [WildFire API Reference](#) for more information.

Hierarchy Location

```
submit wildfire
```

Syntax

```
submit {
  wildfire {
    local-verdict-change {
      hash <value>;
      verdict <value>;
      comment <value>;
    }
  }
}
```

Options

- * **hash** – Specify the SHA-256 hash of the file for which you want change the verdict.
- * **verdict** – Enter the new file verdict: 0 indicates a benign sample; 1 indicates malware; 2 indicates grayware.
- * **comment** – Include a comment to describe the verdict change.

Sample Output

The following shows the output of this command.

```
admin@WF-500> submit wildfire local-verdict-change comment test hash
c323891a87a8c43780b0f2377de2efc8bf856f02dd6b9e46e97f4a9652814b5c
verdict 2
Please enter 'Y' to commit: (y or n)
verdict is changed (old verdict: 1, new verdict:2)
```

Required Privilege Level

superuser, deviceadmin

show wildfire

Description

Shows various information about the WildFire appliance, such global and local device and sample-related details, appliance status, , and the virtual machine that is selected to perform analysis.

Hierarchy Location

```
show wildfire
```

Syntax

```
status | vm-images | wf-vm-pe-utilization | wf-vm-doc-utilization
| wf-vm-email-link-utilization | wf-vm-archive-utilization | wf-
sample-queue-status
}
```

Options

- > **status** – Display the status of the appliance as well as configuration information such as the Virtual Machine (VM) used for sample analysis, whether or not samples/reports are sent to the cloud, vm network, and registration information.
- > **vm-images** – Display the attributes of the available virtual machine images used for sample analysis. To view the current active image, run the following command:

```
admin@WF-500>
show wildfire status
```

and view the VM field.

- > **wf-sample-queue-status** – Displays the number and breakdown of WildFire appliance samples that are waiting to be analyzed.
- > **wf-vm-doc-utilization** – Displays how many analysis environments used to process document files are available and are in use.
- > **wf-vm-elinkda-utilization** – Displays how many analysis environments used to process email links are available and are in use.

> wf-vm-pe-utilization – Displays how many analysis environments used to process portable executable files are available and are in use.

Sample Output

The following shows the output for this command.

```
admin@WF-500>
show
  wildfire status
Connection info:
Wildfire cloud:      s1.wildfire.paloaltonetworks.com
Status:              Idle
Submit sample:       disabled
Submit report:       disabled
Selected VM:         vm-5
VM internet connection: disabled
VM network using Tor: disabled
Best server:         s1.wildfire.paloaltonetworks.com
Device registered:   yes
Service route IP address: 10.3.4.99
Signature verification: enable
Server selection:    enable
Through a proxy:     no

admin@WF-500>
show wildfire vm-images

Supported VM images:
vm-1
Windows XP, Adobe Reader 9.3.3, Flash 9, Office 2003. Support PE,
PDF, Office 2003 and earlier
vm-2
Windows XP, Adobe Reader 9.4.0, Flash 10n, Office 2007. Support
PE, PDF, Office 2007 and earlier
vm-3
Windows XP, Adobe Reader 11, Flash 11, Office 2010. Support PE,
PDF, Office 2010 and earlier
vm-4
Windows 7 32bit, Adobe Reader 11, Flash 11, Office 2010. Support
PE, PDF, Office 2010 and earlier
vm-5
Windows 7 64bit, Adobe Reader 11, Flash 11, Office 2010. Support
PE, PDF, Office 2010 and earlier
vm-6
Windows XP, Internet Explorer 8, Flash 11. Support E-MAIL Links

admin@WF-500>
show wildfire wf-sample-queue-status
DW-ARCHIVE: 4,
DW-DOC: 2,
DW-ELINK: 0,
DW-PE: 21,
DW-URL_UPLOAD_FILE: 2,

admin@WF-500>
```

```
show wildfire wf-vm-pe-utilization
{
  available: 2,
  in_use: 1,
}
```

Required Privilege Level

superuser, superreader

show wildfire global

Description

Shows various information about global devices and the status of samples, such as available API keys, registration information, sample verdict changes, activity, sample device origin, and recent samples that the appliance analyzed.

Hierarchy Location

```
show wildfire global
```

Syntax

```
api-keys {
  all {
    details;
  }
  key <value>;
}
devices-reporting-data;
last-device-registration {
  all;
}
local-verdict-change {
  all;
  sha256 <value>;
}
}
sample-analysis {
  number;
  type;
}
}
sample-device-lookup {
  sha256 {
    equal <value>;
  }
}
sample-status {
  sha256 {
    equal <value>;
```

```

}
}
signature-status {
sha256 {
equal <value>;
}
}
}

```

Options

- > **api-keys** – Show details about the API keys generated on the WildFire appliance. You can view the last time the key was used, the key name, status (Enabled or Disabled), and the date/time the key was generated.
- > **devices-reporting-data** – Show list of latest registration activities.
- > **last-device-registration** – Show list of latest registration activities.
- > **local-verdict-change** – Shows samples with changed verdicts.
- > **sample-analysis** – Show wildfire analysis results for up to a maximum of 1,000 samples.
- > **sample-status** – Show wildfire sample status. Enter the SHA256 value of the file to view the current analysis status.
- > **sample-device-lookup** – Shows the firewall that sent the specified SHA256 sample.
- > **signature-status** – Show wildfire signature status. Enter the SHA256 value of the file to view the current analysis status.

Sample Output

The following shows the output for this command.

```

admin@WF-500>
show wildfire global api-keys all
+-----+-----+-----+-----+
|  Apikey  | Name      | Status | Create Time      |
| Last Used Time |          |        |                   |
+-----+-----+-----+-----+
| <API KEY> | happykey1 | Enabled | 2017-03-01 23:21:02 |
| 2017-03-01 23:21:02 |          |        |                   |
+-----+-----+-----+-----+

```

```

admin@WF-500>
show wildfire global devices-reporting-data
+-----+-----+-----+-----+
| Device ID | Last Registered | Device IP | SW Version |
| HW Model | Status          |           |            |
+-----+-----+-----+-----+
| 000000000000 | 2017-03-01 22:28:25 | 10.1.1.1 | 8.1.4 |
| PA-220 | OK              |           |            |

```

```

+-----+-----+-----+-----+
+-----+-----+
admin@WF-500>
show wildfire global last-device-registration
all
+-----+-----+-----+-----+
| Device ID      | Last Registered      | Device IP  | SW Version |
HW Model | Status |
+-----+-----+-----+-----+
| 000000000000  | 2017-07-31 12:35:53 | 10.1.1.1   | 8.1.4     |
PA-220   | OK    |
+-----+-----+-----+-----+
+-----+-----+

admin@WF-500> show wildfire global local-verdict-change

+-----+-----+-----+-----+
|                               | SHA256
| Verdict | Source |
+-----+-----+-----+-----+
|                               |
c883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496| 2
-> 1 | Yes |
+-----+-----+-----+-----+
+-----+-----+

admin@WF-500>
show wildfire global sample-analysis

Last Created 100 Malicious Samples
+-----+-----+-----+-----+
| SHA256          | Finish Date      | Create Date  |
Malicious |
+-----+-----+-----+-----+
| <HASH VALUE>  | 2017-03-01 23:27:57 | 2017-03-01 23:27:57 |
Yes      |
+-----+-----+-----+-----+
+-----+-----+
+-----+-----+-----+-----+
| Storage Nodes  | Analysis Nodes  | Status      | File
Type |
+-----+-----+-----+-----+
| 00926ld1_2,0094:d1_2 | qa16          | Notify Finish | Elink
File |

```



```

+-----+-----+-----+
+-----+
| 2017-03-01 22:34:17 | 2017-03-01 22:28:23 | No |
009026:smp_27,097010smp_27 |
+-----+-----+-----+
+-----+

+-----+-----+-----+
| Analysis Nodes | Status | File Type |
+-----+-----+-----+
| qa15 | Notify Finish | Adobe Flash File |
+-----+-----+-----+

admin@WF-500>
show wildfire global signature-status sha256

equalc883b5d2e16d22b09b176ca0786128f8064d47edf26186b95845aa3678868496
Signature Name: Virus/Win32.WPCGeneric.cr
Current Status: released
Release History:
+-----+-----+-----+
+-----+
| Build Version | Timestamp | UTID | Internal ID |
Status |
+-----+-----+-----+
+-----+
| 155392 | 2017-02-03 10:11:06 | 5000259 | 10411 |
released |
+-----+-----+-----+
+-----+

```

Required Privilege Level

superuser, superreader

show wildfire local

Description

Shows various information about local devices and samples, activity, recent samples that the appliance analyzed, and basic WildFire statistics.

Hierarchy Location

```
show wildfire local
```

Syntax

```
latest {
  analysis {
    filter malicious|benign;
```



```

Status;      sort-by SHA256|Submit Time|Start Time|Finish Time|Malicious|
              sort-direction asc|desc;
              limit 1-20000;
              days 1-7;
            }
            OR...
samples {
  filter malicious|benign;
  sort-by SHA256|Create Time|File Name|File Type|File Size|
Malicious|Status;
  sort-direction asc|desc;
  limit 1-20000;
  days 1-7;
}
sample-processed {
  count 1-1000;
  time {last-1-hr|last-12-hrs|last-15-minutes|last-24-hrs|
last-30-days|last-7-days|last-calender-day|last-calender-month;
}
sample-status {
  sha256 {
    equal <value>;
  }
}
statistics days <1-31> | hours <0-24> | minutes <0-60>;
}

```

Options

> **latest** – Show latest 30 activities, which include the last 30 analysis activities, the last 30 files that were analyzed, network session information on files that were analyzed and files that were uploaded to the public cloud server.

> **sample-processed** – Shows the number of samples processed locally within a specified timespan or maximum number of samples.

> **sample-status** – Show wildfire sample status. Enter the SHA256 value of the file to view the current analysis status.

> **statistics** – Display basic wildfire statistics.

Sample Output

The following shows the output for this command.

```

admin@WF-500> show
wildfire latest analysis
Latest analysis information:
+-----+-----+-----+-----+
+-----+
| SHA256      | Submit Time      | Start Time      | Finish
| Time        |                  |                 |
+-----+-----+-----+-----+
+-----+

```

```

| <HASH VALUE>| 2017-03-01 14:28:26 | 2017-03-01 14:28:26 |
2017-03-01 14:34:24 |
| <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 |
2017-03-01 14:28:41 |
| <HASH VALUE>| 2017-03-01 14:28:25 | 2017-03-01 14:28:25 |
2017-03-01 14:28:26 |
+-----+-----+-----+
+-----+
+-----+
+-----+
| Malicious   | VM Image
|   Status    |
+-----+
+-----+
+-----+
| Yes         | Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office
2010 | completed |
| No          | Java/Jar Static Analyzer
      | completed |
| Suspicious  | Java/Jar Static Analyzer
      | completed |
+-----+
+-----+
+-----+

```

admin@WF-500> **show wildfire local latest samples**

Latest samples information:

```

+-----+-----+-----+
+-----+
| SHA256      | Create Time          | File Name      | File Type
|
+-----+-----+-----+
+-----+
| <HASH VALUE>| 2017-03-01 14:28:25 |                | JAVA Class
|
| <HASH VALUE>| 2017-03-01 14:28:25 |                | JAVA Class
|
| <HASH VALUE>| 2017-03-01 14:28:25 |                | PE
|
+-----+-----+-----+
+-----+

```

```

+-----+-----+-----+
| File Size   | Malicious | Status
+-----+-----+-----+
|           20,407 | No        | analysis complete
|           1,584 | Yes       | analysis complete
|          259,024 | No        | analysis complete
+-----+-----+-----+

```

admin@WF-500> **show wildfire local sample-processed count**
2

Time Window: last-15-minutes
Display Count: 2:

```

+-----+
+-----+-----+-----+-----+
+-----+-----+
|                               SHA256                               |
| Create Time      | File Name | File Type | File Size | Malicious |
| Status          |          |          |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ce752b7b76ac2012bdf2b76b6c6af18e132ae8113172028b9e02c6647ee19bb |
| 2018-12-09 16:55:53 |          | Email Link | 31,522 |          |
| download complete |          |          |          |          |
| 349e57e51e7407abcd6eccda81c8015298ff5d5ba4cedf09c7353c133ceaa74b |
| 2018-12-09 16:53:40 |          | Email Link | 39,679 |          |
| download complete |          |          |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+
admin@WF-500> show wildfire local sample-status sha256
equal
0f2114010d00d7fa453177de93abca9643f4660457536114898c56149f819a9b

Sample information:
+-----+-----+
+-----+-----+
| Create Time      | File Name | File Type
|
+-----+-----+
+-----+-----+
| 2017-03-01 22:28:24 | rmr.doc | Microsoft Word 97 - 2003 Document
|
+-----+-----+
+-----+-----+
| File Size | Malicious | Status
+-----+-----+
| 133120 | Yes | analysis complete
+-----+-----+
Analysis information:
+-----+-----+
+-----+-----+
| Submit Time      | Start Time | Finish Time |
| Malicious |
+-----+-----+
+-----+-----+
| 2017-03-01 22:28:24 | 2017-03-01 22:28:24 | 2017-03-01 22:28:24 |
| Suspicious |
| 2017-03-01 22:28:24 | 2017-03-01 22:28:24 | 2017-03-01 22:34:07 |
| Yes |
+-----+-----+
+-----+-----+
+-----+-----+
|                               VM Image                               |
| Status |

```



```

|| FileType | Submitted | Analyzed | Pending | Malware | Grayware |
Benign | Error ||
+-----+-----+-----+-----+-----+-----+
|| pdf | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| jar | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| doc | 1 | 1 | 0 | 1 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| ppt | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| xls | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| docx | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| pptx | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| xlsx | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| rtf | 0 | 0 | 0 | 0 | 0 |
0 | 0 | ||
+-----+-----+-----+-----+-----+-----+
|| class | 2 | 2 | 0 | 1 | 0 |
1 | 0 | ||
+-----+-----+-----+-----+-----+-----+

```

```

|| swf | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 ||
|
+-----+
+|

```

Environment Analysis Summary for Non-Executable:
 VM Utilization : 0/16
 Files Analyzed : 4

```

+-----+
+
||                               Links
|                               ||
|
+-----+
+|

```

FileType	Submitted	Analyzed	Pending	Malware	Grayware
Benign	Error				

```

|| elink | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 ||
|
+-----+
+|

```

Environment Analysis Summary for Links:
 Files Analyzed : 1

```

+-----+
|                               General Stats                               |
+-----+

```

Total Disk Usage: 67/1283(GB) (5%)

Sample Queue		
SUBMITTED	ANALYZED	PENDING
7	7	0

Verdicts			
Malware	Grayware	Benign	Error
3	0	4	0

```

+-----+
|                               Session and Upload Count                               |
+-----+

```

Sessions	Uploads
7	5

Required Privilege Level

superuser, superreader

test wildfire registration

Description

Performs a test to check the registration status of a WildFire appliance or Palo Alto Networks firewall to a WildFire server. If the test is successful, the IP address or server name of the WildFire server is displayed. A successful registration is required before a WildFire appliance or firewall can forward files to the WildFire server.

Syntax

```
test {
wildfire {
registration;
}
}
```

Options

No additional options.

Sample Output

The following shows a successful output on a firewall that can communicate with a WildFire appliance. If this is a WildFire appliance pointing to the Palo Alto Networks WildFire cloud, the server name of one of the cloud servers is displayed in the `select the best server:` field.

Testing wildfire Public Cloud

```
wildfire registration:      successful
download server list:     successful
select the best server:   ca-
s1.wildfire.paloaltonetworks.com
```

Required Privilege Level

superuser, superreader

