



TECHDOCS

WildFire Administrator's Guide

Version 10.1

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

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

©2021–2022 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

May 21, 2021

Table of Contents

WildFire Overview.....	7
About WildFire.....	8
WildFire Concepts.....	10
Samples.....	10
Firewall Forwarding.....	10
Session Information Sharing.....	10
Analysis Environment.....	11
Verdicts.....	13
File Analysis.....	13
Email Link Analysis.....	15
URL Analysis.....	16
Compressed and Encoded File Analysis.....	16
WildFire Signatures.....	17
WildFire Deployments.....	18
WildFire Public Cloud.....	18
WildFire Private Cloud.....	19
WildFire Hybrid Cloud.....	20
WildFire: U.S. Government Cloud.....	20
WildFire File Type Support.....	23
WildFire Subscription.....	25
WildFire Example.....	27
Get Started with WildFire.....	31
WildFire Deployment Best Practices.....	37
WildFire Best Practices.....	38
Submit Files for WildFire Analysis.....	41
Forward Files for WildFire Analysis.....	42
Forward Decrypted SSL Traffic for WildFire Analysis.....	48
Verify WildFire Submissions.....	49
Test a Sample Malware File.....	49
Verify File Forwarding.....	50
Manually Upload Files to the WildFire Portal.....	55
Submit Malware or Reports from the WildFire Appliance.....	57
Sample Removal Request.....	58
Firewall File-Forwarding Capacity by Model.....	60
Set Up and Manage a WildFire Appliance.....	61
About the WildFire Appliance.....	62

WildFire Appliance Interfaces.....	62
Configure the WildFire Appliance.....	64
Set Up Authentication Using a Custom Certificate on a Standalone WildFire Appliance.....	72
WildFire Appliance Mutual SSL Authentication.....	72
Configure Authentication with Custom Certificates on the WildFire Appliance.....	73
Set Up the WildFire Appliance VM Interface.....	76
Virtual Machine Interface Overview.....	76
Configure the VM Interface on the WildFire Appliance.....	78
Connect the Firewall to the WildFire Appliance VM Interface.....	80
Enable WildFire Appliance Analysis Features.....	82
Set Up WildFire Appliance Content Updates.....	82
Enable Local Signature and URL Category Generation.....	85
Submit Locally-Discovered Malware or Reports to the WildFire Public Cloud.....	87
Upgrade a WildFire Appliance.....	89
Monitor WildFire Activity.....	93
About WildFire Logs and Reporting.....	94
Use the Firewall to Monitor Malware.....	95
Configure WildFire Submissions Log Settings.....	95
Monitor WildFire Submissions and Analysis Reports.....	95
Set Up Alerts for Malware.....	97
Use the WildFire Portal to Monitor Malware.....	101
Configure WildFire Portal Settings.....	101
Add WildFire Portal Users.....	102
View Reports on the WildFire Portal.....	103
Use the WildFire Appliance to Monitor Sample Analysis Status.....	104
View WildFire Analysis Environment Utilization.....	104
View WildFire Sample Analysis Processing Details.....	105
Use the WildFire CLI to Monitor the WildFire Appliance.....	107
View the WildFire Appliance System Logs.....	107
WildFire Analysis Reports—Close Up.....	109
WildFire Appliance Clusters.....	113
WildFire Appliance Cluster Resiliency and Scale.....	114
WildFire Cluster High Availability.....	116
Benefits of Managing WildFire Clusters Using Panorama.....	116
WildFire Appliance Cluster Management.....	118
Deploy a WildFire Cluster.....	122
Configure a Cluster Locally on WildFire Appliances.....	123

Configure a Cluster and Add Nodes Locally.....	123
Configure General Cluster Settings Locally.....	130
Remove a Node from a Cluster Locally.....	133
Configure WildFire Appliance-to-Appliance Encryption.....	137
Configure Appliance-to-Appliance Encryption Using Predefined Certificates Through the CLI.....	137
Configure Appliance-to-Appliance Encryption Using Custom Certificates Through the CLI.....	138
Monitor a WildFire Cluster.....	142
View WildFire Cluster Status Using the CLI.....	142
WildFire Application States.....	154
WildFire Service States.....	161
Upgrade WildFire Appliances in a Cluster.....	162
Upgrade a Cluster Locally with an Internet Connection.....	162
Upgrade a Cluster Locally without an Internet Connection.....	165
Troubleshoot a WildFire Cluster.....	169
Troubleshoot WildFire Split-Brain Conditions.....	169

Use the WildFire Appliance CLI.....173

WildFire Appliance Software CLI Concepts.....	174
WildFire Appliance Software CLI Structure.....	174
WildFire Appliance Software CLI Command Conventions.....	174
WildFire Appliance CLI Command Messages.....	175
WildFire Appliance Command Option Symbols.....	175
WildFire Appliance Privilege Levels.....	177
WildFire CLI Command Modes.....	178
WildFire Appliance CLI Configuration Mode.....	178
WildFire Appliance CLI Operational Mode.....	180
Access the WildFire Appliance CLI.....	182
Establish a Direct Console Connection.....	182
Establish an SSH Connection.....	182
WildFire Appliance CLI Operations.....	183
Access WildFire Appliance Operational and Configuration Modes.....	183
Display WildFire Appliance Software CLI Command Options.....	183
Restrict WildFire Appliance CLI Command Output.....	184
Set the Output Format for WildFire Appliance Configuration Commands....	185
WildFire Appliance Configuration Mode Command Reference.....	186
set deviceconfig cluster.....	186
set deviceconfig high-availability.....	187
set deviceconfig setting management.....	190
set deviceconfig setting wildfire.....	190

set deviceconfig system eth2.....	193
set deviceconfig system eth3.....	194
set deviceconfig system panorama local-panorama panorama-server.....	195
set deviceconfig system panorama local-panorama panorama-server-2.....	196
set deviceconfig system update-schedule.....	197
set deviceconfig system vm-interface.....	198
WildFire Appliance Operational Mode Command Reference.....	200
clear high-availability.....	201
create wildfire api-key.....	202
delete high-availability-key.....	203
delete wildfire api-key.....	204
delete wildfire-metadata.....	205
disable wildfire.....	206
edit wildfire api-key.....	206
load wildfire api-key.....	208
request cluster decommission.....	208
request cluster reboot-local-node.....	210
request high-availability state.....	211
request high-availability sync-to-remote.....	213
request system raid.....	214
request wildfire sample redistribution.....	215
request system wildfire-vm-image.....	217
request wf-content.....	218
save wildfire api-key.....	219
set wildfire portal-admin.....	220
show cluster all-peers.....	221
show cluster controller.....	222
show cluster data migration status.....	223
show cluster membership.....	223
show cluster task.....	226
show high-availability all.....	228
show high-availability control-link.....	229
show high-availability state.....	231
show high-availability transitions.....	232
show system raid.....	233
submit wildfire local-verdict-change.....	234
show wildfire.....	235
show wildfire global.....	237
show wildfire local.....	241
test wildfire registration.....	248

WildFire 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 WildFire](#)
- > [WildFire Concepts](#)
- > [WildFire Deployments](#)
- > [WildFire File Type Support](#)
- > [WildFire Subscription](#)
- > [WildFire Example](#)
- > [Get Started with WildFire](#)

About WildFire

The WildFire [Analysis Environment](#) identifies previously unknown malware and generates signatures that Palo Alto Networks firewalls can use to then detect and block the malware. When a Palo Alto Networks firewall detects an unknown sample (a file or a link included in an email), the firewall can automatically forward the sample for WildFire analysis. Based on the properties, behaviors, and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire determines the sample to be benign, grayware, phishing, or malicious. WildFire then generates signatures to recognize the newly-discovered malware, and makes the latest signatures globally available for retrieval in real-time. All Palo Alto Networks firewalls can then compare incoming samples against these signatures to automatically block the malware first detected by a single firewall. The following workflow describes the WildFire process lifecycle from when a user downloads a file carrying an advanced VM-aware payload to the point where WildFire generates a signature package used by Palo Alto Networks firewalls to protect against future exposure to malware.

In this example, the following assumptions are made:

- A firewall is registered to the WildFire cloud and is configured to forward supported file types.
- The malware found in the file attachment is an advanced VM-aware threat and has not been encountered before.
- The file download is logged if the data filtering logs and WildFire submissions logs are configured to be forwarded to the firewall.

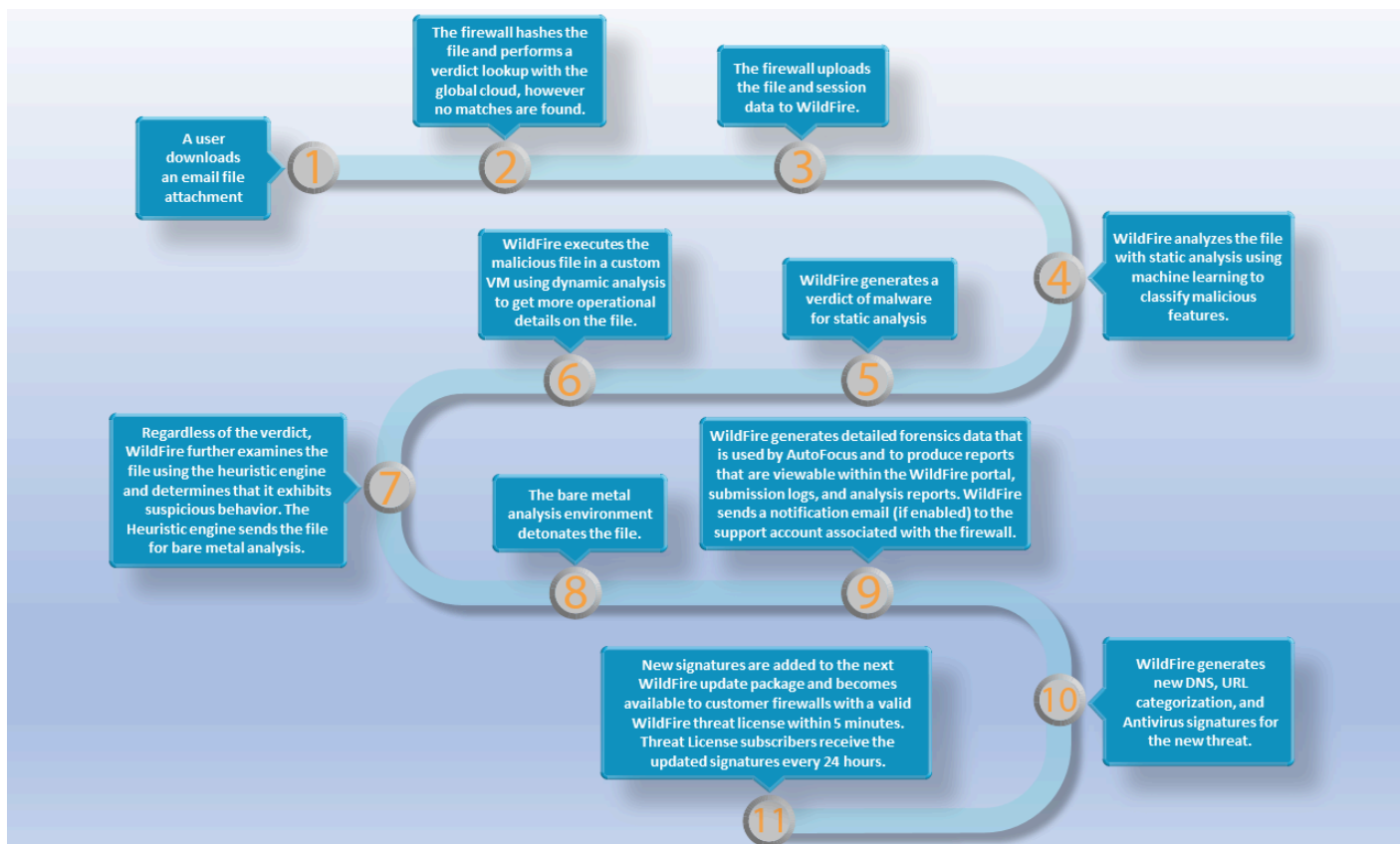


Figure 1: WildFire Process Workflow

To learn more about WildFire, or to get started with WildFire now, see the following topics:

- ❑ Review [WildFire Concepts](#) to learn more about the types of samples you can submit for WildFire analysis, WildFire verdicts, and WildFire signatures.
- ❑ Learn more about [WildFire Deployments](#) deployments you can set up with the firewall. You can submit samples you would like to have analyzed to a Palo Alto Networks-hosted WildFire cloud, a locally-hosted WildFire private cloud, or you can use a hybrid cloud, where the firewall submits certain samples to the public cloud and certain samples to a private cloud.
- ❑ [Get Started with WildFire](#) to define the samples that you want to submit for analysis, and to begin submitted samples to a WildFire cloud.
- ❑ *Manage WildFire Appliances* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) using Panorama to manage up to 200 WildFire appliances centrally instead of individually.
- ❑ *Create WildFire Appliance Clusters* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) to increase analysis and storage capacity, support more firewalls on a single network, and implement high-availability to provide fault tolerance. You can manage WildFire appliance clusters using the local WildFire CLI or using Panorama.

WildFire Concepts

- [Samples](#)
- [Firewall Forwarding](#)
- [Session Information Sharing](#)
- [Analysis Environment](#)
- [Verdicts](#)
- [File Analysis](#)
- [Email Link Analysis](#)
- [URL Analysis](#)
- [Compressed and Encoded File Analysis](#)
- [WildFire Signatures](#)
- [WildFire Example](#)

Samples

Samples are all file types and email links submitted for WildFire analysis from the firewall and the public API. See [File Analysis](#) and [Email Link Analysis](#) for details on the file types and links that a firewall can submit for WildFire analysis.

Firewall Forwarding

The firewall forwards unknown samples, as well as blocked files that match antivirus signatures, for WildFire analysis based on the configured WildFire Analysis profile settings (**Objects > Security Profiles > WildFire Analysis**). In addition to detecting links included in emails, files that are attached to emails, and browser-based file downloads, the firewall leverages the App-ID to detect file transfers within applications. For samples that the firewall detects, the firewall analyzes the structure and content of the sample and compares it against existing signatures. If the sample matches a signature, the firewall applies the default action defined for the signature (allow, alert, or block). If the sample matches an antivirus signature or if the sample remains unknown after comparing it against WildFire signatures, the firewall forwards it for WildFire analysis.

By default, the firewall also forwards information about the session in which an unknown sample was detected. To manage the session information that the firewall forwards, select **Device > Setup > WildFire** and edit Session Information Settings.

Session Information Sharing

In addition to forwarding unknown and blocked samples for analysis, the firewall also forwards information about the network session for a sample. Palo Alto Networks uses session information to learn more about the context of the suspicious network event, indicators of compromise related to the malware, affected hosts and clients, and applications used to deliver the malware.

The firewall is enabled to forward session information by default; however, you can adjust the default settings and choose what type of session information the firewall forwards to WildFire.

On the firewall, select **Device > Setup > WildFire** and select or clear the following **Session Information Settings**:

- **Source IP**—Forward the source IP address that sent the unknown file.
- **Source Port**—Forward the source port that sent the unknown file.
- **Destination IP**—Forward the destination IP address for the unknown file.
- **Destination Port**—Forward the destination port for the unknown file.
- **Virtual System**—Forward the virtual system that detected the unknown file.
- **Application**—Forward the user application that transmitted the unknown file.
- **User**—Forward the targeted user.
- **URL**—Forward the URL associated with the unknown file.
- **Filename**—Forward the name of the unknown file.
- **Email sender**—Forward the sender of an unknown email link (the name of the email sender also appears in WildFire logs and reports).
- **Email recipient**—Forward the recipient of an unknown email link (the name of the email recipient also appears in WildFire logs and reports).
- **Email subject**—Forward the subject of an unknown email link (the email subject also appears in WildFire logs and reports).

Analysis Environment

WildFire reproduces a variety of analysis environments, including the operating system, to identify malicious behaviors within samples. Depending on the characteristics and features of the sample, multiple analysis environments may be used to determine the nature of the file. WildFire uses static analysis with machine learning to initially determine if known and variants of known samples are malicious. Based on the initial verdict of the submission, WildFire sends the unknown samples to analysis environment(s) to inspect the file in greater detail by extracting additional information and indicators from dynamic analysis. If the file has been obfuscated using custom or open source methods, the WildFire cloud decompresses and decrypts the file in-memory within the dynamic analysis environment before analyzing it using static analysis. During dynamic analysis, WildFire observes the file as it would behave when executed within client systems and looks for various signs of malicious activities, such as changes to browser security settings, injection of code into other processes, modification of files in operating system folders, or attempts by the sample to access malicious domains. Additionally, PCAPs generated during dynamic analysis in the WildFire cloud undergo deep inspection and are used to create network activity profiles. Network traffic profiles can detect known malware and previously unknown malware using a one-to-many profile match.

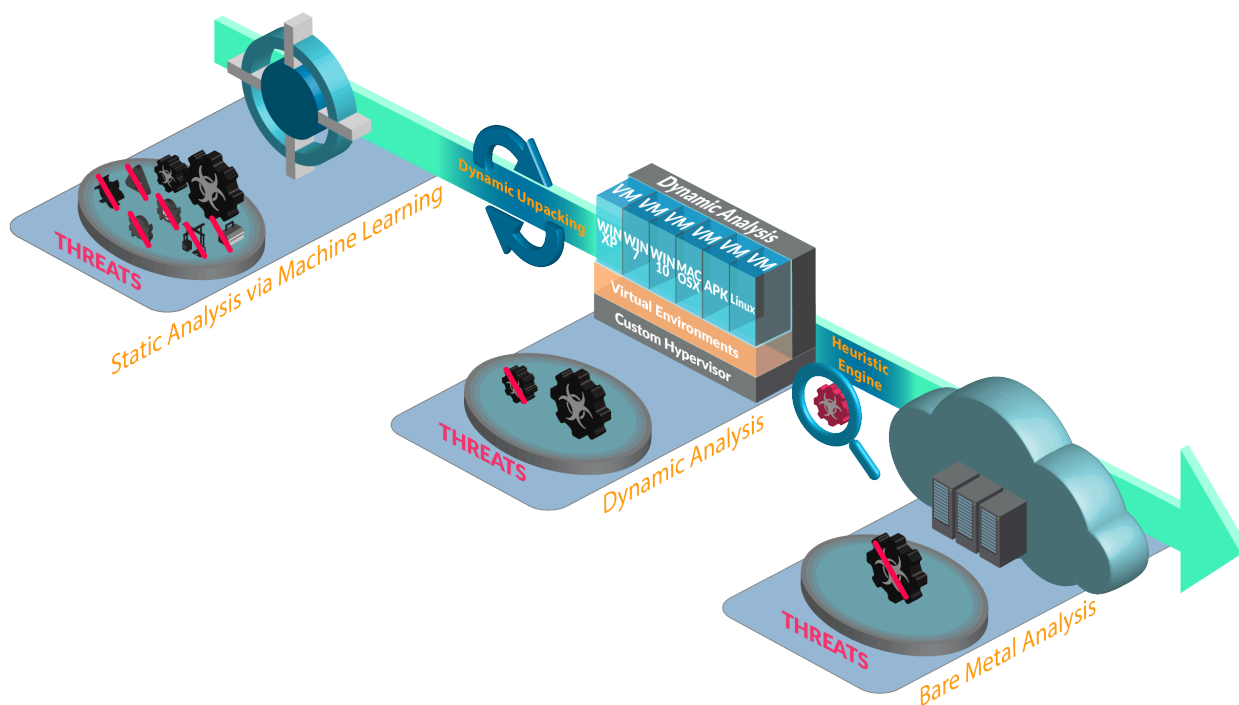


Figure 2: WildFire Sample Analysis Workflow

WildFire analyzes files using the following methods:

- **Static Analysis**—Detects known threats by analyzing the characteristics of samples prior to execution.
- **Machine Learning**—Identifies variants of known threats by comparing malware feature sets against a dynamically updated classification systems.
- **Dynamic Unpacking (WildFire Cloud analysis only)**—Identifies and unpacks files that have been encrypted using custom/open source methods and prepares it for static analysis.
- **Dynamic Analysis**—A custom built, evasion resistant virtual environment in which previously unknown submissions are detonated to determine real-world effects and behavior.
- **Bare Metal Analysis (WildFire Cloud analysis only)**—A fully hardware-based analysis environment specifically designed for advanced VM-aware threats. Samples that display the characteristics of an advanced VM-aware threat are steered towards the bare metal appliance by the heuristic engine.



Bare metal analysis is not available on the WildFire appliance.

WildFire operates analysis environments that replicate the following operating systems:

- Microsoft Windows XP 32-bit
- Microsoft Windows 7 64-bit
- Microsoft Windows 7 32-bit (Supported as an option for WildFire appliance only)
- Microsoft Windows 10 64-bit (WildFire Cloud Analysis and WildFire appliance running PAN-OS 10.0 or later)
- Mac OS X (WildFire Cloud Analysis only)

- **Android (WildFire Cloud Analysis only)**
- **Linux (WildFire Cloud Analysis only)**

The WildFire public cloud also analyzes files using multiple versions of software to accurately identify malware that target specific versions of client applications. The WildFire private cloud does not support multi-version analysis, and does not analyze application-specific files across multiple versions.

Verdicts

When WildFire analyzes a previously unknown sample in one of the Palo Alto Networks-hosted WildFire public clouds or a locally-hosted WildFire private cloud, a verdict is produced to identify samples as malicious, unwanted (grayware is considered obtrusive but not malicious), phishing, or benign:

- **Benign**—The sample is safe and does not exhibit malicious behavior.
- **Grayware**—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).
- **Phishing**—The link directs users to a phishing site and poses a security threat. Phishing sites are sites that attackers disguise as legitimate websites with the aim to steal user information, especially corporate passwords that unlock access to your network. The WildFire appliance does not support the phishing verdict and continues to classify these types of links as malicious.
- **Malicious**—The sample is malware and poses a security threat. Malware can include viruses, worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For files identified as malware, WildFire generates and distributes a signature to prevent against future exposure to the threat.

Each WildFire cloud—global (U.S.), regional, and private—analyzes samples and generates WildFire verdicts independently of the other WildFire clouds. With the exception of WildFire private cloud verdicts, WildFire verdicts are shared globally, enabling WildFire users to access a worldwide database of threat data.



Verdicts that you suspect are either false positives or false negatives can be submitted to the Palo Alto Networks threat team for additional analysis. You can also manually change verdicts of samples submitted to WildFire appliances.

File Analysis

A Palo Alto Networks firewall configured with a WildFire analysis profile forwards samples for WildFire analysis based on file type (including email links). Additionally, the firewall decodes files that have been encoded or compressed up to four times (such as files in ZIP format); if the decoded file matches WildFire Analysis profile criteria, the firewall forwards the decoded file for WildFire analysis.


The WildFire analysis capabilities can also be enabled on the firewall to provide inline antivirus protection. The WildFire inline ML option present in the Antivirus profiles enables the firewall dataplane to apply machine learning analysis on PE and ELF files as well as PowerShell scripts in real-time. Each inline ML model dynamically detects malicious files of a specific type by evaluating


file details, including decoder fields and patterns, to formulate a high probability classification of a file. This protection extends to currently unknown as well as future variants of threats that match characteristics that Palo Alto Networks has identified as malicious. To keep up with the latest changes in the threat landscape, inline ML models are added or updated via content releases. See [WildFire Inline ML](#) for more information.

The WildFire cloud is also capable of analyzing certain file types which are used as secondary payloads as part of multi-stage PE, APK, and ELF malware packages. Analysis of secondary payloads can provide additional coverage to disrupt sophisticated attacks by advanced threats. These advanced threats operate by executing code which activate additional malicious payloads, including those designed to assist in the circumvention of security measures as well as facilitate proliferation of the primary payload. WildFire analyzes the multi-stage threats by processing them in static, dynamic, or bare metal analysis environments. Files referenced by multi-stage malware are treated independently during analysis; as a result, verdicts and protections are delivered as soon as they finish for each file. The overall verdict for the multi-stage file is determined based on a threat assessment of malicious content found in all analyzed stages of the attack. Any malicious content discovered during analysis of the multi-stage file immediately marks the file as malicious.

Organizations with safe-handling procedures for malicious content can manually submit password-protected samples using the RAR format through the API or WildFire portal. When the WildFire cloud receives a sample that has been encrypted using the password *infected* or *virus*, the WildFire cloud decrypts and analyzes the archive file. You can view the WildFire verdict and analysis results for the file in the format that it was received, in this case, an archive.

While the firewall can forward all the file types listed below, WildFire analysis support can vary depending on the WildFire cloud to which you are submitted samples. Review [WildFire File Type Support](#) to learn more.

File Types Supported for WildFire Forwarding	Description
apk	Android Application Package (APK) files.  <i>DEX files contained within APK files are analyzed as part of the APK file analysis.</i>
flash	Adobe Flash applets and Flash content embedded in web pages.
jar	Java applets (JAR/class files types).
ms-office	Files used by Microsoft Office, including documents (DOC, DOCX, RTF), workbooks (XLS, XLSX), PowerPoint (PPT, PPTX) presentations, and Office Open XML (OOXML) 2007+ documents. Internet Query (IQY) and Symbolic Link (SLK) files are supported with content version 8462.
pe	Portable Executable (PE) files. PEs include executable files, object code, DLLs, FON (fonts), and LNK files. MSI files are supported with content

File Types Supported for WildFire Forwarding	Description
	version 8462. A subscription is not required to forward PE files for WildFire analysis, but is required for all other supported file types.
pdf	Portable Document Format (PDF) files.
MacOSX	Mach-O, DMG, and PKG files are supported with content version 599. You can also manually or programmatically submit all Mac OS X supported file types for analysis (including application bundles, for which the firewall does not support automatic forwarding).
email-link	HTTP/HTTPS links contained in SMTP and POP3 email messages. See Email Link Analysis .
archive	<p>Roshal Archive (RAR) and 7-Zip (7z) archive files. Multi-volume archives that are split into several smaller files cannot be submitted for analysis.</p> <p>Only RAR files encrypted with the password <i>infected</i> or <i>virus</i> are decrypted and analyzed by the WildFire cloud.</p> <p> <i>While the firewall is capable of forwarding supported files contained within ZIP archives after it has been decoded, it cannot forward complete ZIP files in its encoded state. If you want to submit complete ZIP files, you can manually upload a ZIP file using the WildFire portal or through the WildFire API.</i></p>
linux	Executable and Linkable Format (ELF) files.
script	<p>Various script files.</p> <ul style="list-style-type: none"> • Jscript (JS), VBScript (VBS), and PowerShell Scripts (PS1) are supported with content version 8101. • Batch (BAT) files are supported with content version 8168. • HTML Application (HTA) files are supported with content version 8229.

Email Link Analysis

A Palo Alto Networks firewall can extract HTTP/HTTPS links contained in SMTP and POP3 email messages and forward the links for WildFire analysis. The firewall only extracts links and associated session information (sender, recipient, and subject) from email messages; it does not receive, store, forward, or view the email message.

WildFire visits submitted links to determine if the corresponding web page hosts any exploits or displays phishing activity. A link that WildFire finds to be malicious or phishing is:

- Recorded on the firewall as a WildFire Submissions log entry. The WildFire analysis report that details the behavior and activity observed for the link is available for each WildFire Submissions log entry. The log entry also includes the email header information—email sender, recipient, and subject—so that you can identify the message and delete it from the mail server, or mitigate the threat if the email has been delivered or opened.
- Added to PAN-DB and the URL is categorized as malware.

The firewall forwards email links in batches of 100 email links or every two minutes (depending on which limit is hit first). Each batch upload to WildFire counts as one upload toward the upload per-minute capacity for the given firewall *Firewall Forwarding Capacity by Model* (PAN-OS 9.1, 10.0, 10.1, 10.2). If a link included in an email corresponds to a file download instead of a URL, the firewall forwards the file only if the corresponding file type is enabled for WildFire analysis.

To enable the firewall to forward links included in emails for WildFire analysis, see *Forward Files for WildFire Analysis* (PAN-OS 9.1, 10.0, 10.1, 10.2). With a PAN-DB URL Filtering license, you can also block user access to malicious and phishing sites.

URL Analysis

The WildFire global cloud (U.S.) and regional clouds can analyze URLs, and by extension, email links, to provide standardized verdicts and reports through the [WildFire API](#). By aggregating threat analysis details from all Palo Alto Networks services, including PAN-DB, WildFire is able to generate a more accurate verdict and provide consistent URL analysis data.

The URL analyzers operating in the WildFire global cloud (U.S.) processes URL feeds, correlated URL sources (such as email links), NRD (newly registered domain) lists, PAN-DB content, and manually uploaded URLs, to provide all WildFire clouds with the improved capabilities, without affecting GDPR compliance. After a URL has been processed, you can retrieve the WildFire URL analysis report, which includes the verdict, detection reasons with evidence, screenshots, and analysis data generated for the web request. You can also retrieve web page artifacts (downloaded files and screenshots) seen during URL analysis to further investigate anomalous activity.

No additional configuration is necessary to take advantage of this feature, however, if you want to automatically submit email links for analysis (which are now analyzed through this service), you must configure your firewall to forward email link (PAN-OS 9.1, 10.0, 10.1, 10.2).

Verdicts that you suspect are either false positives or false negatives can be submitted (PAN-OS 9.1, 10.0, 10.1, 10.2) to the Palo Alto Networks threat team for additional analysis.

Compressed and Encoded File Analysis

By default, the firewall decodes files that have been encoded or compressed up to four times, including files that have been compressed using the ZIP format. The firewall then inspects and enforces policy on the decoded file; if the file is unknown, the firewall forwards the decoded file for WildFire analysis. While the firewall cannot forward complete ZIP archive files for WildFire analysis, you can submit files directly to the WildFire public cloud using the WildFire portal or the WildFire API.



RAR and 7-Zip archive files are not decoded by the firewall. All processing of these files occurs in the WildFire public cloud.

WildFire Signatures

WildFire can discover zero-day malware in web traffic (HTTP/HTTPS), email protocols (SMTP, IMAP, and POP), and FTP traffic and can quickly generate signatures to identify and protect against future infections from the malware it discovers. WildFire automatically generates a signature based on the malware payload of the sample and tests it for accuracy and safety.

Each WildFire cloud—global, regional, and private—analyzes samples and generates malware signatures independently of the other WildFire clouds. With the exception of WildFire private cloud signatures, WildFire signatures are shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location in which the malware was first detected. Because malware evolves rapidly, the signatures that WildFire generates address multiple variants of the malware.

Firewalls with an active WildFire license can retrieve the latest WildFire signatures in real-time, as soon as they become available. If you do not have a WildFire subscription, signatures are made available within 24-48 hours as part of the antivirus update for firewalls with an active Threat Prevention license.

As soon as the firewall downloads and installs the new signature, the firewall can block the files that contain that malware (or a variant of the malware). Malware signatures do not detect malicious and phishing links; to enforce these links, you must have a PAN-DB URL Filtering license. You can then block user access to malicious and phishing sites.

WildFire Deployments

You can set up a Palo Alto Networks firewall to submit unknown samples to one of the Palo Alto Networks-hosted WildFire public clouds, the U.S. Government cloud, a locally-hosted WildFire private cloud, or enable the firewall to forward certain samples to one of the WildFire public cloud options and certain samples to a WildFire private cloud:

- [WildFire Public Cloud](#)
- [WildFire Private Cloud](#)
- [WildFire Hybrid Cloud](#)
- [WildFire: U.S. Government Cloud](#)

WildFire Public Cloud

A Palo Alto Networks firewall can forward unknown files and email links to the WildFire global cloud (U.S.) or to the WildFire regional clouds that Palo Alto Networks owns and maintains. Choose the WildFire public cloud to which you want to submit samples for analysis (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) based on your location and your organization's needs:

- **WildFire Global Cloud (U.S.)**

The WildFire global cloud (U.S.) is a public cloud environment hosted in the United States.

Use the following URL to submit files to the WildFire global cloud (U.S.) for analysis and to access the WildFire global cloud (U.S.) portal: wildfire.paloaltonetworks.com.

- **WildFire Europe Cloud**

The WildFire Europe cloud is a regional public cloud environment hosted in The Netherlands. It is designed to adhere to European Union (EU) data privacy regulations and samples submitted to the WildFire Europe cloud remain within EU borders.

Use the following URL to submit files to the WildFire Europe cloud for analysis and to access the WildFire Europe cloud portal: eu.wildfire.paloaltonetworks.com.

- **WildFire Japan Cloud**

The WildFire Japan cloud is a regional public cloud environment hosted in Japan.

Use the following URL to submit files to the WildFire Japan cloud for analysis and to access the WildFire Japan cloud portal: jp.wildfire.paloaltonetworks.com.

- **WildFire Singapore Cloud**

The WildFire Singapore cloud is a regional public cloud environment hosted in Singapore.

Use the following URL to submit files to the WildFire Singapore cloud for analysis and to access the WildFire Singapore cloud portal: sg.wildfire.paloaltonetworks.com.

- **WildFire United Kingdom Cloud**

The WildFire UK cloud is a regional public cloud environment hosted in the United Kingdom.

Use the following URL to submit files to the WildFire UK cloud for analysis and to access the WildFire UK cloud portal: uk.wildfire.paloaltonetworks.com.

- **WildFire Canada Cloud**

The WildFire Canada cloud is a regional public cloud environment hosted in Canada.

Use the following URL to submit files to the WildFire Canada cloud for analysis and to access the WildFire Canada cloud portal: ca.wildfire.paloaltonetworks.com.

- **WildFire Australia Cloud**

The WildFire Australia cloud is a regional public cloud environment hosted in Australia.

Use the following URL to submit files to the WildFire Australia cloud for analysis and to access the WildFire Australia cloud portal: au.wildfire.paloaltonetworks.com.

- **WildFire Germany Cloud**

The WildFire Germany cloud is a regional public cloud environment hosted in Germany.

Use the following URL to submit files to the WildFire Germany cloud for analysis and to access the WildFire Germany cloud portal: de.wildfire.paloaltonetworks.com.

- **WildFire India Cloud**

The WildFire India cloud is a regional public cloud environment hosted in India.

Use the following URL to submit files to the WildFire India cloud for analysis and to access the WildFire India cloud portal: in.wildfire.paloaltonetworks.com.

Each WildFire cloud—global (U.S.) and regional—analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds. WildFire signatures and verdicts are then shared globally, enabling WildFire users worldwide to benefit from malware coverage regardless of the location in which the malware was first detected. Review [WildFire File Type Support](#) to learn more about the file types that each cloud analyzes.

If you have a WildFire appliance, you can enable a [WildFire Hybrid Cloud](#) deployment, where the firewall can forward certain files to a WildFire public cloud, and other files to a WildFire private cloud for local analysis. The WildFire appliance can also be configured to quickly gather verdicts for known samples by querying the public cloud before performing analysis. This allows the WildFire appliance to dedicate analysis resources to samples that are unknown to both your private network and the global WildFire community.

WildFire Private Cloud

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* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).
- *Manually Upload Files to the WildFire Portal* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) 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* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) 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

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 Analysis* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).

WildFire: U.S. Government Cloud

The Palo Alto Networks WildFire U.S. Government cloud is a high-security malware analysis platform that is [FedRAMP](#) (Federal Risk and Authorization Management Program) authorized. This WildFire cloud environment is intended for use only by U.S. federal agencies requiring a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The WildFire: U.S. Government cloud operates as a separate and distinct entity — Any privacy information that might be present in samples sent for analysis, such as email addresses, IP addresses, and passive DNS, will not be shared with any other WildFire cloud instance. However, it is still able to leverage threat data generated by the WildFire public cloud to maximize coverage capability as well as protections and antivirus signatures produced through file analysis.

For more detailed information about Palo Alto Network's WildFire FedRAMP authorization, visit: [Palo Alto Networks Government Cloud Services - WildFire](#)

The WildFire public cloud (the global and regional clouds) and the WildFire U.S. Government cloud has several functional differences from the public cloud. The following functionality is not available for customers connecting to the WildFire: U.S. Government cloud:

- Bare Metal Analysis is not supported by the U.S. Government cloud.
- Script file (Bat, JS, BVS, PS1, Shell script, and HTA) analysis is currently not supported.
- The WildFire: U.S. Government cloud cannot be accessed through the WildFire portal.
- The WildFire: U.S. Government cloud cannot be integrated with other cloud-based services.
- Right to delete functionality is not available.

Get Started with the WildFire: U.S. Government Cloud

In order to connect to the WildFire: U.S. Government cloud, you must apply for access. Follow any internal procedural measures to determine the suitability of using the WildFire: U.S. Government cloud within your network, such as, but not limited to conducting a risk analysis, evaluation of the CSP submission package, and authorization approvals. Please contact your Palo Alto Networks sales representative / WildFire: U.S. Government Cloud point of contact to discuss any additional operational details.

Requests to access the WildFire U.S. Government cloud begins when you have met the proper organization requirements for operating a FedRAMP authorized service. There are two entity categories who can access the WildFire U.S. government cloud: U.S. government contractors and U.S. federal agencies (and other approved governmental departments). Both entities have specific requirements for accessing the WildFire U.S. government cloud:

1. U.S. Federal Agencies

U.S. federal agencies, departments, and bureaus must receive an Authority to Operate (ATO) by the Designated Approving Authority (DAA), which authorizes operation of the WildFire U.S. government cloud within an agencies operations, before access is granted.

1. Inform the Palo Alto Networks Point of Contact (fedramp@paloaltonetworks.com) of the intention to use the WildFire U.S. government cloud.
2. Send a request to info@fedramp.gov.
3. Complete the FedRAMP Package Access Request Form and submit it to info@fedramp.gov.



The FedRAMP Program Management Office (PMO) reviews the form and typically issues a temporary 30 day access to the WildFire FedRAMP package.

4. Review the FedRAMP security package for the WildFire U.S. Government cloud. Complete any internal processes required to deploy the WildFire U.S. Government cloud into your organization.
5. Issue the ATO.
6. Send a request to the FedRAMP PMO for permanent access to the WildFire U.S. government cloud.

2. U.S. Government Contractors

U.S. government contractors who use or access the WildFire U.S. government cloud must meet the following requirements.

1. Must be a citizen of the United States.
2. Hold an active contract (or subcontract) with a U.S. federal government agency with an occupational requirement for information exchange using the Internet, such as email correspondence, sharing of documents, and other forms of Internet communication.
3. Upon termination of a contractor's employment, the user must cease using or accessing the WildFire U.S. government cloud.
4. Abide by the confidentiality provisions contained within the Palo Alto Networks EULA.

After your organization issues an Authorization to Operate (ATO) or when applicable U.S. government contractors meet all usage requirements, only then can a request be made to access the WildFire U.S. Government cloud by contacting your Palo Alto Networks Account team.

1. Contact your FedRAMP Program Management Office (PMO) to determine the viability of the U.S. Government cloud for your security needs.
2. Contact the Palo Alto Networks point of contact specified in the [FedRAMP Marketplace](#). The point of contact provides additional information about the service, as well as any other operational details pertinent to your particular WildFire deployment.
3. Contact the Palo Alto Networks Account Team to begin the on-boarding process. The Account Team will request the following information regarding customer details and deployment specifics.
 - Contact information.
 - A brief description for migrating to the WildFire U.S. Government cloud.
 - A statement of organizational compliance with the confidentiality provisions outlined within the Palo Alto Networks EULA.
 - Egress IP addresses of all firewall gateways (including management planes), as well as all instances of Panorama.
4. After WildFire Program Management grants approval to use the WildFire U.S. Government cloud (typically in one to three business days), Palo Alto Networks Development Operations applies the appropriate controls.
5. After access to the WildFire U.S. Government cloud is granted, reconfigure the firewall to forward unknown files and email links for analysis using the following URL: wildfire.gov.paloaltonetworks.com. For more information, see Forward Files for Wildfire Analysis. If you require any additional assistance, contact Palo Alto Networks Customer Support.

WildFire File Type Support

The following table lists the file types that are supported for analysis in the WildFire cloud environments.

File Types Supported for Analysis	WildFire Public Cloud (all regions)	WildFire U.S. Government Cloud	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	✓	✓	✗	✓

File Types Supported for Analysis	WildFire Public Cloud (all regions)	WildFire U.S. Government Cloud	WildFire Private Cloud (WildFire appliance)	WildFire Portal API (direct upload; all regions)
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.



Looking for more?

- For details on each WildFire cloud analysis environment, see [WildFire Deployments](#).
- For details about each file type supported for WildFire analysis, see [File Analysis](#).

WildFire Subscription

The basic WildFire service is included as part of the Palo Alto Networks next generation firewall and does not require a WildFire subscription. With the basic WildFire service, the firewall can forward portable executable (PE) files for WildFire analysis, and can retrieve WildFire signatures only with antivirus and/or Threat Prevention updates which are made available every 24-48 hours.

A WildFire subscription unlocks the following WildFire features:

- **WildFire Real-Time Updates**—(PAN-OS 10.0 and later) The firewall can retrieve WildFire signatures for newly-discovered malware as soon as the WildFire public cloud can generate them. Signatures that are downloaded during a sample check are saved in the firewall cache, and are available for fast (local) look-ups. In addition, to maximize coverage, the firewall also automatically downloads a signature package on a regular basis when real-time signatures is enabled. These supplemental signatures are added to the firewall cache and remain available until they become stale and are refreshed or are overwritten by new signatures. Using real-time WildFire updates is a recommended best practice setting.

Select **Device > Dynamic Updates** and enable the firewall to [get the latest WildFire signatures](#) in real-time.

- **WildFire Five-Minute Updates**—(All PAN-OS versions) The WildFire public cloud and a WildFire private cloud can generate and distribute WildFire signatures for newly-discovered malware every five minutes, and you can set the firewall to retrieve and install these signatures every minute (this allows the firewall to get the latest signatures within a minute of availability).



If you are running PAN-OS 10.0 or later, it is a best practice to use real-time WildFire updates instead of scheduling recurring updates.

Select **Device > Dynamic Updates** to enable the firewall to [get the latest WildFire signatures](#). Depending on your WildFire deployment, you can set up one or both of the following signature package updates:

- **WildFire**—Get the latest signatures from the WildFire public cloud.
- **WF-Private**—Get the latest signatures from a WildFire appliance that is configured to locally generate signatures and URL categories (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).
- **WildFire Inline ML**—(PAN-OS 10.0 and later) Prevent malicious variants of portable executables, executable and linked format (ELF) files, and PowerShell scripts from entering your network in real-time using machine learning (ML) on the firewall dataplane. By utilizing WildFire® Cloud analysis technology on the firewall, [WildFire Inline ML](#) dynamically detects malicious files of a specific type by evaluating various file details, including decoder fields and patterns, to formulate a high probability classification of a file. This protection extends to currently unknown as well as future variants of threats that match characteristics that Palo Alto Networks identified as malicious. WildFire inline ML complements your existing Antivirus profile protection configuration. Additionally, you can specify file hash exceptions to exclude any false-positives that you encounter, which enables you to create more granular rules in your profiles to support your specific security needs.
- **WildFire Advanced File Type Support**—In addition to PEs, forward advanced file types for WildFire analysis, including APKs, Flash files, PDFs, Microsoft Office files, Java Applets,

Java files (.jar and .class), and HTTP/HTTPS email links contained in SMTP and POP3 email messages. (WildFire private cloud analysis does not support APK, Mac OS X, Linux (ELF), archive (RAR/7-Zip), and script (JS, BAT, VBS, Shell Script, PS1, and HTA) files).

- **WildFire API**—Access to the [WildFire API](#), which enables direct programmatic access to the WildFire public cloud or a WildFire private cloud. Use the WildFire API to submit files for analysis and to retrieve the subsequent WildFire analysis reports. As part of the WildFire subscription, you can submit up to 150 sample submissions and up to 1,500 sample queries a day. These daily sample submission limits can be extended, based on your organization's specific needs. Please contact your Palo Alto Networks sales representative for more information.
- **WildFire Private and Hybrid Cloud Support**—*Forward Files to a WildFire Appliance* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)). WildFire private cloud and WildFire hybrid cloud deployments both require the firewall to be able to submit samples to a WildFire appliance. Enabling a WildFire appliance requires only a support license.

If you have purchased a WildFire subscription, you must activate (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) it before you can take advantage of the subscription-only WildFire features.

WildFire Example

The following example scenario summarizes the full WildFire™ lifecycle. In this example, a sales representative from Palo Alto Networks downloads a new software sales tool that a sales partner uploaded to Dropbox. The sales partner unknowingly uploaded an infected version of the sales tool install file and the sales rep then downloads the infected file.

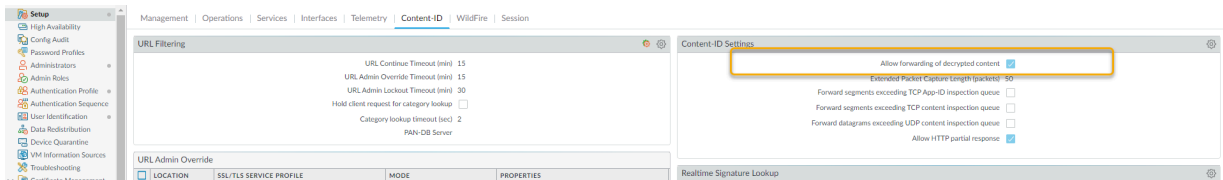
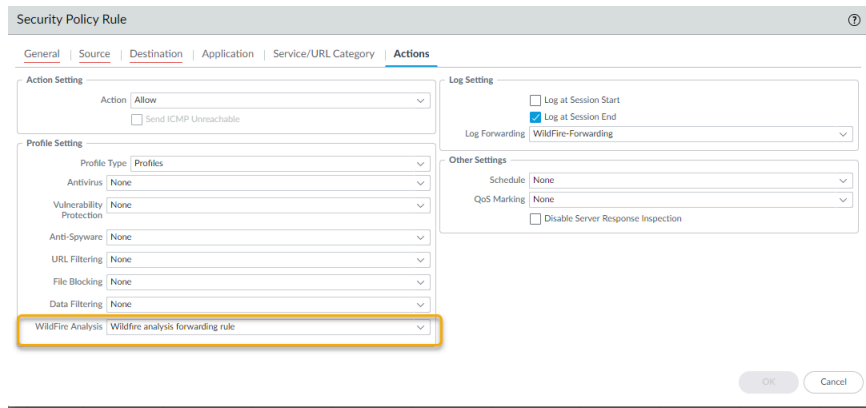
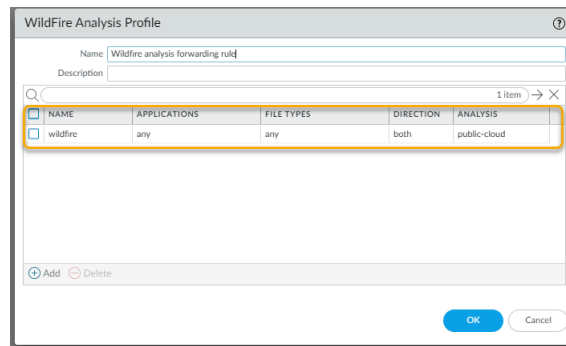
This example will demonstrate how a Palo Alto Networks firewall in conjunction with WildFire can discover zero-day malware downloaded by an end user, even if the traffic is SSL encrypted. After WildFire identifies the malware a log is sent to the firewall and the firewall alerts the administrator who then contacts the user to eradicate the malware. WildFire then generates a new signature for the malware and firewalls with a Threat Prevention or WildFire subscription automatically downloads the signature to protect against future exposure. Although some file sharing web sites have an antivirus feature that checks files as they are uploaded, they can only protect against known malware.



This example uses a web site that uses SSL encryption. In this case, the firewall has decryption (PAN-OS 9.1, 10.0, 10.1, 10.2) enabled, including the option to forward decrypted content for analysis.

- STEP 1 |** The sales person from the partner company uploads a sales tool file named sales-tool.exe to his Dropbox account and then sends an email to the Palo Alto Networks sales person with a link to the file.
- STEP 2 |** The Palo Alto sales person receives the email from the sales partner and clicks the download link, which takes her to the Dropbox site. She then clicks **Download** to save the file to her desktop.
- STEP 3 |** The firewall that is protecting the Palo Alto sales rep has a WildFire Analysis profile rule attached to a security policy rule that will look for files in any application that is used to download or upload any of the supported file types. The firewall can also be configured to forward the email-link file type, which enables the firewall to extract HTTP/HTTPS links contained in SMTP and POP3 email messages. As soon as the sales rep clicks download, the firewall forwards the sales-toole.exe file to WildFire, where the file is analyzed for zero-day malware. Even though the sales rep is using Dropbox, which is SSL encrypted, the firewall is configured to decrypt traffic, so all traffic can be inspected. The following screen shots show the WildFire Analysis profile rule, the security policy rule configured with the WildFire

analysis profile rule attached, and the option to allow forwarding of decrypted content enabled.



STEP 4 | At this point, WildFire has received the file and is analyzing it for more than 200 different malicious behaviors.

STEP 5 | After WildFire has completed the file analysis, it sends a WildFire log back to the firewall with the analysis results. In this example, the WildFire log shows that the file is malicious.

RECEIVE TIME	FILE NAME	URL	SOURCE ZONE	DESTINA... ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	DEST... PORT	APPLICATION	RULE	VERDICT
08/27 11:53:35	malicious.exe											dropbox	Wildfire Rule	malicious

STEP 6 | The firewall is configured with a log forwarding profile that will send WildFire alerts to the security administrator when malware is discovered.

<input type="checkbox"/>	NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
<input type="checkbox"/>	WildFire-Forwarding			threat	(severity eq critical)			WildFire-Forwarding				
				wildfire	(category eq benign)	<input type="checkbox"/>						
				wildfire	(category neq benign) and (category neq malicious)			WildFire-Forwarding				
				wildfire	(category eq malicious)	<input type="checkbox"/>		WildFire-Forwarding				

STEP 7 | The security administrator identifies the user by name (if User-ID is configured), or by IP address if User-ID is not enabled. At this point, the administrator can shut down the network or VPN connection that the sales representative is using and will then contact the desktop support group to work with the user to check and clean the system.

By using the WildFire detailed analysis report, the desktop support person can determine if the user system is infected with malware by looking at the files, processes, and registry information detailed in the WildFire analysis report. If the user runs the malware, the support person can attempt to clean the system manually or re-image it.

FILE INFORMATION

File Type	PE
File Signer	
SHA-256	721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77
SHA-1	2e8a6dd285f8fa829918aae60cb1b6172d918437
MD5	c67fdb7887368e41469a1a2556ac30df
File Size	55296 bytes
First Seen Timestamp	2016-12-13 18:39:45 UTC
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

File Source	
File Destination	
User-ID	
Timestamp	2016-12-13 18:39:45 UTC
Serial Number	Manual
Firewall Hostname/IP	
Virtual System	
Application	
URL	
File Name	wildfire-test-pe-file (3).exe
Status	

COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit [VirusTotal](#)

STEP 8 | Now that the administrator has identified the malware and the user system is being checked, how do you protect from future exposure? Answer: In this example, the administrator set


a schedule on the firewall to download and install WildFire signatures every 15 minutes and to download and install Antivirus updates once per day. In less than an hour and a half after the sales rep downloaded the infected file, WildFire identified the zero-day malware, generated a signature, added it to the WildFire update signature database provided by Palo Alto Networks, and the firewall downloaded and installed the new signature. This firewall and any other Palo Alto Networks firewall configured to download WildFire and antivirus signatures is now protected against this newly discovered malware. The following screenshot shows the WildFire update schedule:

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Last checked: 2020/09/30 11:03:09 PDT Schedule: Every hour (Download and Install)										
3961-4425	panup-all-antivirus-3961-4425.candidate		Full	101 MB	860ee6ee9892...	2020/09/25 11:27:18 PDT			Download	Release Notes
3962-4426	panup-all-antivirus-3962-4426.candidate		Full	102 MB	fa0deabe07a8...	2020/09/26 11:27:23 PDT			Download	Release Notes
3963-4427	panup-all-antivirus-3963-4427.candidate		Full	102 MB	116fa5e5c7b5...	2020/09/27 11:26:25 PDT			Download	Release Notes
3964-4428	panup-all-antivirus-3964-4428.candidate		Full	102 MB	a9c10272b4fd...	2020/09/28 11:27:06 PDT	✓ previously		Revert	Release Notes
3965-4429	panup-all-antivirus-3965-4429.candidate		Full	102 MB	710a823e484...	2020/09/29 11:28:38 PDT	✓	✓		Release Notes
Last checked: 2020/09/30 11:05:09 PDT Schedule: Every hour at 5 minutes past the hour (Download and Install)										
8323-6320	panupv2-all-contents-	Apps, Threats	Full	57 MB	7b4f370d6bd...	2020/09/18 11:26:06 PDT			Download	Release Notes

All of this occurs well before most antivirus vendors are even aware of the zero-day malware. In this example, within a very short period of time, the malware is no longer considered zero-day because Palo Alto Networks has already discovered it and has provided protection to customers to prevent future exposure.

Get Started with WildFire

The following steps provide a quick workflow to get started with WildFire™. If you'd like to learn more about WildFire before getting started, take a look at the [WildFire Overview](#) and review the [WildFire Best Practices](#).

- STEP 1 |** Get your [WildFire Subscription](#). If you do not have a WildFire subscription, you can still forward PEs for WildFire analysis (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).
- STEP 2 |** Decide which of the [WildFire Deployments](#) works for you:
- WildFire Public Cloud—Forward samples to a Palo Alto Networks-hosted WildFire public cloud.
 - WildFire U.S. Government cloud—Forward samples to a Palo Alto Networks-hosted WildFire U.S. Government cloud.
 - WildFire Private Cloud—(Requires a WildFire appliance) Forward samples to a local WildFire appliance that resides on your network.
 - WildFire Hybrid Cloud—(Requires a WildFire appliance) Forward some samples to the WildFire public cloud and some samples to a WildFire private cloud.
- STEP 3 |** (WildFire private and hybrid cloud only) Set up and manage a WildFire appliance (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)), including upgrading the WildFire appliance (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) to the latest release version. Firewalls connected to the appliance must be running the same release version.
- STEP 4 |** Confirm your WildFire license is active on the firewall.
1. Log in to the firewall.
 2. Select **Device** > **Licenses** and check that the WildFire License is active.
- If the WildFire License is not displayed, select one of the License Management options to activate the license.
- STEP 5 |** Connect the firewall to WildFire and configure WildFire settings.
1. Select **Device** > **Setup** > **WildFire** and edit General Settings.
 2. Use the **WildFire Private Cloud** and **WildFire Public Cloud** fields to specify the WildFire deployments to which you want to forward samples (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).
 3. Define the size limits for files the firewall forwards and configure WildFire logging and reporting settings (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).
-  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.
4. Click **OK** to save the WildFire General Settings.

STEP 6 | Enable the firewall to forward decrypted SSL traffic for WildFire analysis (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).



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

STEP 7 | Start submitting samples for WildFire analysis.

1. Define traffic to forward for WildFire analysis (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)). (Select **Objects > Security Profiles > WildFire Analysis** and modify or **Add** a WildFire Analysis profile).



*As a best practice, use the WildFire Analysis default profile to ensure complete WildFire coverage for traffic the firewall allows. If you still decide to create a custom WildFire Analysis profile, set the profile to forward **Any** file type—this enables the firewall to automatically start forwarding newly-supported file types for analysis.*

2. For each profile rule, set the [WildFire Deployments Destination](#) to which you want the firewall to forward samples for analysis—**public-cloud** or the **private-cloud**.
3. Attach the WildFire analysis profile to a security policy rule (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)). Traffic matched to the policy rule is forwarded for WildFire analysis (**Policies > Security** and **Add** or modify a security policy rule).

STEP 8 | Enable the firewall to get the latest WildFire signatures.

New WildFire signatures are retrieved in real-time to detect and identify malware. If you are operating PAN-OS 9.1 or earlier, you can receive new signatures every five minutes.

- PAN-OS 9.1 and earlier
 1. Select **Device > Dynamic Updates**:
 - ([WildFire public and hybrid cloud](#)) Check that **WildFire** updates are displayed.
 - ([WildFire private and hybrid cloud](#)) Check that **WF-Private** updates are displayed. For the firewall to receive signatures from a WildFire appliance, you must enable the

WildFire appliance to locally generate signature and URL categories (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).

- Select **Check Now** to retrieve the latest signature update packages.
2. Set the **Schedule** to download and install the latest WildFire signatures.
 3. Use the **Recurrence** field to set the frequency at which the firewall checks for new updates to **Every Minute**.



As new WildFire signatures are available every five minutes, this setting ensures the firewall retrieves these signatures within a minute of availability.

4. Enable the firewall to **Download and Install** these updates as the firewall retrieves them.
 5. Click **OK**.
- PAN-OS 10.0 and later
 1. Select **Device > Dynamic Updates**:
 2. Check that the **WildFire** updates are displayed.
 3. Select **Schedule** to configure the update frequency and then use the **Recurrence** field to configure the firewall to retrieve WildFire signatures in **Real-time**.
 4. Click **OK**.

STEP 9 | Start scanning traffic for threats (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)), including malware that WildFire identifies.

Attach the **default** Antivirus profile to a security policy rule to scan traffic the rules allows based on WildFire antivirus signatures (select **Policies > Security** and add or a modify the defined **Actions** for a rule).

STEP 10 | Control site access to web sites where WildFire has identified the associated link as malicious or phishing.



This option requires a PAN-DB URL Filtering license. Learn more about URL Filtering (PAN-OS 9.1, 10.0, 10.1, 10.2) and how it enables you to control web site access and corporate credential submissions (to prevent phishing attempts) based on URL category.

To configure URL Filtering (PAN-OS 9.1, 10.0, 10.1, 10.2):

1. Select **Objects > Security Profiles > URL Filtering** and **Add** or modify a URL Filtering profile.
2. Select **Categories** and define **Site Access** for the phishing and malicious URL categories.
3. **Block** users from accessing sites in these categories altogether, or instead, allow access but generate an **Alert** when users access sites in these categories, to ensure you have visibility into such events.
4. Enable credential phishing prevention (PAN-OS 9.1, 10.0, 10.1, 10.2) to stop users from submitting credentials to untrusted sites, without blocking their access to these sites.
5. Apply the new or updated URL Filtering profile, and attach it to a security policy rule to apply the profile settings to allowed traffic:
 1. Select **Policies > Security** and **Add** or modify a security policy rule.
 2. Select **Actions** and in the Profile Setting section, set the **Profile Type** to profiles.
 3. Attach the new or updated **URL Filtering** profile to the security policy rule.
 4. Click **OK** to save the security policy rule.

STEP 11 | Confirm that the firewall is successfully forwarding samples.

- If you enabled logging of benign files, select **Monitor > WildFire Submissions** and check that entries are being logged for benign files submitted to WildFire. (If you'd like to disable logging of benign files after confirming that the firewall is connected to WildFire, select **Device > Setup > WildFire** and clear **Report Benign Files**).
- Other options to allow you to confirm that the firewall forwarded a specific sample, view samples the firewall forwards according to file type, and to view the total number of samples the firewall forwards.
- Test a sample malware file (PAN-OS 9.1, 10.0, 10.1, 10.2) to test your complete WildFire configuration.

STEP 12 | Investigate WildFire analysis results.

- Find WildFire analysis results:
 - Use the firewall to monitor malware (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) and view WildFire analysis reports for a sample.
 - View reports on the WildFire portal (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) for all samples submitted to the WildFire public cloud, including samples that you manually submitted to the WildFire public cloud.
 - Use the WildFire API to retrieve sample verdicts and reports from a WildFire appliance.
- Assess the risk of malware you find on your network with the [AutoFocus](#) threat intelligence portal. AutoFocus layers data from global WildFire submissions with statistics to identify pervasive and targeted malware, both on your network, within our industry, and globally.

STEP 13 | Next step:

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

WildFire Deployment Best Practices

The following topics describe deployments and configurations that Palo Alto Networks recommends when you are using WildFire[®] hardware or services as part of your network threat detection and prevention solution.

- > [WildFire Best Practices](#)

WildFire Best Practices

- ❑ Follow the best practices (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) to secure your network from Layer 4 and Layer 7 evasions to ensure reliable content identification and analysis. Specifically, make sure that you implement the best practices for TCP settings (**Device > Setup > Session > TCP Settings**) and Content-ID™ settings (**Device > Setup > Content-ID > Content-ID Settings**).
- ❑ Also make sure that you have an active Threat Prevention subscription (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)). Together, WildFire® and Threat Prevention enable comprehensive threat detection and prevention.
- ❑ Download and install content updates (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) on a daily basis to receive the latest product updates and threat protections generated by Palo Alto Networks. Review the instructions for installing content and software updates (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) for more information about what is included in the update packages.
- ❑ If you are running PAN-OS 10.0 or later, [configure your firewall to retrieve WildFire signatures in real-time](#). This provides access to newly-discovered malware signatures as soon as the WildFire public cloud can generate them, thereby preventing successful attacks by minimizing your exposure time to malicious activity.
- ❑ If you configured your firewall to decrypt SSL traffic (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)), then enable the firewall to *Forward Decrypted SSL Traffic for WildFire Analysis* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)). Only a superuser can enable this option.
- ❑ Use the default WildFire Analysis profile to define the traffic that the firewall should forward for WildFire analysis (**Objects > Security Profiles > WildFire Analysis**). The default WildFire Analysis profile ensures complete WildFire coverage for all traffic that your Security policy allows—it specifies that all supported file types across all applications are forwarded for WildFire analysis regardless whether the files are uploaded or downloaded.

If you choose to create a custom WildFire Analysis profile, it is a best practice to still set the profile to forward **any** file type. This enables the firewall to automatically begin forwarding file types as they become supported for WildFire analysis.

For details on applying a WildFire Analysis profile to firewall traffic, review how to *Forward Files for WildFire Analysis* (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)).



*WildFire Action settings in the Antivirus profile may impact traffic if the traffic generates a WildFire signature that results in a reset or a drop action. You can exclude internal traffic, such as software distribution applications through which you deploy custom-built programs, to transition safely (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)) to best practices because WildFire may identify custom-built programs as malicious and generate a signature for them. Check **Monitor > Logs > WildFire Submissions** to see if any internal custom-built programs trigger WildFire signatures.*

- ❑ While you are configuring the firewall to forward files for WildFire analysis (PAN-OS [9.1](#), [10.0](#), [10.1](#), [10.2](#)), review the file **Size Limit** for all supported file types. Set the **Size Limit** for all file types to the default limits. (Select **Device > Setup > WildFire** and edit the General Settings to

adjust file size limits based on file type. You can view the Help information to find the default size limit for each file type).

About the Default File Size Limits for WildFire Forwarding

The default file size limits on the firewall are designed to include the majority of malware in the wild (which is smaller than the default size limits) and to exclude large files that are very unlikely to be malicious and that can impact WildFire file-forwarding capacity. Because the firewall has a specific capacity reserved to forward files for WildFire analysis, forwarding high numbers of large files can cause the firewall to skip forwarding of some files. This condition occurs when the maximum file size limits are configured for a file type that is traversing the firewall at a high rate. In this case, a potentially malicious file might not get forwarded for WildFire analysis. Consider this possible condition if you would like to increase the size limit for files other than PEs beyond their default size limit.

The following graph is a representative illustration of the distribution of file sizes for malware as observed by the Palo Alto Networks threat research team. You can increase the firewall default file size settings to the maximum file size setting to gain a relatively small increase in the malware catch rate for each file type.

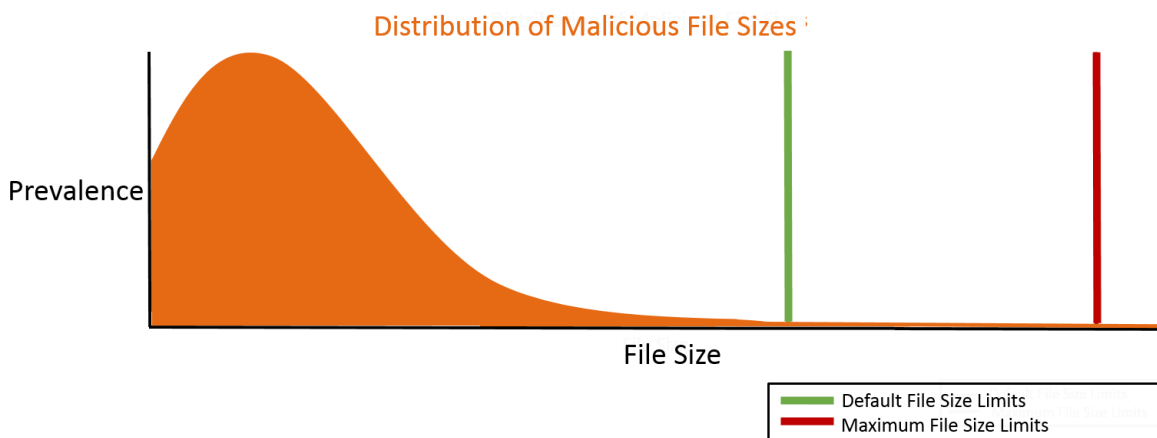


Figure 3: Recommended File Size Limits to Catch Uncommonly Large Malicious Files

If you are concerned specifically about uncommonly large malicious files, then you can increase file size limits beyond the default settings. In these cases, the following settings are recommended to catch rare, very large malicious files.

Select **Device > Setup > WildFire** and edit General Settings to adjust the **Size Limit** for each file type:

File Type	PAN-OS 9.0 and later File-Forwarding Maximum Size Recommendations	PAN-OS 8.1 File-Forwarding Maximum Size Recommendations
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1,000KB

File Type	PAN-OS 9.0 and later File-Forwarding Maximum Size Recommendations	PAN-OS 8.1 File-Forwarding Maximum Size Recommendations
ms-office	16,384KB	2,000KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
linux	50MB	10MB
script	20KB	20KB

Submit Files for WildFire Analysis

The following topics describe how to submit files for WildFire™ analysis. You can set up Palo Alto Networks firewalls to automatically forward unknown files to the WildFire public cloud or a WildFire private cloud, and you can also manually submit files for analysis using the WildFire portal. Samples submitted for WildFire analysis receive a verdict of benign, grayware, malicious, or phishing, and a detailed analysis report is generated for each sample.

- > [Forward Files for WildFire Analysis](#)
- > [Forward Decrypted SSL Traffic for WildFire Analysis](#)
- > [Verify WildFire Submissions](#)
- > [Manually Upload Files to the WildFire Portal](#)
- > [Submit Malware or Reports from the WildFire Appliance](#)
- > [Sample Removal Request](#)
- > [Firewall File Forwarding Capacity by Model](#)

Forward Files for WildFire Analysis

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 cloud (use the public cloud or a private cloud), 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.

If you are using a WildFire appliance to host a WildFire private cloud, 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 deployments** to which you want to forward samples.

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



The WildFire U.S. Government Cloud is only available to U.S. Federal agencies as an optional analysis environment.

WildFire Public 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**
2. Make sure the **WildFire Private Cloud** field is clear.

WildFire U.S. Government Cloud:

1. Enter the **WildFire U.S. Government Cloud URL**: `wildfire.gov.paloaltonetworks.com`
2. Make sure the **WildFire Private Cloud** field is clear.

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**
2. Enter the **WildFire U.S. Government Cloud URL**:

- U.S. Government Cloud: **wildfire.gov.paloaltonetworks.com**
3. 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.

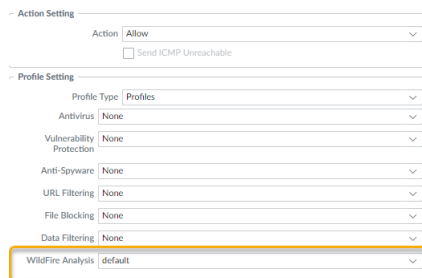
Confirm that all WildFire appliances processes are running by running the following command:

```
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 | Choose what to do next...

- [Verify WildFire Submissions](#) to confirm that the firewall is successfully forwarding files for WildFire analysis.
- ([WildFire Private Cloud Only](#)) [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 Activity](#) to assess alerts and details reported for malware.

Forward Decrypted SSL Traffic for WildFire Analysis

Enable the firewall to forward decrypted SSL traffic for WildFire analysis. Traffic that the firewall decrypts is evaluated against security policy rules; if it matches the WildFire analysis profile attached to the security rule, the decrypted traffic is forwarded for WildFire analysis before the firewall re-encrypts it. Only a super user can enable this option.



Forwarding decrypted SSL traffic for WildFire analysis is a [WildFire best practice](#).

- On a firewall that does not have multiple virtual systems enabled:
 1. If you have not already, enable the firewall to perform [decryption](#) and [Forward Files for WildFire Analysis](#).
 2. Select **Device > Setup > Content-ID**.
 3. Edit the Content-ID settings and **Allow Forwarding of Decrypted Content**.
 4. Click **OK** to save the changes.

- On a firewall with virtual systems enabled:
 1. If you have not already, enable [decryption](#) and [Forward Files for WildFire Analysis](#).
 2. Select **Device > Virtual Systems**, click the virtual system you want to modify, and **Allow Forwarding of Decrypted Content**.

Verify WildFire Submissions

Test your WildFire setup using malware test samples, and also verify that the firewall is correctly forwarding files for WildFire analysis.

- [Test a Sample Malware File](#)
- [Verify File Forwarding](#)

Test a Sample Malware File

Palo Alto Networks provides sample malware files that you can use to test a WildFire configuration. Take the following steps to download the malware sample file, verify that the file is forwarded for WildFire analysis, and view the analysis results.

STEP 1 | Download one of the malware test files. You can select from PE, APK, MacOSX, and ELF.



*Before downloading an encrypted WildFire sample malware file, you must temporarily disable the *.wildfire.paloaltonetworks.com entry from the exclude from decryption list on the **Device > Certificate Management > SSL Decryption Exclusion** page, otherwise the sample will not download correctly. After conducting a verification test, be sure to re-enable the *.wildfire.paloaltonetworks.com entry on the SSL decryption exclusion page.*

- If you have SSL decryption enabled on the firewall, use one of the following URLs:
 - PE—<https://wildfire.paloaltonetworks.com/publicapi/test/pe>
 - APK—<https://wildfire.paloaltonetworks.com/publicapi/test/apk>
 - MacOSX—<https://wildfire.paloaltonetworks.com/publicapi/test/macos>
 - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf
- If you do *not* have SSL decryption enabled on the firewall, use one of the following URLs instead:
 - PE—<http://wildfire.paloaltonetworks.com/publicapi/test/pe>
 - APK—<http://wildfire.paloaltonetworks.com/publicapi/test/apk>
 - MacOSX—<http://wildfire.paloaltonetworks.com/publicapi/test/macos>
 - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf

The test file is named `wildfire-test-file_type-file.exe` and each test file has a unique SHA-256 hash value.



You can also use the WildFire API to retrieve a malware test file. See the [WildFire API Reference](#) for details.

STEP 2 | On the firewall web interface, select **Monitor > WildFire Submissions** to confirm that the file was forwarded for analysis.

Please wait at least five minutes for analysis results to be displayed for the file on the **WildFire Submissions** page. The verdict for the test file will always display as malware.

Verify File Forwarding

After the firewall is set up to [Forward Files for WildFire Analysis](#), use the following options to verify the connection between the firewall and the WildFire public or private cloud, and to monitor file forwarding.



Several of the options to verify that a firewall is forwarding samples for WildFire analysis are CLI commands; for details on getting started with and using the CLI, refer to the [PAN-OS CLI Quick Start Guide](#).

- Verify the status of the firewall connection to the WildFire public and/or private cloud, including the total number of files forwarded by the firewall for analysis.

Use the **show wildfire status** command to:

- Check the status of the WildFire public and/or private cloud to which the firewall is connected. The status **Idle** indicates that the WildFire cloud (public or private) is ready to receive files for analysis.
- Confirm the configured size limits for files forwarded by the firewall (**Device > Setup > WildFire**).
- Monitor file forwarding, including how the total count of files forwarded by the firewall for WildFire analysis. If the firewall is in a WildFire hybrid cloud deployment, the number of files forwarded to the WildFire public cloud and the WildFire private cloud are also displayed.

The following example shows the `showwildfire status` output for a firewall in a WildFire private cloud deployment:

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:      enable
  Server selection:           enable
  File cache:                 enable

WildFire Public Cloud:
  Server address:             wildfire.paloaltonetworks.com
  Status:                     Disabled due to configuration
  Best server:
  Device registered:          no
  Through a proxy:            no
  Valid wildfire license:     yes
  Service route IP address:   X.X.X.X

WildFire Private Cloud:
  Server address:             X.X.X.X
  Status:                     Idle
  Best server:                X.X.X.X:XXXXX
  Device registered:          yes
  Through a proxy:            no
  Valid wildfire license:     yes
  Service route IP address:   X.X.X.X

File size limit info:
  pe                           9 MB
  apk                          49 MB
  pdf                          1000 KB
  ms-office                     9500 KB
  jar                           9 MB
  flash                         10 MB
  MacOSX                       1 MB

Forwarding info:
  file idle time out (second): 90
  total concurrent files:      0
  Public Cloud:
    total file forwarded:      0
    file forwarded in last minute: 0
    concurrent files:          0
  Private Cloud:
    total file forwarded:      0
    file forwarded in last minute: 0
    concurrent files:          0
```

To view forwarding information for only the WildFire public cloud or WildFire private cloud, use the following commands:

- **show wildfire status channel public**
- **show wildfire status channel private**

- View samples forwarded by the firewall according to file type (including email links).



*Use this option to confirm that email links are being forwarded for WildFire analysis, since only email links that receive a malicious or phishing verdict are logged as **WildFire Submissions** entries on the firewall, even if logging for benign and grayware samples is enabled. This is due to the sheer number of WildFire Submissions entries that would be logged for benign email links.*

Use the **show wildfire statistics** command to confirm the file types being forwarded to the WildFire public or private cloud:

- The command displays the output of a working firewall and shows counters for each file type that the firewall forwards for WildFire analysis. If a counter field shows 0, the firewall is not forwarding that file type.
 - Confirm that email links are being forwarded for analysis by checking that the following counters do not show zero:
 - **FWD_CNT_APPENDED_BATCH**—Indicates the number of email links added to a batch waiting for upload to WildFire.
 - **FWD_CNT_LOCAL_FILE**— Indicates the total number of email links uploaded to WildFire.
- Verify that a specific sample was forwarded by the firewall and check that status of that sample.



This option can be helpful when troubleshooting to:

- Confirm that samples that have not yet received a WildFire verdict were correctly forwarded by the firewall. Because **WildFire Submissions** are logged on the firewall only when WildFire analysis is complete and the sample has received a WildFire verdict, use

this option to verify the firewall forwarded a sample that is currently undergoing WildFire analysis.

- Track the status for a single file or email link that was allowed according to your security policy, matched to a WildFire Analysis profile, and then forwarded for WildFire analysis.
- Check that a firewall in a **hybrid cloud** deployment is forwarding the correct file types and email links to either the WildFire public cloud or a WildFire private cloud.

Execute the following CLI commands on the firewall to view samples the firewall has forwarded WildFire analysis:

- View all samples forwarded by the firewall with the CLI command **debug wildfire upload-log**.
- View only samples forwarded to the WildFire public cloud with the CLI command **debug wildfire upload-log channel public**.
- View only samples forwarded to the WildFire private cloud with the CLI command **debug wildfire upload-log channel private**.

The following example shows the output for the three commands listed above when issued on a firewall in a WildFire public cloud deployment:

```
user@firewall> debug wildfire upload-log
+ channel WildFire channel (Public/Private)
  | Pipe through a command
  <Enter> Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:

user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

log: 0, filename: support-login.swf
processed 353590 seconds ago, action: skipped - remote benign dup
vsys_id: 1, session_id: 169651, transaction_id: 261
file_len: 91536, flag: 0x81c, file type: flash
threat id: 52145, user id: 1238, app id: 872
from XX.XX.XX.XX/XXXXX to XX.XXX.XXX.XXX/XXX
SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
processed 611505 seconds ago, action: skipped - remote benign dup
vsys_id: 1, session_id: 259049, transaction_id: 260
file_len: 39206, flag: 0x81c, file type: flash
threat id: 52145, user id: 20583, app id: 872
from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

- Monitor samples successfully submitted for WildFire analysis.

Using the firewall web interface, select **Monitor > Logs > WildFire Submissions**. All files forwarded by a firewall to the WildFire public or private cloud for analysis are logged on the WildFire Submissions page.

- Check the WildFire verdict for a sample:

By default, only samples that receive malicious or phishing verdicts are displayed as **WildFire Submissions** entries. To enable logging for benign and/or grayware samples, select **Device > Setup > WildFire > Report Benign Files/ Report Grayware Files**.



*Enable logging for benign files as a quick troubleshooting step to verify that the firewall is forwarding files. Check the **WildFire Submissions** logs to verify that files are being submitted for analysis and receiving WildFire verdicts (in this case, a benign verdict).*

- Confirm the analysis location for a sample:

The **WildFire Cloud** column displays the location to which the file was forwarded and where it was analyzed (public cloud or private cloud). This is useful when deploying a [hybrid cloud](#).

Manually Upload Files to the WildFire Portal

All Palo Alto Networks customers with a support account can use the Palo Alto Networks [WildFire portal](#) to manually submit up to five samples a day for WildFire analysis. If you have a WildFire subscription, you can manually submit samples to the portal as part of your 1000 sample uploads daily limit; however, keep in mind that the 1000 sample daily limit also includes WildFire API submissions.

STEP 1 | Manually upload files or URLs to the WildFire portal for analysis.

1. Log in to the [WildFire Portal](#).
2. Click **Upload Sample** on the menu bar.
 - To submit files for analysis, select **File Upload** and **Open** the files you want to submit for WildFire analysis. Click **Start** to begin WildFire analysis of a single file, or click **Start Upload** to submit all the files you added for WildFire analysis.
 - To submit a URL for analysis, click **URL Upload**, enter a URL, and **Submit** for WildFire analysis.

The screenshot shows the WildFire portal interface. At the top, there is a navigation bar with 'Dashboard', 'Reports', 'Upload Sample', 'Settings', 'Account', and 'Kim, Howard'. The main heading is 'UPLOAD SAMPLE'. There are two tabs: 'File Upload' (selected) and 'URL Upload'. Below the tabs, there is a section for uploading files, including instructions and a list of supported file formats. Three buttons are visible: '+ Add files...', 'Start upload', and 'Cancel upload'. The 'Start upload' button is circled in orange. Below the buttons is a table showing two uploaded files, both with 'Success' status, also circled in orange.

6.1-cloud-report-Beta-b057cad21f57a4f66680b5622eeb9410bbe8ed36a8d698117f3ccf7f517e823d.pdf	90.9 KB	Success	Adobe PDF document
PA-3000-Hardware_Guide.pdf	961.5 KB	Success	Adobe PDF document

3. Close the **Uploaded File Information** pop-up.

STEP 2 | View the WildFire verdict and analysis results for the file.

Please wait at least five minutes for WildFire to analyze the sample.



Because a manual upload is not associated with a specific firewall, manual uploads do not show session information in the reports.

1. Return to the [WildFire Portal](#) dashboard.
2. In the Previous 1 Hour section, select **Manual** under the source column to view analysis information for the latest manually-submitted samples.
3. Find the files or URLs you uploaded and click the detail icon to the left of the Received Time.

Submit Malware or Reports from the WildFire Appliance

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.

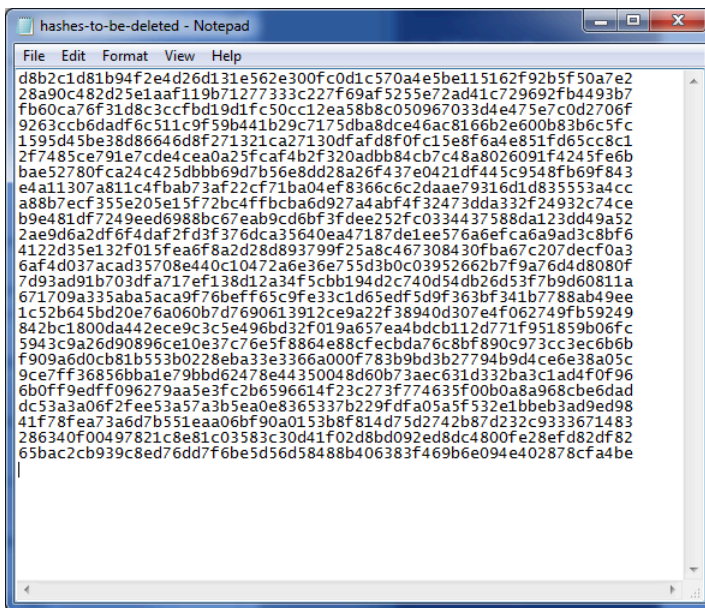
Sample Removal Request

Unique samples sent to the WildFire cloud for analysis can be deleted at the discretion of the user. This allows users who are subject to data protection policies, including those who must comply with GDPR, to permanently dispose of sample data based on their organization's retention policies. Sample data includes session / upload data and the sample file itself.

STEP 1 | Create a text file with a list of SHA256 or MD5 hashes of the samples to be deleted. Each hash must be on an individual line in the file and can include up to 100 samples.



Only files that are unique to your environment can be deleted. If files are found to be available in other public or private feeds, only the session and upload data for a given account is removed.



STEP 2 | Log in to the WildFire cloud using your Palo Alto Networks support credentials or your WildFire account.

STEP 3 | Select **Settings** on the menu bar.

STEP 4 | Click **Choose File** and select the hash list text file that you created in step 1 and then **Remove Samples**. You will receive a confirmation upon a successful file upload.

SETTINGS

Remove samples, update the default timezone, clear logs, and change notification settings.

Remove Samples No file chosen

STEP 5 | After the samples are removed from the WildFire cloud, you will receive a confirmation email with the details of the request. This includes a list of the samples that were requested to be deleted, and the removal status of each sample. This process can take up to 7 days.

Dear wildFire customer,
your request for removal of samples from wildFire cloud has been completed. In total 1 samples were removed from wildFire, the following table shows removal status for each individual sample hash

Hash	Status	Information
6d2ef9f79b5b81429cb1ffeed6b2919a9a84ec0cc0e5023cbf45a68967c6e1c	Deleted	



*Samples that do not exist or are not unique to your environment will return statuses of **Not found** and **Rejected**, respectively.*

Firewall File-Forwarding Capacity by Model

File-forwarding capacity is the maximum rate per minute at which each Palo Alto Networks firewall model can submit files to the WildFire® cloud or to a WildFire appliance for analysis. If the firewall reaches the per-minute limit, it queues any remaining samples.

The Reserved Drive Space in the following table represents the amount of drive space on the firewall that is reserved for queuing files. If the firewall reaches the drive space limit, it cancels forwarding of new files to WildFire until more space in the queue is available.



The speed at which the firewall can forward files to WildFire also depends on the bandwidth of the upload link from the firewall.

Platform	Maximum Files Per Minute	Reserved Drive Space
VM-50	5	100MB
VM-100	10	100MB
VM-200	15	200MB
VM-300	25	200MB
VM-500	30	250MB
VM-700	40	250MB
PA-220	20	100MB
PA-400	20	100MB
PA-820	75	300MB
PA-850	75	300MB
PA-3220	100	200MB
PA-3250/3260	100	500MB
PA-5200 Series	250	1500MB
PA-5450	250	1500MB
PA-7000 Series	300	1GB

Set Up and Manage a WildFire Appliance

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](#)
- > [Upgrade a WildFire Appliance](#)

About the WildFire Appliance

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.

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 Appliance Interfaces

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.

Configure the WildFire Appliance

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 | (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 12 | (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 13 | (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 14 | (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 15 | (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 16 | (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 17 | 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>
```

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

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

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

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 on 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


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

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.

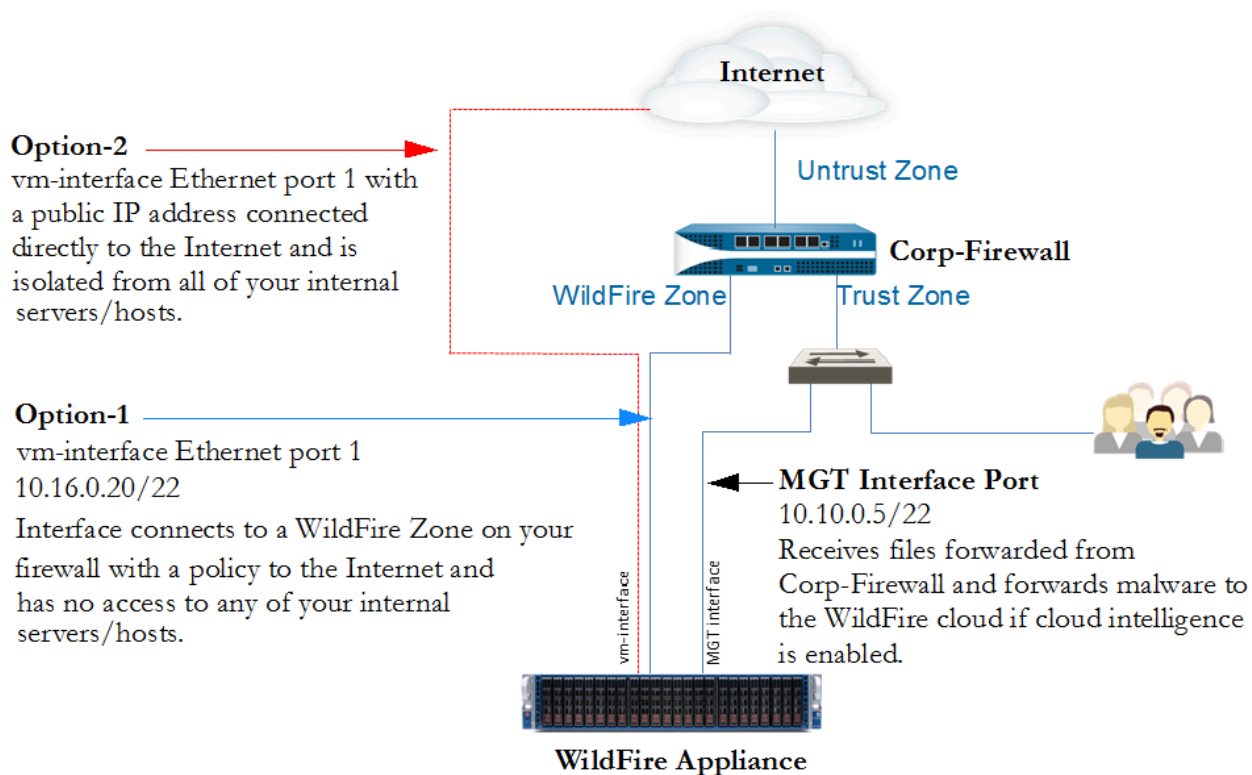


Figure 4: Virtual Machine Interface Example

- **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

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

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

- [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

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

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

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

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

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 `Submit report` fields.

Upgrade a WildFire Appliance

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.

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.

These updates equip the appliance with the latest threat information to accurately detect malware.

```
admin@WF-500> request
wf-content upgrade install version 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](#).

STEP 4 | Download the PAN-OS 10.1 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 10.1. Replace 10.1 with the appropriate target release for your upgrade.

Download the 10.1 software version:

- Direct Internet Connectivity:

1.

```
admin@WF-500>
request system software download version 10.1
```

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-10.1.0
```

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

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

STEP 5 | Confirm that all services are running.

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

STEP 6 | Install the 10.1 software version.

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

system software install version 10.1.0

STEP 7 | 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 8 | Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the `sw-version` field shows 10.1:

```
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 9 | (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.

- View the active virtual machine image by running the following command and refer to the `SelectedVM` 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 10 | Next steps:

- (Optional) Upgrade firewalls to PAN-OS 10.1. See the [firewall upgrade instructions](#) included in the PAN-OS 10.1 New Features Guide. Firewalls running release versions earlier than PAN-OS 10.0 can still continue to forward samples to a WildFire appliance running 10.1.
- (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.

Monitor WildFire Activity

Depending on your WildFire™ deployment—public, private, or hybrid—you can view samples submitted to WildFire and analysis results for each sample using the [WildFire portal](#), 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 Firewall to Monitor Malware](#)
- > [Use the WildFire Portal to Monitor Malware](#)
- > [Use the WildFire CLI to Monitor the WildFire Appliance](#)
- > [WildFire Analysis Reports—Close Up](#)

The [AutoFocus threat intelligence portal](#) provides a different lens through which to view WildFire analysis details for a sample. AutoFocus layers statistics over WildFire analysis data to indicate high-risk artifacts found during sample analysis (such as an IP address or a domain).

About WildFire Logs and Reporting

You can [Monitor WildFire Activity](#) 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 Firewall to Monitor Malware

Samples forwarded by the firewall 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.

- [Configure WildFire Submissions Log Settings](#)
- [Monitor WildFire Submissions and Analysis Reports](#)
- [Set Up Alerts for Malware](#)

Configure WildFire Submissions Log Settings

Enable the following options for **WildFire Submissions** logs:

- [Enable Logging for Benign and Grayware Samples](#)
- [Include Email Header Information in WildFire Logs and Reports](#)

Enable Logging for Benign and Grayware Samples

Logging for benign and grayware samples is disabled by default. Email links that receive benign or grayware verdicts are not logged.

STEP 1 | Select **Device > Setup > WildFire**, edit **General Settings**.

STEP 2 | Select **Report Benign Files** and/or **Report Grayware Files** and click **OK** to save the settings.

Include Email Header Information in WildFire Logs and Reports

Use the following steps to include email header information—email sender, recipient(s), and subject—in WildFire logs and reports.

Session information is forwarded to the WildFire cloud along with the sample, and used to generate the WildFire analysis report. Neither the firewall nor the WildFire cloud receive, store, or view actual email contents.



Session information can help you to quickly track down and remediate threats detected in email attachments or links, including how to identify recipients who have downloaded or accessed malicious content.

STEP 1 | Select **Device > Setup > WildFire**.

STEP 2 | Edit the Session Information Settings section and enable one or more of the options (**Email sender**, **Email recipient**, and **Email subject**).

STEP 3 | Click **OK** to save.

Monitor WildFire Submissions and Analysis Reports

Samples that firewalls submit for WildFire analysis are displayed as entries in the **WildFire Submissions** log on the firewall web interface. For each WildFire entry, you can open an expanded log view which displays log details and the WildFire analysis report for the sample.



Mozilla Firefox users: The WildFire Analysis Report displays correctly only in Firefox v54 and earlier releases. If you experience issues viewing the report, consider using a different web browser such as Google Chrome. Alternatively, you can download and open the PDF version or view the report through the WildFire portal.

STEP 1 | [Forward Files for WildFire Analysis.](#)

STEP 2 | [Configure WildFire Submissions Log Settings.](#)

STEP 3 | To view samples submitted by a firewall to a WildFire public, private, or hybrid cloud, select **Monitor > Logs > WildFire Submissions**. When WildFire analysis of a sample is complete, the results are sent back to the firewall that submitted the sample and are accessible in the WildFire Submissions logs. The submission logs include details about a given sample, including the following information:

- The Verdict column indicates whether the sample is benign, malicious, phishing, or grayware.
- The Action column indicates whether the firewall allowed or blocked the sample.
- The Severity column indicates how much of a threat a sample poses to an organization using the following values: critical, high, medium, low, and informational.



The values for the following severity levels are determined by a combination of verdict and action values.

- *Low*—Grayware samples with the action set to allow.
- *High*—Malicious samples with the action set to allow.
- *Informational*:
 - Benign samples with the action set to allow.
 - Samples with any verdict with the action set to block.

RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	VERDICT	ACTION
08/27 11:53:35	1.png	I3-vlan-trust	I3-untrust	192.168.2.11	2.22.146.91	80	web-browsing	benign	allow
08/19 14:10:00	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.6.66	4502	web-browsing	benign	allow
08/16 15:19:08	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:13:07	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:07:08	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	I3-vlan-trust	I3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow

STEP 4 | For any entry, select the Log Details icon to open a detailed log view for each entry:

RECEIVE TIME	FILE NAME
08/27 11:53:35	1.png
08/19 14:10:00	zero-trust-best-practices.pdf
08/16 15:19:08	zero-trust-best-practices.pdf

The detailed log view displays Log Info and the WildFire Analysis Report for the entry. If the firewall has packet captures (PCAPs) enabled, the sample PCAPs are also displayed.

For all samples, the WildFire analysis report displays file and session details. For malware samples, the WildFire analysis report is extended to include details on the file attributes and behavior that indicated the file was malicious.

STEP 5 | (Optional) **Download PDF** of the WildFire Analysis Report.

Set Up Alerts for Malware

You can configure a Palo Alto Networks firewall to send an alert when WildFire identifies a malicious or phishing sample. You can configure alerts for benign and grayware files as well, but not for benign and grayware email links. This example describes how to configure an email alert; however, you could also configure [log forwarding](#) to set up alerts to be delivered as syslog messages, SNMP traps, or Panorama alerts.

STEP 1 | Configure an email server profile.


1. Select **Device > Server Profiles > Email**.
2. Click **Add** and then enter a **Name** for the profile. For example, WildFire-Email-Profile.
3. (**Optional**) Select the virtual system to which this profile applies from the **Location** drop-down.
4. Click **Add** to add a new email server entry and enter the information required to connect to the Simple Mail Transport Protocol (SMTP) server and send email (up to four email servers can be added to the profile):
 - **Server**—Name to identify the mail server (1-31 characters). This field is just a label and does not have to be the host name of an existing SMTP server.
 - **Display Name**—The name to show in the From field of the email.
 - **From**—The email address where notification emails are sent from.
 - **To**—The email address to which notification emails are sent.
 - **Additional Recipient(s)**—Enter an email address to send notifications to a second recipient.
 - **Gateway**—The IP address or host name of the SMTP gateway to use to send the emails.
5. Click **OK** to save the server profile.
6. Click **Commit** to save the changes to the running configuration.

STEP 2 | Test the email server profile.

1. Select **Monitor > PDF Reports > Email Scheduler**.
2. Click **Add** and select the new email profile from the **Email Profile** drop-down.
3. Click the **Send test email** button and a test email should be sent to the recipients defined in the email profile.

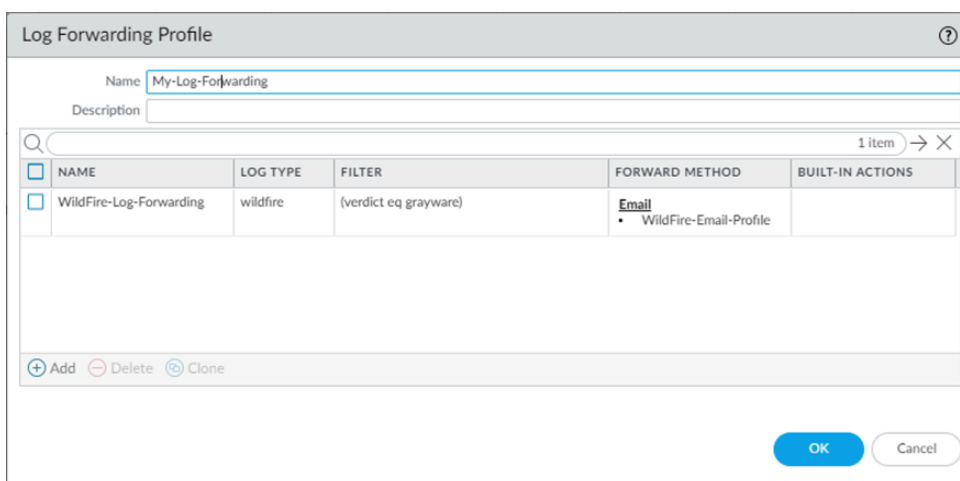
STEP 3 | Configure a log forwarding profile to enable WildFire logs to be forwarded to Panorama, an email account, SNMP, a syslog server, and as HTTP requests.

In this example you will set up email logs for when a sample is determined to be malicious. You can also enable Benign and Grayware logs to be forwarded, which will produce more activity if you are testing.

 *The firewall does not forward WildFire logs for blocked files to an email account.*

1. Select **Objects > Log Forwarding**.
2. **Add** and name the profile, for example, WildFire-Log-Forwarding. Optionally, you can add a **Description** of the log forwarding profile.
3. **Add** to configure forwarding methods.

1. Provide a name for the **Log Forwarding Profile Match List**.
2. Select the **WildFire** Log Type.
3. **Filter** the logs using **(verdict eq malicious)** query.
4. Under the **Forward Method** options, choose the Email profile that was created in step 1 (in this case, WildFire-Email-Profile), and click **OK** to save the match list updates.
4. Click **OK** again to save the Log Forwarding Profile updates.



STEP 4 | Add the log forwarding profile to a security policy being used for WildFire forwarding (with a WildFire Analysis profile attached).

The WildFire Analysis profile defines the traffic that the firewall forwards for WildFire analysis. To set up a WildFire analysis profile and attach it to a security policy rule, see [Forward Files for WildFire Analysis](#).

1. Select **Policies > Security** and click on the policy that is used for WildFire forwarding.
2. In the **Actions** tab **Log Setting** section, select the **Log Forwarding** profile you configured.
3. Click **OK** to save the changes and then **Commit** the configuration.

Use the WildFire Portal to Monitor Malware

Log in to the Palo Alto Networks [WildFire portal](#) using your Palo Alto Networks support credentials or your WildFire account. The portal opens to display the dashboard, which lists summary report information for all of the firewalls associated with the specific WildFire subscription or support account. For each device listed, the portal displays statistics for the number of malware samples that have been detected, benign samples that have been analyzed, and the number of pending files that are waiting to be analyzed. Your WildFire portal account displays data for all samples submitted by firewalls on your network that are connected to the WildFire public cloud, as well as data for samples manually submitted to the portal. Additionally, if you have [enabled a WildFire appliance to forward malware to the WildFire public cloud](#) for signature generation and distribution, reports for those malware samples can also be accessed on the portal.

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

- [Configure WildFire Portal Settings](#)
- [Add WildFire Portal Users](#)
- [View Reports on the WildFire Portal](#)

Configure WildFire Portal Settings

This section describes the settings that can be customized for a WildFire cloud account, such as time zone and email notifications for each firewall connected to the account. You can also delete firewall logs stored in the cloud.

STEP 1 | Access the portal settings.

1. Log in to the [WildFire cloud](#).
2. Select **Settings** on the menu bar.

STEP 2 | Configure the time zone for the WildFire cloud account.

Select a time zone from the **Set Time Zone** drop-down and **Update Time Zone** to save the change.



The time stamp that appears on WildFire analysis reports is based on the time zone configured for the WildFire cloud account.

STEP 3 | (Optional) Delete WildFire logs hosted on the cloud for specific firewalls.

1. In the **Delete WildFire Reports** drop-down, select a firewall (by serial number) and **Delete Reports** to remove logs for that firewall from WildFire portal. This action does not delete logs stored on the firewall.
2. Click **OK** to proceed with the deletion.

STEP 4 | (Optional) Configure email notifications based on WildFire analysis verdicts.



The WildFire portal does not send alerts for blocked files that the firewall forwarded for WildFire analysis.

1. In the Configure Alerts section, select **Malware**, **Phishing**, **Grayware**, and/or **Benign** check boxes to receive email notifications based on those verdicts:
 - Select the verdict check boxes in the **All** row to receive verdict notifications for all samples uploaded to the WildFire cloud.
 - Select the verdict check boxes in the **Manual** row to receive verdict notifications for all samples that are manually uploaded to the WildFire public cloud using the WildFire portal.
 - Select the verdict check boxes for one or several firewall serial numbers to receive verdict notifications for samples submitted by those firewalls.
2. Select **Update Notification** to enable verdict notifications to be emailed to the email address associated with your support account.

Add WildFire Portal Users

WildFire portal accounts are created by a super user (the registered owner of a Palo Alto Networks device) to give additional users the ability to log in to the WildFire cloud and view device data for which they are granted access by the super user. A WildFire user can be a user associated with an existing Palo Alto Networks account or a user not associated with a Palo Alto Networks support account, to whom you can allow access to just the WildFire public clouds and a specific set of firewall data.

STEP 1 | Select the account for which you want to add users who can access the WildFire portal.

WildFire portal users can view data for all firewalls associated with the support account.

1. Log in to the [Palo Alto Networks Support Portal](#).
2. Under **Manage Account**, click on **Users and Accounts**.
3. Select an existing account or sub-account.

STEP 2 | Add a WildFire user.

1. Click **Add WildFire User**.
2. Enter the email address for the user you would like to add.



The only restriction when adding a user is that the email address cannot be from a free web-based email account (such as Gmail, Hotmail, and Yahoo). If an email address is entered for a domain that is not supported, a pop-up warning is displayed.

STEP 3 | Assign firewalls to the new user account and access the WildFire cloud.

Select the firewall(s) by serial number for which you want to grant access and fill out the optional account details.

Users with an existing support account will receive an email with a list of the firewalls that are now available for WildFire report viewing. If the user does not have a support account,

the portal sends an email with instructions on how to access the portal and how to set a new password.

The new user can now log in to the [WildFire cloud](#) and view WildFire reports for the firewalls to which they have been granted access. Users can also configure automatic email alerts for these devices in order to receive alerts on files analyzed. They can choose to receive reports on malicious and/or benign files.

View Reports on the WildFire Portal

The Wildfire portal displays reports for samples that are submitted from firewalls, manually uploaded, or uploaded using the WildFire API. Select **Reports** to display the latest reports for samples analyzed by the WildFire cloud. For each sample listed, the report entry shows the date and time the sample was received by the cloud, the serial number of the firewall that submitted the file, the file name or URL, and the verdict delivered by WildFire (benign, grayware, malware, or phishing).

Use the search option to search for reports based on the file name or the sample hash value. You can also narrow the results displayed by viewing only reports for samples submitted by a specific **Source** (view only results submitted manually or by a specific firewall) or for samples that received a specific WildFire **Verdict** (any, benign, malware, grayware, phishing, or pending).

To view an individual report from the portal, click the **Reports** icon to the left of the report name. To save the detailed report, click the **Download as PDF** button on the upper right of the report page. For details on WildFire analysis reports, see [WildFire Analysis Reports—Close Up](#).

The following shows a list of sample files submitted by a specific firewall:

The screenshot shows the WildFire portal interface. At the top, there is the Palo Alto Networks logo and the WildFire logo. Below the logo is a navigation bar with options: Dashboard, Reports (selected), Upload Sample, Settings, Account, and a user profile for Ly, Jonathan. The main heading is 'REPORTS'. Below this is a search bar with the text 'Search by file name or sha256'. To the right of the search bar are two dropdown menus: 'Source' set to 'Any' and 'Verdict' set to 'Any'. There are 'Reset' and 'Search' buttons. Below the search bar is a pagination control showing 'Prev', '1', '2', '3', '4', '...', '100', 'Next', and '20'. The main content is a table with the following columns: Received Time, Source, File / URL, and Verdict. The table contains 10 rows of data, all with a 'Manual' source and a 'Benign' verdict. The first row has a 'Benign' verdict, the second row has a 'Pending' verdict, and the remaining 8 rows have a 'Benign' verdict.

Received Time	Source	File / URL	Verdict
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual	Friday, February 20, 2015 FreePassReportGroupedByCashier16.pdf	Pending
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign
2020-09-30 19:54:26	Manual		Benign

Use the WildFire Appliance to Monitor Sample Analysis Status

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

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-elinkda-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

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:

```
+-----+-----+-----+-----+
+-----+-----+-----+-----+
+-----+-----+-----+-----+
|                               SHA256
|                               |
| Create Time | File Name | 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 sha256 equal <SHA_256>
```

```
Sample
1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
last seen on following devices:
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

Device ID	Device IP	SHA256 Submitted Time
1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e	Manual	Manual 2019-08-05 19:24:39

Use the WildFire CLI to Monitor the WildFire Appliance

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

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

```

WildFire Analysis Reports—Close Up

Access WildFire analysis reports [on the firewall](#), [the WildFire portal](#), and [the WildFire API](#).



WildFire analysis reports display detailed sample information, as well as information on targeted users, email header information (if enabled), the application that delivered the file, and all URLs involved in the command-and-control activity of the file. WildFire reports contain some or all of the information described in the following table based on the session information configured on the firewall that forwarded the file and depending on the observed behavior for the file.



When viewing a WildFire report for a file that was manually uploaded to the WildFire portal or by using the WildFire API, the report will not show session information because the traffic did not traverse the firewall. For example, the report would not show the Attacker/Source and Victim/Destination.

Report Heading	Description
File Information	<ul style="list-style-type: none"> • File Type—Flash, PE, PDF, APK, JAR/Class, archive, linux, script, or MS Office. This field is named URL for HTTP/HTTPS email link reports and will display the URL that was analyzed. • File Signer—The entity that signed the file for authenticity purposes. • Hash Value—A file hash is much like a fingerprint that uniquely identifies a file to ensure that the file has not been modified in any way. The following lists the hash versions that WildFire generates for each file analyzed: <ul style="list-style-type: none"> • SHA-1—Displays the SHA-1 value for the file. • SHA-256—Displays the SHA-256 value for the file. • MD5—Displays the MD5 information for the file. • File Size—The size (in bytes) of the file that WildFire analyzed. • First Seen Timestamp—If the WildFire system has analyzed the file previously, this is the date/time that it was first observed. • Verdict—Displays analysis verdicts. • Sample File—Click the Download File link to download the sample file to your local system. Note that you can only download files with the malware verdict, not benign.
Coverage Status	<p>Click the Virus Total link to view endpoint antivirus coverage information for samples that have already been identified by other vendors. If the file has never been seen by any of the listed vendors, file not found appears.</p> <p>In addition, when the report is rendered on the firewall, up-to-date information about what signature and URL filtering coverage that Palo Alto Networks currently provides to protect against the threat</p>



Report Heading	Description
	<p>will also be displayed in this section. Because this information is retrieved dynamically, it will not appear in the PDF report.</p> <p>The following coverage information is provided for active signatures:</p> <ul style="list-style-type: none"> • Coverage Type—The type of protection provided by Palo Alto Networks (virus, DNS, WildFire, or malware URL). • Signature ID—A unique ID number assigned to each signature that Palo Alto Networks provides. • Detail—The well-known name of the virus. • Date Released—The date that Palo Alto Networks released coverage to protect against the malware. • Latest Content Version—The version number for the content release that provides protection against the malware.
Session Information	<p>Contains session information based on the traffic as it traversed the firewall that forwarded the sample. To define the session information that WildFire will include in the reports, select Device > Setup > WildFire > Session Information Settings.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • Source IP • Source Port • Destination IP • Destination Port • Virtual System (If multi-vsyst is configured on the firewall) • Application • User (If User-ID is configured on the firewall) • URL • Filename • Email sender • Email recipient • Email subject <p>By default, session information includes the field Status, which indicates if the firewall allowed or blocked the sample.</p>
Dynamic Analysis	<p>If a file is low risk and WildFire can easily determine that it is safe, only static analysis is performed on the file, instead of dynamic or bare metal analysis.</p>

Report Heading	Description
<p> Files analyzed using bare metal are shown as a virtual machine configuration under dynamic analysis.</p>	<p>When dynamic or bare metal analysis is performed, this section contains tabs showing analysis results for each environment type that the sample was run in. For example, the Virtual Machine 1 tab might show an analysis environment operating Windows XP, Adobe Reader 9.3.3, and Office 2003 and Virtual Machine 3 might have similar attributes, but running in a bare metal environment. Samples are analyzed using bare metal in addition to dynamic analysis if it displays characteristics of an advanced VM-aware threat.</p> <p> On the WildFire appliance, only one virtual machine is used for the analysis, which you select based on analysis environment attributes that best match your local environment. For example, if most users have Windows 7 32-bit, that virtual machine would be selected.</p>

Behavior Summary	Description
	<p>Each Virtual Machine tab summarizes the behavior of the sample file in the specific environment. Examples include whether the sample created or modified files, started a process, spawned new processes, modified the registry, or installed browser helper objects.</p> <p>The Severity column indicates the severity of each behavior. The severity gauge will show one bar for low severity and additional bars for higher severity levels. This information is also added to the dynamic and static analysis sections.</p>


BEHAVIORAL SUMMARY

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
<p>Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.</p>	<p></p>
<p>Deleted itself Malware often deletes itself after installation to avoid detection. Legitimate applications do not delete themselves directly.</p>	<p></p>

The following describes the various behaviors that are analyzed:

- **Network Activity**—Shows network activity performed by the sample, such as accessing other hosts on the network, DNS queries, and phone-home activity. A link is provided to download the packet capture.
- **Host Activity (by process)**—Lists activities performed on the host, such as registry keys that were set, modified, or deleted.
- **Process Activity**—Lists files that started a parent process, the process name, and the action the process performed.
- **File**—Lists files that started a child processes, the process name, and the action the process performed.

Report Heading	Description
	<ul style="list-style-type: none"> • Mutex—If the sample file generates other program threads, the mutex name and parent process is logged in this field. • Activity Timeline—Provides a play-by-play list of all recorded activity of the sample. This will help in understanding the sequence of events that occurred during the analysis. <p> <i>The activity timeline information is only available in the PDF export of the WildFire reports.</i></p>
<p>Submit Malware</p>	<p>Use this option to manually submit the sample to Palo Alto Networks. The WildFire cloud will then re-analyze the sample and generate a signatures if it determines that the sample is malicious. This is useful on a WildFire appliance that does not have signature generation or cloud intelligence enabled, which is used to forward malware from the appliance to the WildFire cloud.</p>
<p>Report an Incorrect Verdict</p>	<p>Click this link to submit the sample to the Palo Alto Networks threat team if you feel the verdict is a false positive or false negative. The threat team will perform further analysis on the sample to determine if it should be reclassified. If a malware sample is determined to be safe, the signature for the file is disabled in an upcoming antivirus signature update or if a benign file is determined to be malicious, a new signature is generated. After the investigation is complete, you will receive an email describing the action that was taken.</p>

WildFire Appliance Clusters

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

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:

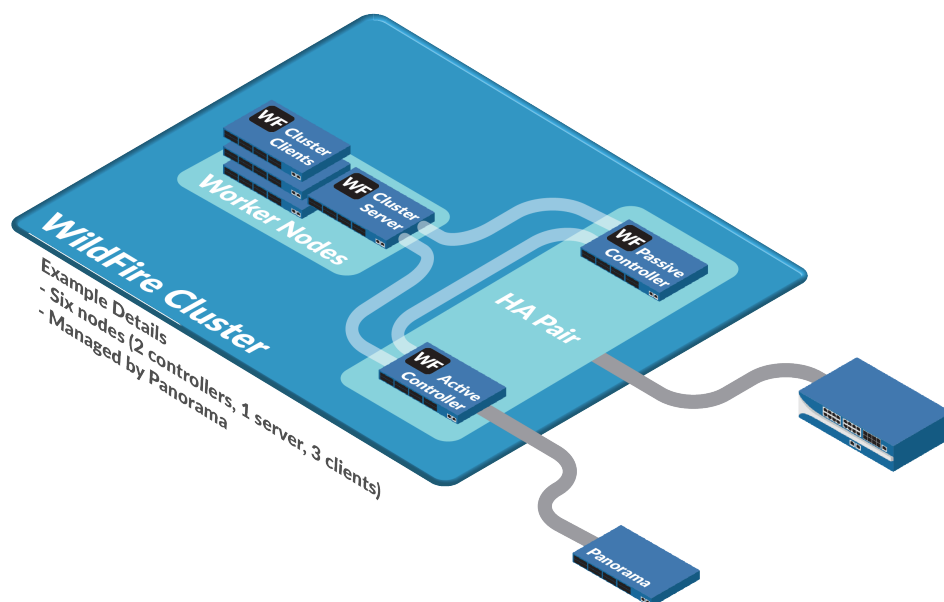
- From 2 to 20 WildFire appliances that you want to group and manage as a cluster. At a minimum, a cluster must have two WildFire appliances configured in a high-availability (HA) pair.
- Firewalls that forward samples to the cluster for traffic analysis and signature generation.
- (Optional) One or 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.
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

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.

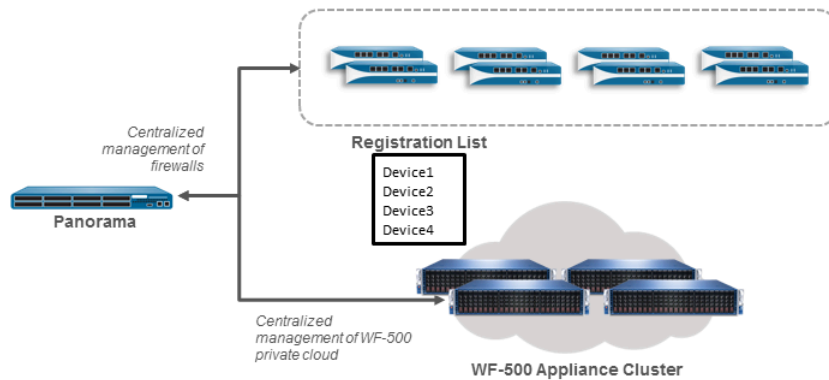
Additional nodes that are added to a WildFire cluster function as a worker or server node. The third node is automatically configured as a server, while each subsequent addition is added as a worker.

Benefits of Managing WildFire Clusters Using Panorama

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

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-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.

Category	Description
	<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. • Use low-latency connections between cluster nodes. The maximum latency for a connection should be no greater than 500 ms.
Dedicated cluster management interface	<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>

Category	Description
	<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. <p>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.</p>
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>

Category	Description
	<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

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

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

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 ha1 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
ha1-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

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

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

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

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

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.

1. 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>
```
2. 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 | oosp-responder-url days-till-expiry hostname [ ... ] request certificate generate certificate-name name digest country-code state locality organization email filename ca signed-by | oosp-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

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

To confirm that you 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 cluster controller
```

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 `Server role applied` next to `Status`. If the node has been configured to be a server, but isn't operating as a server, the status displays `Server role 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 cluster data-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 system subtype 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—**match queue**, for example **show log system direction equal backward | match queue**
 - global-database—**match global**, for example **show log system direction equal backward | match global**
 - 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"> ❑ 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"> ❑ info wildfir cluster 0 Signature generation service status set to ReadyMaster ❑ info wildfir cluster 0 Signature generation service 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	<ul style="list-style-type: none"> ❑ info general 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-queue service - succeeded ❑ info general general 0 Setup policy for global-queue service
global-database	<ul style="list-style-type: none"> ❑ info general 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-db bootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-db bootstrap and join cluster ❑ info general general 0 Start wf_services, For global-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-db bootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-db bootstrap and join cluster ❑ info general general 0 Stop wf_services, For global-db bootstrap and join cluster ❑ info general general 0 Bootstrap and join cluster for global-db service

Component	Passive Controller Status Example
signature-generation	<ul style="list-style-type: none"> ❑ info wildfir cluster 0 Signature generation service status set to ReadySlave ❑ info wildfir cluster 0 Signature generation service status set to ReadySlave



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	<ul style="list-style-type: none"> ❑ info wildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded with status JoinedCluster ❑ info general general 0 Join cluster for global-queue service - succeeded ❑ info general general 0 Setup policy for global-queue service
global-database	<ul style="list-style-type: none"> ❑ info general general 0 Restore applications: done, For global-db bootstrap and join cluster ❑ info general general 0 Start vm_mgr, For global-db bootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-db bootstrap and join cluster ❑ info general general 0 Start wf_services, For global-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-db bootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-db bootstrap and join cluster

Component	Active Controller Status
	<ul style="list-style-type: none"> ❑ 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"> ❑ info wildfire 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"> ❑ info wildfire cluster 0 Signature generation service status set to ReadySlave ❑ info wildfire cluster 0 Signature generation service 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"> ❑ info wildfire cluster 0 Global queue (rabbitmq) cluster formation succeeded with status JoinedCluster ❑ info general general 0 Join cluster for global-queue service - 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"> ❑ info general general 0 Restore applications: done, For global-db bootstrap and join cluster ❑ info general general 0 Start vm_mgr, For global-db bootstrap and join cluster ❑ info general general 0 Start uwsgi, For global-db bootstrap and join cluster ❑ info general general 0 Start wf_services, For global-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-db bootstrap and join cluster ❑ info general general 0 Stop uwsgi, For global-db bootstrap and join cluster ❑ info general general 0 Stop wf_services, For global-db bootstrap and join cluster ❑ 2019/07/19 14:32:50 info general general 0 Promote worker node and join cluster for global-db service

Component	Server Node Status
signature-generation	<ul style="list-style-type: none"> ❑ info wildfire 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

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.
		FailedToStartServices	Internal database services failed to start.

Name	Description	Possible Status Conditions	Definition
		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	If 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.
		DataMigrationDone	The data migration process is complete.

Name	Description	Possible Status Conditions	Definition
		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.
		FailedToBootstrap	The bootstrapping process has failed.

Name	Description	Possible Status Conditions	Definition
		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.
		ReadyLeader	The queuing service is in a ready state and the

Name	Description	Possible Status Conditions	Definition
			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.
		DataMigrationFailed	The data migration process has failed.

Name	Description	Possible Status Conditions	Definition
		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.
		ReadySlave	The signature database service is in backup mode

Name	Description	Possible Status Conditions	Definition
			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

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) / passive (backup) controller	
wfcore	Indicates that the node is running as a server for WildFire cluster infrastructure services.	Server node	

Upgrade WildFire Appliances in a Cluster

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

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.

These updates equip the appliance with the latest threat information to accurately detect malware.

```
admin@WF-500(passive-controller)> request
wf-content upgrade install version latest
```

STEP 3 | Verify that the WildFire appliance software version you want to install is available

```
admin@WF-500(passive-controller)> request
system software check
```

STEP 4 | Download the PAN-OS 9.0 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.

Download the 9.0.0 software version.

```
admin@WF-500(passive-controller)> request
system software download version 9.0.0
```

To check the status of the download, use the following command

```
admin@WF-500(passive-controller)> show
jobs all
```

STEP 5 | Confirm that all services are running.

```
admin@WF-500(passive-controller)> show
system software status
```

STEP 6 | Install the 9.0 software version.

```
admin@WF-500(passive-controller)> request
system software install version 9.0.0
```

STEP 7 | 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 8 | Repeat steps 1-7 for each WildFire worker node in the cluster.

STEP 9 | (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 10 | Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the sw-version field shows 9.0.0:

```
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.

Upgrade a Cluster Locally without an Internet Connection

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 | 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 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 | Verify that the WildFire appliance software version you want to install is available.

```
admin@WF-500(passive-controller)> request  
system software check
```

STEP 6 | Download the PAN-OS 9.0 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.

Download the 9.0.0 software version:

1. Navigate to the [PaloAlto 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-9.0.0
```

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

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

STEP 7 | Confirm that all services are running.

```
admin@WF-500(passive-controller)> show
system software status
```

STEP 8 | Install the 9.0 software version.

```
admin@WF-500(passive-controller)> request
system software install version 9.0.0
```

STEP 9 | 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 10 | Repeat steps 1-9 for each WildFire worker node in the cluster.

STEP 11 | (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 12 | Check that the WildFire appliance is ready to resume sample analysis.

1. Verify that the sw-version field shows 9.0:

```
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

Refer to the following topics to diagnose and troubleshoot WildFire cluster issues:

- [Troubleshoot WildFire Split-Brain Conditions](#)

Troubleshoot WildFire Split-Brain Conditions

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?

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

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 anaysis queued: 0
                sample anaysis 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

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

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

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

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

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

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

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.

Symbol	Description
+	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: test is not a valid name.</p> <p> A single quote would also be invalid in this example.</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

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.
superuser	Has complete read-write access to the appliance.

WildFire CLI Command Modes

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

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](#)

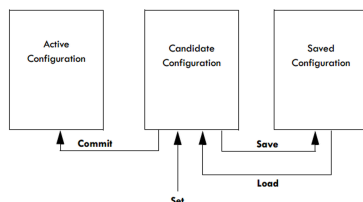
Configuration Mode Command Usage

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.

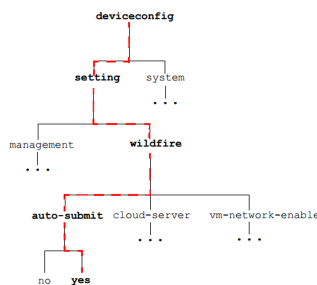
Because the candidate configuration is always unique, all authorized changes to the candidate configuration are consistent with each other.

Configuration Hierarchy

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 `show mgt-config`, only the `mgt-config` part of the hierarchy displays.

Hierarchy Paths

When entering commands, the path is traced through the hierarchy as follows:



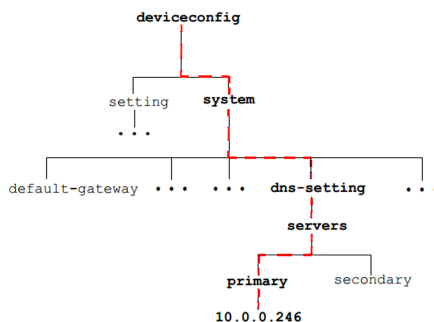
For example, the following command assigns the primary DNS server 10.0.0.246 for the appliance:

```
[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

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

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

This section describes how to access WildFire appliance software CLI:

- [Establish a Direct Console Connection](#)
- [Establish an SSH Connection](#)

Establish a Direct Console Connection

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

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

- [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

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

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

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

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 10.1 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

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 10.1 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
+-----+-----+-----+
|                                     |         Name         |
+-----+-----+-----+
|                                     | my-api-key          |
|                                     | my-api-key          |
|                                     | my-api-key          |
+-----+-----+-----+
+-----+-----+-----+
| 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
```

Apikey		Name
<API KEY>		stu-key1
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: 22:45:50 UTC reboot from qa16 (009701000044/35535) at 2017-02-17
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 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 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 as 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 |

```

```

+-----+-----+-----+
+-----+
      Last Created 100 Non-malicious Samples
+-----+-----+-----+
+-----+
|   SHA256   |   Finish Date   |   Create Date   |
Malicious |
+-----+-----+-----+
+-----+
| <HASH VALUE> | 2017-03-01 23:31:15 | 2017-03-01 23:24:29 |
No |
+-----+-----+-----+
+-----+
+-----+-----+-----+
+-----+-----+-----+
|   Storage Nodes   | Analysis Nodes |   Status   |
File Type |
+-----+-----+-----+
+-----+-----+-----+
| 0712:smp_27,94:smp_7 |   qa16   | Notify Finish | MS
Office document |
+-----+-----+-----+
+-----+

admin@WF-500>
show wildfire global sample-device-lookup sha256
equal
d75f2f71829153775fa33cf2fa95fd377f153551aadf0a642704595100efd460
Sample
1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e
last seen on following devices:

+-----+-----+-----+
+-----+-----+-----+
|   SHA256   |
| Device ID | Device IP | Submitted Time |
+-----+-----+-----+
+-----+-----+-----+
|
1024609813c57fe174722c53b3167dc3cf5583d5c7abaf4a95f561c686a2116e |
Manual | Manual | 2019-08-05 19:24:39 |
+-----+-----+-----+
+-----+-----+-----+

admin@WF-500>
show wildfire global sample-status sha256
equal
dc9f3a2a053c825e7619581f3b31d53296fe41658b924381b60aee3eeea4c088
+-----+-----+-----+
+-----+-----+-----+
|   Finish Date   |   Create Date   | Malicious |
Storage Nodes |

```



```

+-----+-----+-----+
+-----+
| 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 | | |

```

```

+-----+
+-----+
|          DOC/CDF Static Analyzer          |
| completed |                               |
| Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010 |
| completed |                               |
+-----+
+-----+

```

admin@WF-500> **show wildfire local statistics**

Current Time: 2017-03-01 17:44:31
 Received After: 2017-02-28 17:44:31
 Received Before: 2017-03-01 17:44:31

```

+-----+
|                               Wildfire Stats                               |
+-----+
+-----+
+-----+
+|                               Executable                               |
||                               ||
|                               ||
+-----+
+| File Type | Submitted | Analyzed | Pending | Malware | Grayware |
| Benign | Error ||
+-----+
+|                               ||
|| exe | 2 | 2 | 0 | 0 | 0 |
| 2 | 0 ||
+-----+
+|                               ||
|| dll | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 ||
+-----+
+|

```

Environment Analysis Summary for Executable:
 VM Utilization : 0/10
 Files Analyzed : 2

```

+-----+
+-----+
||                               Non-Executable                               |
|                               ||
+-----+
+|

```

FileType	Submitted	Analyzed	Pending	Malware	Grayware
pdf	0	0	0	0	0
jar	0	0	0	0	0
doc	1	1	0	1	0
ppt	0	0	0	0	0
xls	0	0	0	0	0
docx	0	0	0	0	0
pptx	0	0	0	0	0
xlsx	0	0	0	0	0
rtf	0	0	0	0	0
class	2	2	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