Advanced WildFire Administration

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

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

Copyright

Last Revised

June 29, 2023

Table of Contents

Advanced WildFire Overview

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Advanced WildFire™ provides detection and prevention of zero-day malware using a combination of dynamic / static analysis and Intelligent Run-time Memory Analysis to detect highly evasive threats and create protections to block malware.

The Advanced WildFire Analysis Environment identifies previously unknown malware and generates signatures that Palo Alto Networks NGFWs can use to then detect and block the malware. When a Palo Alto Networks firewall detects an unknown sample, the firewall automatically forwards all supported file types from any application to the WildFire public-cloud service for Advanced WildFire analysis. Based on the properties, behaviors, and activities the sample displays when analyzed and executed in the sandbox, Advanced WildFire determines the sample to be benign, grayware, phishing, or malicious, and 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.

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

- Review Advanced WildFire Concepts to learn more about the types of samples you can submit for WildFire analysis, WildFire verdicts, and WildFire signatures.
- Learn more about Advanced 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 Advanced WildFire to define the samples that you want to submit for analysis, and to begin submitted samples to a WildFire cloud.
- If you are deploying a WildFire appliance, refer to the WildFire Appliance Administration.

Subscription Options

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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

Palo Alto Networks offers several subscription options:

- **WildFire**—The WildFire subscription provides protection from malware by forwarding samples to the Advanced WildFire cloud, where a series of analysis environments are used to detect and prevent unknown malware threats by generating protections that to block further instances of the threat. As part of your subscription, you get access to regular Advanced WildFire signature updates, advanced file type forwarding, as well as the ability to upload files using the WildFire API. If you are operating an environment that requires an on-prem solution, the WildFire subscription can be used to forward files to a local WildFire appliance.
- **Advanced WildFire**—(PAN-OS 10.0 and later) The Advanced WildFire subscription includes all of the features found in the standard WildFire subscription, and improves upon it by providing sample analysis through an advanced cloud-based detector. The advanced detection system analyzes samples using intelligent real-time runtime memory analysis, runtime DLL emulation, automated unpacking, family classification, stealth observation, and other techniques to target highly-evasive malware.
- **Standalone WildFire API**—Palo Alto Networks customers operating SOAR tools, custom security applications, and other threat assessment software can access the advanced file analysis capabilities of the WildFire cloud with a standalone subscription that provides API-only access. This allows you to leverage WildFire-based analytics without relying on the Palo Alto Networks firewall as a forwarding mechanism. The WildFire Standalone API subscription allows you to make direct queries to the WildFire cloud threat database for information about potentially malicious content, and submit files for analysis using the advanced threat analysis capabilities of WildFire, based on your organization's specific requirements. The enhanced access limits of the subscription allow organizations of various sizes to customize their access limits according to their usage - this includes scalable licenses that allow a specific number of file/report queries, sample submissions (for Advanced WildFire analysis), or a combination of the two. For more information, refer to the WildFire API Reference.

The standard WildFire subscription unlocks the following features:

- **Real-Time Updates**—(PAN-OS 10.0 and later) The firewall can retrieve Advanced WildFire signatures for newly-discovered malware as soon as the Advanced 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 Advanced WildFire updates is a recommended best practice setting.

  Select **Device** > **Dynamic Updates** and enable the firewall to get the latest Advanced WildFire signaturesin real-time.

- **Five-Minute Updates**—(All PAN-OS versions) The Advanced WildFire public cloud can generate and distribute Advanced 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 Advanced WildFire updates instead of scheduling recurring updates.

  Select **Device** > **Dynamic Updates** to enable the firewall to get the latest Advanced WildFire signatures. Depending on your Advanced 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.

- **Advanced 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 Advanced WildFire Cloud analysis technology on the firewall, Advanced 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. Advanced 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.

- **File Type Support**—In addition to PEs, forward advanced file types for Advanced 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).

- **Advanced WildFire API**—Access to the WildFire API, which enables direct programmatic access to the Advanced WildFire public cloud or a WildFire private cloud. Use the API to submit files for analysis and to retrieve the subsequent Advanced WildFire analysis reports. As part of the Advanced WildFire or WildFire subscription, you can submit up to 150 sample submissions and up to 1,050 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 for Advanced WildFire Analysis. 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 Advanced WildFire subscription, you must activate the license before you can take advantage of the subscription-only WildFire features.

The Advanced WildFire subscription unlocks the following feature:

- **Intelligent Run-time Memory Analysis**—Intelligent Run-time Memory Analysis is a cloud-based, advanced analysis engine that complements the static and dynamic analysis engines, to detect and prevent evasive malware threats. These evasive techniques used by advanced threats include, but are not limited to, malware using cloaking strategies, displaying signs of bespoke design / ephemeral behaviors, created using sophisticated tools, and exhibit fast-spreading qualities. By leveraging a cloud-based detection infrastructure, introspective analysis detectors operate a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download content update packages or run resource intensive, appliance-based analyzers. The cloud-based detection engines are continuously monitored and updated using based on ML-based datasets used to analyze Advanced WildFire samples, with additional support from Palo Alto Networks threat researchers, who provide human intervention for highly accurized detection enhancements.

  Intelligent Run-time Memory Analysis relies on the existing WildFire analysis profile settings and does not require any additional configuration; however, you must have an active Advanced WildFire license. Samples that display or otherwise indicate evasive and/or advanced malware qualities are automatically forwarded to the appropriate analysis environments.

Advanced WildFire Concepts

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

- Samples
- Firewall Forwarding
- Session Information Sharing
- Analysis Environment
- Advanced WildFire Inline Cloud Analysis
- Advanced WildFire Inline ML
- Verdicts
- File Analysis
- Email Link Analysis
- URL Analysis
- Compressed and Encoded File Analysis
- Advanced WildFire Signatures
- Advanced WildFire Example

Samples

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Samples are all file types and email links submitted for Advanced 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 Advanced WildFire analysis.

Firewall Forwarding

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

The firewall forwards unknown samples, as well as blocked files that match antivirus signatures, for Advanced 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 Advanced WildFire signatures, the firewall forwards it for Advanced 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

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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.

Forward of session information is enabled by default; however, you can adjust the default settings and choose what type of session information is forwarded to one of the WildFire cloud options.

- Cloud Management
- PAN-OS & Panorama

Cloud Management

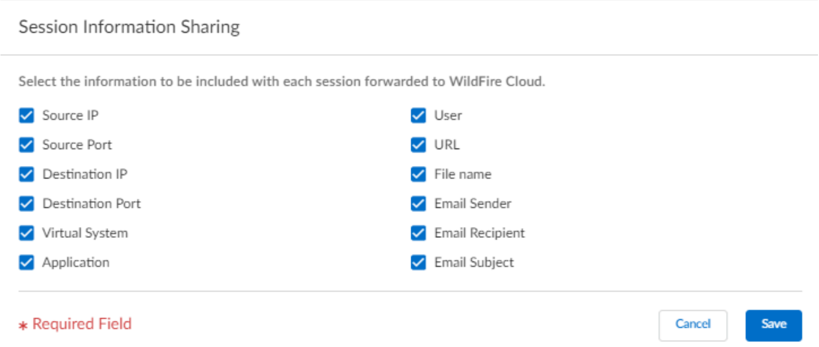
If you're using Panorama to manage Prisma Access:

*Toggle over to the **PAN-OS** tab and follow the guidance there.*

If you're using Prisma Access Cloud Management, continue here.

STEP 1 | Use the credentials associated with your Palo Alto Networks support account and log in to the Strata Cloud Manager application on the hub.

STEP 2 | Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus** and configure your **Session Information Settings** options.



Session Information Sharing

Select the information to be included with each session forwarded to WildFire Cloud.

☑ Source IP	☑ User
☑ Source Port	☑ URL
☑ Destination IP	☑ File name
☑ Destination Port	☑ Email Sender
☑ Virtual System	☑ Email Recipient
☑ Application	☑ Email Subject

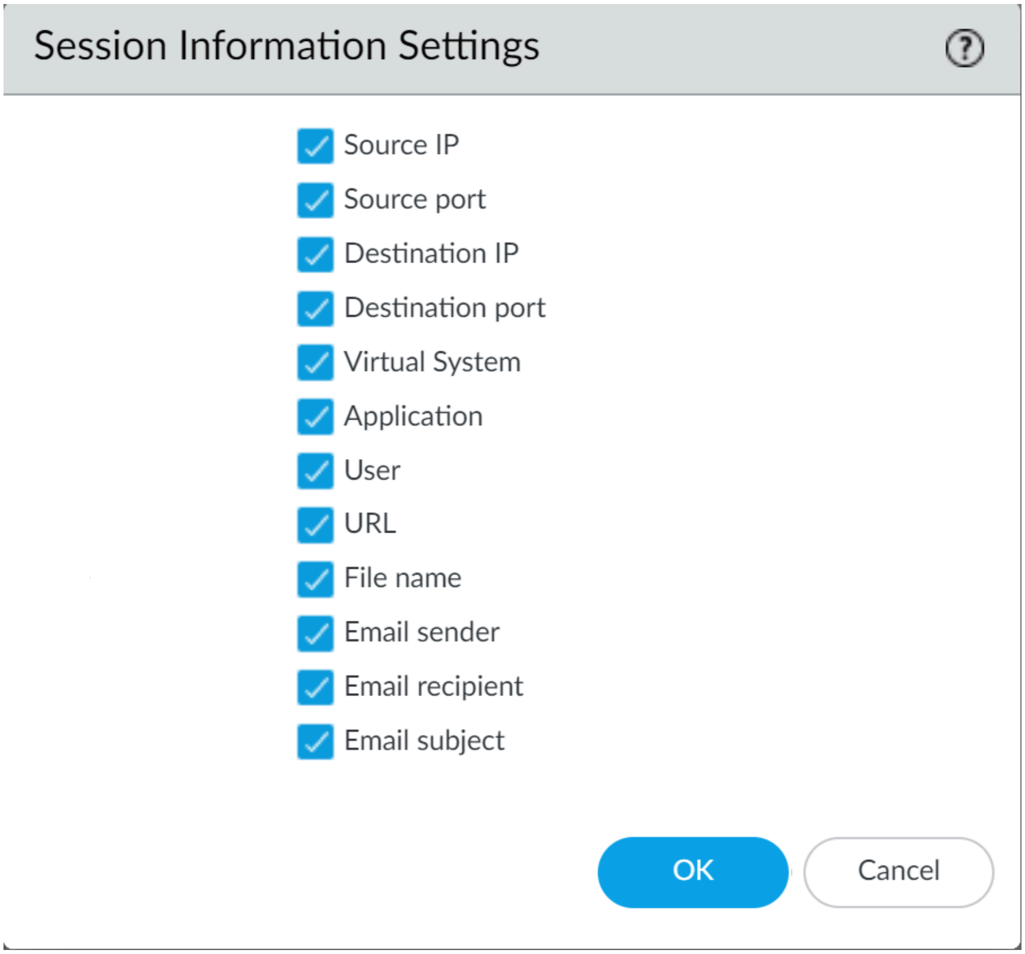
- **Source IP**—Forward the source IP address that sent the unknown file.
- **Source Port**—Forward the source port that sent the unknown file.
- **Destination IP**—Forward the destination IP address for the unknown file.
- **Destination Port**—Forward the destination port for the unknown file.
- **Virtual 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).

STEP 3 | **Save** your changes.

PAN-OS & Panorama

STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | Select **Device** > **Setup** > **WildFire** and select or clear the following **Session Information Settings** options.



Session Information Settings

☑ Source IP
☑ Source port
☑ Destination IP
☑ Destination port
☑ Virtual System
☑ Application
☑ User
☑ URL
☑ File name
☑ Email sender
☑ Email recipient
☑ Email subject

- **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).

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

Analysis Environment

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Advanced 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. Advanced 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, Advanced 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 Advanced WildFire cloud decompresses and decrypts the file in-memory within the dynamic analysis environment before analyzing it using static analysis. During dynamic analysis, Advanced 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 Advanced 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.

Advanced WildFire can analyze files using the following methods, based on sample characteristics:

- **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 (Advanced WildFire global cloud 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.
- **Intelligent Run-time Memory Analysis (Advanced WildFire License | Advanced WildFire global cloud only — requires PAN-OS 10.0 and later on NGFWs)**—A cloud-based analysis environment operating advanced detectors used to analyze modern threats utilizing a multitude of evasion techniques.

Advanced WildFire operates analysis environments that replicate the following operating systems:

- **Microsoft Windows XP 32-bit (Supported as an option for the WildFire private cloud only)**
- **Microsoft Windows 7 64-bit**
- **Microsoft Windows 7 32-bit (Supported as an option for WildFire private cloud only)**
- **Microsoft Windows 10 64-bit (Supported as an option for the Advanced WildFire public cloud and WildFire private cloud running PAN-OS 10.0 or later)**
- **Mac OS X (Advanced WildFire public cloud only)**
- **Android (Advanced WildFire public cloud only)**
- **Linux (Advanced WildFire public cloud only)**

The Advanced 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.

Advanced WildFire Inline Cloud Analysis

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

The Advanced WildFire cloud operates a series of inline cloud ML-based detection engines to analyze PE (portable executable) samples traversing through your network to detect and prevent unknown malware in real-time. This allows the Advanced WildFire cloud service to detect never-before seen malware (that does not have an existing WildFire signature or is detectable through the local Advanced WildFire inline cloud ML detectors) and block it from infecting the client. This includes scenarios where certain types of malware that have been previously unseen in the wild, and are not intercepted by Advanced WildFire Inline ML, can proceed unhindered because the file was not seen recently enough for its signature to be present on the firewall due to signature age-out or signature database capacity limits. Newly defined malicious files will be blocked in subsequent encounters by the firewall as the signature has become part of the current set, however, that occurs after a malicious file is analyzed by the WildFire cloud.

The Advanced WildFire Inline Cloud can hold files from downloading (and potentially spreading within your network) while analyzing these suspicious files for malware in the cloud, in a real-time exchange. As with other malicious content that is analyzed by WildFire, any threat detected by Advanced WildFire Inline Cloud generates a threat signature that is disseminated by Palo Alto Networks to customers through a signature update package to provide a future defense for all Palo Alto Networks customers.

Advanced WildFire Inline Cloud operates using a lightweight forwarding mechanism on the firewall to minimize any local performance impact; and to keep up with the latest changes in the threat landscape, cloud inline ML detection models are added and updated seamlessly in the cloud, without requiring content updates or feature release support.

Advanced WildFire Inline Cloud Analysis is enabled and configured through the WildFire Analysis profile and requires PAN-OS 11.1 or later with an active Advanced WildFire license.

Advanced WildFire Inline ML

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

The Advanced WildFire inline ML option present in the Antivirus profile enables the firewall dataplane to apply machine learning on PE (portable executable), ELF (executable and linked format) and MS Office files, and PowerShell and shell scripts in real-time. This layer of antivirus protection complements the Advanced WildFire-based signatures to provide extended coverage for files of which signatures do not already exist. 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. Before you can enable Advanced WildFire inline ML, you must possess an active Advanced WildFire or standard WildFire subscription.

Inline ML-based protection can also be enabled to detect malicious URLs in real-time as part of your URL Filtering configuration.

Advanced WildFire inline ML is not supported on the VM-50 or VM50L virtual appliance.

Verdicts

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

When Advanced WildFire analyzes a previously unknown sample in one of the Palo Alto Networks-hosted Advanced 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, signatures are generated and distributed to prevent against future exposure to the threat.

Each Advanced WildFire cloud—global (U.S.) and regional, and the WildFire private cloud—analyzes samples and generates WildFire verdicts independently of the other WildFire cloud options. With the exception of WildFire private cloud verdicts, verdicts are shared globally, enabling Advanced 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

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

A Palo Alto Networks firewall configured with a WildFire analysis profile forwards samples for Advanced 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 Advanced WildFire Analysis profile criteria, the firewall forwards the decoded file for analysis.

The Advanced WildFire analysis capabilities can also be enabled on the firewall to provide inline antivirus protection. The Advanced 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 Advanced WildFire Inline ML for more information.

The Advanced 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. Advanced WildFire analyzes the multi-stage threats by processing them in static and dynamic 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 Advanced WildFire cloud receives a sample that has been encrypted using the password *infected* or *virus*, the Advanced WildFire cloud decrypts and analyzes the archive file. You can view the 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, Advanced WildFire analysis support can vary depending on the Advanced WildFire cloud to which you are submitted samples. Review Advanced WildFire File Type Support to learn more.

File Types Supported for WildFire Forwarding	Description
`apk`	Android Application Package (APK) files. *DEX files contained within APK files are analyzed as part of the APK file analysis.*
`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)

File Types Supported for WildFire Forwarding	Description
	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 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`	Roshal Archive (RAR) and 7-Zip (7z) archive files. Multi-volume archives are that are split into several smaller files cannot be submitted for analysis. Only RAR files encrypted with the password *infected* or *virus* are decrypted and analyzed by the Advanced WildFire cloud. *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.*
`linux`	Executable and Linkable Format (ELF) files.
`script`	Various script files. • 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

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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 File-Forwarding Capacity by Model. 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 Advanced WildFire Analysis. With a Advanced URL Filtering license, you can also block user access to malicious and phishing sites.

URL Analysis

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Where Can I Use This?	What Do I Need?
- VM-Series - CN-Series	

The Advanced 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, Advanced WildFire is able to generate a more accurate verdict and provide consistent URL analysis data.

The URL analyzers operating in the Advanced WildFire global cloud 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 Advanced WildFire clouds with the improved capabilities, without affecting GDPR compliance. After a URL has been processed, you can retrieve the 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 Forward Files for Advanced WildFire Analysis.

Verdicts that you suspect are either false positives or false negatives can be submitted to the Palo Alto Networks threat team for additional analysis.

Compressed and Encoded File Analysis

Where Can I Use This?	What Do I Need?
- Prisma Access (Managed by Strata Cloud Manager) - Prisma Access (Managed by Panorama) - NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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 Advanced WildFire analysis, you can submit files directly to the Advanced 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 Advanced WildFire public cloud.

Advanced WildFire Signatures

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Advanced 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. Advanced WildFire automatically generates a signature based on the malware payload of the sample and tests it for accuracy and safety.

Each Advanced WildFire cloud analyzes samples and generates malware signatures independently of the other Advanced WildFire clouds. With the exception of WildFire private cloud signatures, Advanced WildFire signatures are shared globally, enabling 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 Advanced WildFire generates address multiple variants of the malware.

Firewalls with an active Advanced WildFire license can retrieve the latest Advanced WildFire signatures in real-time, as soon as they become available. If you do not have an Advanced 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.

Advanced WildFire Deployments

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

You can set up a Palo Alto Networks firewall to submit unknown samples to one of the Palo Alto Networks-hosted Advanced 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 Advanced WildFire public cloud options and certain samples to a WildFire private cloud:

- Advanced WildFire Public Cloud
- WildFire Private Cloud
- WildFire Hybrid Cloud
- WildFire: U.S. Government Cloud

Advanced WildFire Public Cloud

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

A Palo Alto Networks firewall can forward unknown files and email links to the Advanced WildFire global cloud (U.S.) or to the Advanced WildFire regional clouds that Palo Alto Networks owns and maintains. Choose the Advanced WildFire public cloud to which you want to submit samples for analysis based on your location and your organization's needs:

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

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

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

- **Advanced WildFire Japan Cloud**

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

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

- **Advanced WildFire Singapore Cloud**

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

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

- **Advanced WildFire United Kingdom Cloud**

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

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

- **Advanced 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 Advanced WildFire Canada cloud for analysis and to access the Advanced WildFire Canada cloud portal: ca.wildfire.paloaltonetworks.com.

- **Advanced 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 Advanced WildFire Australia cloud for analysis and to access the Advanced WildFire Australia cloud portal: au.wildfire.paloaltonetworks.com.

- **Advanced WildFire Germany Cloud**

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

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

- **Advanced WildFire India Cloud**

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

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

  The Advanced WildFire Switzerland cloud is a regional public cloud environment hosted in Switzerland.

  Use the following URL to submit files to the Advanced WildFire Switzerland cloud for analysis and to access the Advanced WildFire Switzerland cloud portal: ch.wildfire.paloaltonetworks.com.
- **Advanced WildFire Poland Cloud**

  The Advanced WildFire Poland cloud is a regional public cloud environment hosted in Poland.

  Use the following URL to submit files to the Advanced WildFire Poland cloud for analysis and to access the Advanced WildFire Poland cloud portal: pl.wildfire.paloaltonetworks.com.
- **Advanced WildFire Indonesia Cloud**

  The Advanced WildFire Indonesia cloud is a regional public cloud environment hosted in Indonesia.

  Use the following URL to submit files to the Advanced WildFire Indonesia cloud for analysis and to access the Advanced WildFire Indonesia cloud portal: id.wildfire.paloaltonetworks.com.
- **Advanced WildFire Taiwan Cloud**

  The Advanced WildFire Taiwan cloud is a regional public cloud environment hosted in Taiwan.

  Use the following URL to submit files to the Advanced WildFire Taiwan cloud for analysis and to access the Advanced WildFire Taiwan cloud portal: tw.wildfire.paloaltonetworks.com.
- **Advanced WildFire France Cloud**

  The Advanced WildFire France cloud is a regional public cloud environment hosted in France.

  Use the following URL to submit files to the Advanced WildFire France cloud for analysis and to access the Advanced WildFire France cloud portal: fr.wildfire.paloaltonetworks.com.
- **Advanced WildFire Qatar Cloud**

  The Advanced WildFire Qatar cloud is a regional public cloud environment hosted in Qatar.

  Use the following URL to submit files to the Advanced WildFire Qatar cloud for analysis and to access the Advanced WildFire Qatar cloud portal: qatar.wildfire.paloaltonetworks.com.
- **Advanced WildFire South Korea Cloud**

  The Advanced WildFire South Korea cloud is a regional public cloud environment hosted in South Korea.

  Use the following URL to submit files to the Advanced WildFire South Korea cloud for analysis and to access the Advanced WildFire South Korea cloud portal: kr.wildfire.paloaltonetworks.com.

- **Advanced WildFire Israel Cloud**

  The Advanced WildFire Israel cloud is a regional public cloud environment hosted in Israel.

  Use the following URL to submit files to the Advanced WildFire Israel cloud for analysis and to access the Advanced WildFire Israel cloud portal: il.wildfire.paloaltonetworks.com.
- **Advanced WildFire Saudi Arabia Cloud**

  The Advanced WildFire Saudi Arabia cloud is a regional public cloud environment hosted in Saudi Arabia.

  Use the following URL to submit files to the Advanced WildFire Saudi Arabia cloud for analysis and to access the Advanced WildFire Saudi Arabia cloud portal: sa.wildfire.paloaltonetworks.com.
- **Advanced WildFire Spain Cloud**

  The Advanced WildFire Spain cloud is a regional public cloud environment hosted in Spain.

  Use the following URL to submit files to the Advanced WildFire Spain cloud for analysis and to access the Advanced WildFire Spain cloud portal: es.wildfire.paloaltonetworks.com.

Each Advanced WildFire cloud—global (U.S.) and regional—analyzes samples and generates malware signatures and verdicts independently of the other WildFire clouds. Advanced WildFire signatures and verdicts are then shared globally, enabling all WildFire users worldwide to benefit from malware coverage regardless of the location in which the malware was first detected. Review Advanced 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

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire or WildFire License

In a Palo Alto Networks private cloud deployment, Palo Alto Networks firewalls forward files to a WildFire appliance on your corporate network that is being used to host a private cloud analysis location.

For more information about hybrid cloud forwarding, refer to the WildFire Appliance Administrator's Guide.

WildFire Hybrid Cloud

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire or WildFire License

A firewall in a WildFire hybrid cloud deployment can forward certain samples to one of the Palo Alto Networks-hosted WildFire public clouds and other samples to a WildFire private cloud hosted by a WildFire appliance.

For more information about hybrid cloud forwarding, refer to the WildFire Appliance Administrator's Guide.

WildFire: U.S. Government Cloud

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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.
- The WildFire: U.S Government cloud does not currently support Advanced WildFire analysis.

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.

File Type Support

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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

For a comprehensive list of specific file types supported by WildFire, refer to Supported File Types (Complete List).

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

File Types Supported for Analysis	Advanced WildFire Public Cloud (all regions)	WildFire U.S. Government Cloud	Advanced WildFire Portal | API (direct upload; all regions)
Portable document format (PDF) files	✓	✓	✓
Mac OS X files	✓	✓	✓
Linux (ELF files and Shell scripts) files	✓	✓	✓
Archive (RAR, 7-Zip, ZIP*) files	✓	✓	✓
Script (BAT, JS, VBS, PS1, and HTA) files	✓	✗	✓
Python scripts	✓	✓	✓
Perl scripts	✗	✗	✓
Archive (ZIP [direct upload] and ISO) files	✗	✗	✓
Image (JPG and PNG) files	✗	✗	✓

* ZIP files are not directly forwarded to the Advanced 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 Advanced WildFire cloud deployments, see* Advanced WildFire Deployments.
- *For details about each file type supported for WildFire analysis, see* File Analysis.

Supported File Types (Complete List)

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

The following table lists the file types supported by WildFire analysis. For files marked Yes in the Forwarding Support column, this includes files that are MIME encoded in web traffic (HTTP/ HTTPS) and email protocols (SMTP, IMAP, POP).

Supported Content Type	Extension Example	Forwarding Support
7zip Archive	7z	Yes
Adobe Flash File	swf	Yes
Android APK	apk	Yes
Android DEX	dex	Yes
batch	bat	Yes
Comma-Separated Values	csv	No
DLL, DLL64	dll	Yes
ELF	elf	Yes
HTML Application	hta	Yes
ISO	iso	No
JAVA Class	class	Yes
JAVA JAR	jar	Yes
Javascript/JScript	js, jse, wsf	Yes (JS only)

Supported Content Type	Extension Example	Forwarding Support
Joint Photographic Experts Group	jpg	No
Link	elink	Yes
Mach-O	macho	Yes
macOS App Installer	pkg	Yes
macOS Disk Image	dmg	Yes
Microsoft Excel 97 - 2003 Document	xls	Yes
Microsoft Excel Document	xlsx	Yes
Microsoft PowerPoint 97 - 2003 Document	ppt	Yes
Microsoft PowerPoint Document	pptx	Yes
Microsoft Symbolic Link file	slk	Yes
Microsoft Web Query File	iqy	Yes
Microsoft Word 97 - 2003 Document	doc	Yes
Microsoft Word Document	docx	Yes
OpenDocument Spreadsheet Document	ods	No
OpenDocument Text Document	odt	No
PDF	pdf	Yes
PE, PE64	exe	Yes
Perl Script	pl	No
Portable Network Graphics file	png	No
PowerShell	ps1	Yes

Supported Content Type	Extension Example	Forwarding Support
Python Script	py	Yes
RAR Archive	rar	Yes
RTF	rtf	Yes
Shell Script	sh	Yes
VBScript	vbs, vbe	Yes (VBS only)
Windows Installer Package	msi	Yes
Windows Link File	lnk	Yes
Windows Script	wsf	No
Zip Archive	zip	No
Active Server Pages	asp	No
Active Server Pages Extended	aspx	No
Extensible Markup Language	xml	No
HyperText Markup Language	html	No

Advanced WildFire Example

Where Can I Use This?	What Do I Need?
- Prisma Access (Managed by Strata Cloud Manager) - Prisma Access (Managed by Panorama) - NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

The following example scenario summarizes the full Advanced 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.

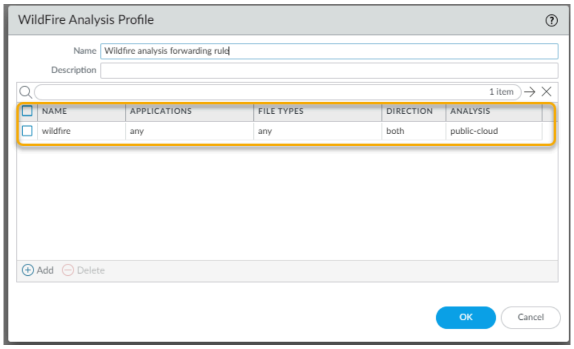
This example will demonstrate how a Palo Alto Networks firewall in conjunction with Advanced WildFire can discover zero-day malware downloaded by an end user, even if the traffic is SSL encrypted. After Advanced WildFire identifies the malware a log is sent to the firewall and the firewall alerts the administrator who then contacts the user to eradicate the malware. Advanced WildFire then generates a new signature for the malware, after which firewalls automatically download 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 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 Advanced 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.



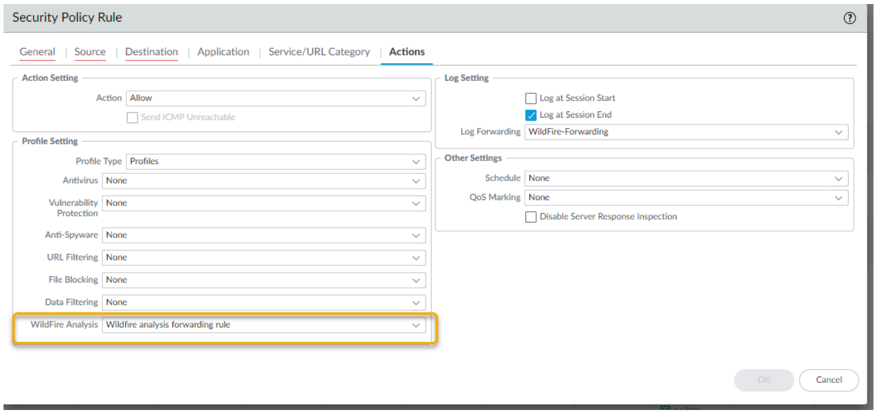
WildFire Analysis Profile

Name: Wildfire analysis forwarding rule

Description:

1 item

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
wildfire	any	any	both	public-cloud



Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions

Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: Wildfire analysis forwarding rule

Log Setting

□ Log at Session Start

☑ Log at Session End

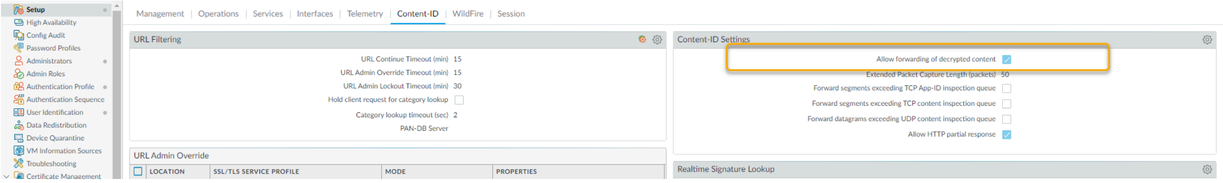
Log Forwarding: WildFire-Forwarding

Other Settings

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection



URL Filtering

URL Continue Timeout (min) 15

URL Admin Override Timeout (min) 15

URL Admin Lockout Timeout (min) 30

Hold client request for category lookup □

Category lookup timeout (sec) 2

PAN-DB Server

URL Admin Override

□	LOCATION	SSL/TLS SERVICE PROFILE	MODE	PROPERTIES

Content-ID Settings

Allow forwarding of decrypted content ☑

Extended Packet Capture Length (packets) 50

Forward segments exceeding TCP App-ID inspection queue □

Forward segments exceeding TCP content inspection queue □

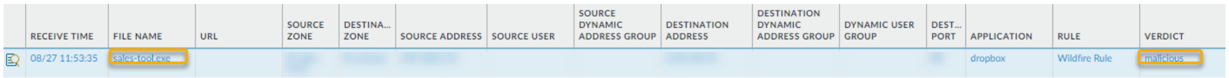
Forward datagrams exceeding UDP content inspection queue □

Allow HTTP partial response ☑

Realtime Signature Lookup

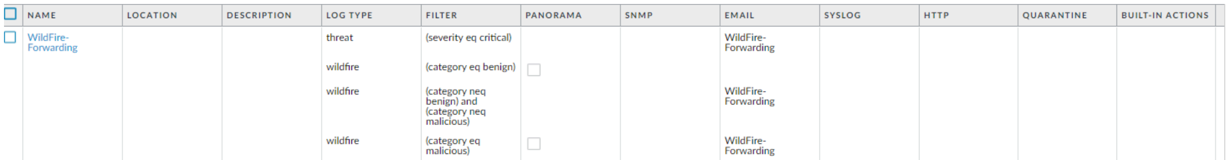
STEP 4 | At this point, Advanced WildFire has received the file and is analyzing it for more than 200 different malicious behaviors.

STEP 5 | After Advanced WildFire has completed the file analysis, it sends an Advanced WildFire log back to the firewall with the analysis results. In this example, the 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	sales-tool.exe		[redacted]	[redacted]	[redacted]			[redacted]			[redacted]	dropbox	Wildfire Rule	malicious

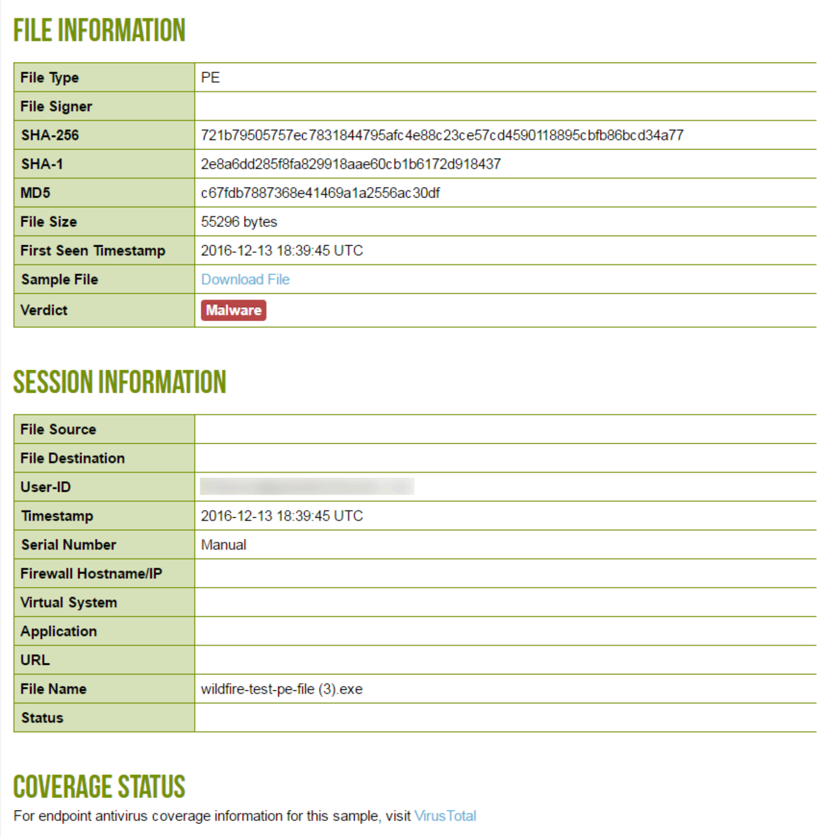
STEP 6 | The firewall is configured with a log forwarding profile that will send alerts to the security administrator when malware is discovered.



☐	NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
☐	WildFire-Forwarding			threat	(severity eq critical)			WildFire-Forwarding				
				wildfire	(category eq benign)	☐						
				wildfire	(category neq benign) and (category neq malicious)			WildFire-Forwarding				
				wildfire	(category eq malicious)	☐		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 Advanced 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 Advanced 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

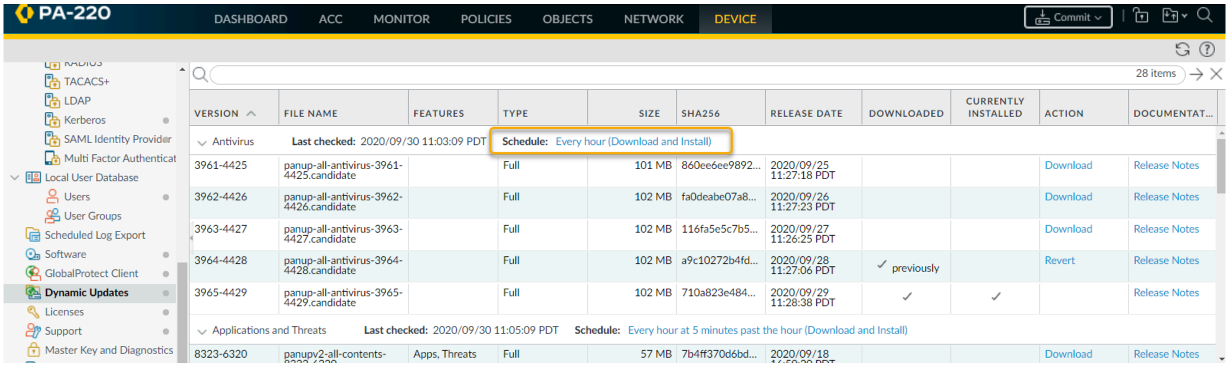
SESSION INFORMATION

File Source	
File Destination	
User-ID	[redacted]
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 Advanced 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, Advanced WildFire identified the zero-day malware, generated a signature, added it to the Advanced 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 Advanced WildFire and antivirus signatures is now protected against this newly discovered malware. The following screenshot shows the Advanced WildFire update schedule:



VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Antivirus **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
Applications and Threats **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	7b4ff370d6bd...	2020/09/18			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 Advanced WildFire

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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

For information about using the WildFire private cloud or hybrid cloud, refer to the WildFire Appliance administration.

I you are using Advanced WildFire on Prisma Access, familiarize yourself with the product before configuring your WildFire Analysis Security Profile to Forward Files for Advanced WildFire Analysis.

STEP 1 | Get your Advanced WildFire or WildFire subscription. If you do not have a subscription, you can still forward PEs for WildFire analysis.

STEP 2 | Decide which of the Advanced WildFire Deployments works for you:

- Advanced WildFire Public Cloud—Forward samples to a Palo Alto Networks-hosted Advanced WildFire public cloud.
- WildFire U.S. Government cloud—Forward samples to a Palo Alto Networks-hosted WildFire U.S. Government cloud.

If you are deploying a WildFire private or hybrid cloud, refer to the WildFire Appliance administration.

STEP 3 | Confirm your 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 4 | Connect the firewall to WildFire and configure WildFire settings.

1. Select **Device** > **Setup** > **WildFire** and edit General Settings.
2. Use **WildFire Public Cloud** field to forward samples to the Advanced WildFire public cloud.
3. Define the size limits for files the firewall forwards and configure WildFire logging and reporting settings.

   *It is a Advanced WildFire Best Practices 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 5 | Enable the firewall to forward decrypted SSL traffic for Advanced WildFire analysis.

This is a recommended Advanced WildFire best practice.

STEP 6 | Start submitting samples for analysis.

1. Define traffic to forward for WildFire analysis. (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 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 **public-cloud** as the **Destination** to forward samples to the Advanced WildFire cloud for analysis.
3. Attach the WildFire analysis profile to a security policy rule. Traffic matched to the policy rule is forwarded for WildFire analysis (**Policies** > **Security** and **Add** or modify a security policy rule).

STEP 7 | Enable the firewall to get the latest Advanced WildFire signatures.

New Advanced 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**:
     - Check that **WildFire** updates are displayed.
     - Select **Check Now** to retrieve the latest signature update packages.
  2. Set the **Schedule** to download and install the latest Advanced 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 8 | Start scanning traffic for threats, including malware that Advanced 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 9 | Control site access to web sites where Advanced WildFire has identified the associated link as malicious or phishing.

> *This option requires a PAN-DB URL Filtering license. Learn more about URL Filtering 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:

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 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 10 | 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 for analysis. (If you'd like to disable logging of benign files after confirming that the firewall is connected to a WildFire cloud, 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 to test your complete WildFire configuration.

STEP 11 | Investigate analysis results.

- Find analysis results:
    - Use the firewall to monitor malware and view WildFire analysis reports for a sample.
    - View reports on the Advanced WildFire portal for all samples submitted to the Advanced WildFire public cloud, including samples that you manually submitted to the WildFire public cloud.
    - Use the Advanced WildFire API to retrieve sample verdicts and reports from a WildFire appliance.

STEP 12 | Next step:

Review and implement Advanced WildFire Best Practices.

Advanced WildFire Deployment Best Practices

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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.

- Advanced WildFire Best Practices

Advanced WildFire Best Practices

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Prisma Access users—Refer to the Prisma Access documentation *for product-specific information about the user-interface.*

□ Follow the best practices 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. Together, Advanced WildFire® and Threat Prevention enable comprehensive threat detection and prevention.

□ Download and install content updates 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 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 Advanced WildFire signatures in real-time. This provides access to newly-discovered malware signatures as soon as the Advanced 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, then enable the firewall to Forward Decrypted SSL Traffic for WildFire Analysis. Only a superuser can enable this option.

□ Use the default WildFire Analysis profile to define the traffic that the firewall should forward for analysis (**Objects** > **Security Profiles** > **WildFire Analysis**). The default WildFire Analysis profile ensures complete coverage for all traffic that your Security policy allows—it specifies that all supported file types across all applications are forwarded for Advanced 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 analysis.

For details on applying a WildFire Analysis profile to firewall traffic, review how to Forward Files for Advanced WildFire Analysis.

> *WildFire Action settings in the Antivirus profile may impact traffic if the traffic generates an Advanced 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 to best practicesbecause Advanced 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 Advanced WildFire signatures.*

□ While you are configuring the firewall to Forward Files for Advanced WildFire Analysis, 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 Advanced 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 Advanced 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.

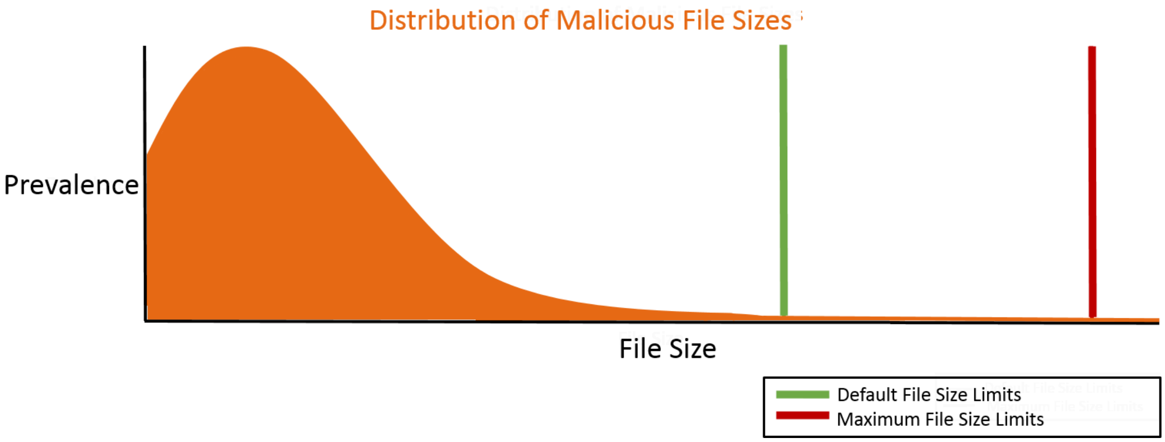


Figure 1: Recommended File Size Limits to Catch Uncommonly Large Malicious Files

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
ms-office	16,384KB	2,000KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
linux	50MB	10MB
script	20KB	20KB

Configure Advanced WildFire Analysis

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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

- Forward Files for Advanced WildFire Analysis
- Forward Decrypted SSL Traffic for Advanced WildFire Analysis
- Enable Advanced WildFire Inline ML
- Enable Advanced WildFire Inline Cloud Analysis
- Enable Hold Mode for Real-Time Signature Lookup
- Verify WildFire Submissions
- Manually Upload Files to the WildFire Portal
- Firewall File Forwarding Capacity by Model

Forward Files for Advanced WildFire Analysis

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Configure Palo Alto Networks firewalls to forward unknown files or email links and blocked files that match existing antivirus signatures for analysis. Use the **WildFire Analysis** profile to define files to forward to one of the Advanced WildFire public cloud options 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 has not been 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. For more information about using and configuring the WildFire appliance, refer to the WildFire Appliance Administration.

Before you begin:

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

Port	Usage
443	Registration, PCAP Downloads, Sample Downloads, Report Retrieval, File Submission, PDF Report Downloads
10443	Dynamic Updates

- Cloud Management
- PAN-OS & Panorama

Cloud Management

If you're using Panorama to manage Prisma Access:

*Toggle over to the **PAN-OS** tab and follow the guidance there.*

If you're using Prisma Access Cloud Management, continue here.

STEP 1 | Specify the Advanced WildFire cloud to which you want to forward samples.

Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus** > **General Settings** 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.

Add the **WildFire Cloud** URL for the cloud environment to forward samples to for analysis.

Advanced WildFire Public Cloud options:

1. Enter the **WildFire Public Cloud** URL:
   - United States: **`wildfire.paloaltonetworks.com`**
   - Europe: **`eu.wildfire.paloaltonetworks.com`**
   - Japan: **`jp.wildfire.paloaltonetworks.com`**
   - Singapore: **`sg.wildfire.paloaltonetworks.com`**
   - United Kingdom: **`uk.wildfire.paloaltonetworks.com`**
   - Canada: **`ca.wildfire.paloaltonetworks.com`**
   - Australia: **`au.wildfire.paloaltonetworks.com`**
   - Germany: **`de.wildfire.paloaltonetworks.com`**
   - India: **`in.wildfire.paloaltonetworks.com`**
   - Switzerland: **`ch.wildfire.paloaltonetworks.com`**
   - Poland: **`pl.wildfire.paloaltonetworks.com`**
   - Indonesia: **`id.wildfire.paloaltonetworks.com`**
   - Taiwan: **`tw.wildfire.paloaltonetworks.com`**
   - France: **`fr.wildfire.paloaltonetworks.com`**
   - Qatar: **`qatar.wildfire.paloaltonetworks.com`**
   - South Korea: **`kr.wildfire.paloaltonetworks.com`**
   - Israel: **`il.wildfire.paloaltonetworks.com`**
   - Saudi Arabia: **`sa.wildfire.paloaltonetworks.com`**
   - Spain: **`es.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.

STEP 2 | Enable Prisma Access to forward decrypted SSL traffic for Advanced WildFire analysis by selecting **Allow Forwarding of Decrypted Content**. Decrypted traffic is evaluated against security policy rules; if it matches the WildFire analysis profile attached to the security rule, the decrypted traffic is forwarded for analysis before it is re-encrypted.

Forwarding decrypted SSL traffic for analysis is an Advanced WildFire Best Practice.

STEP 3 | Define the size limits for samples the Prisma Access forwards for analysis.

It is a Advanced WildFire Best Practice to set the file forwarding values to the default setting.

STEP 4 | Configure submission log settings.

1. Select **Report Benign Files** to allow logging for files that receive a verdict of benign.
2. Select **Report Grayware Files** to allow logging for files that receive a verdict of grayware.

STEP 5 | When finished, **Save** your changes.

STEP 6 | Define traffic to forward for analysis.

1. Select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus**, and then **Add Profile**. Provide a **Name** and **Description** for the profile.
2. **Add Rule** to define traffic to be forwarded for analysis and give the rule a descriptive **Name**, such as local-PDF-analysis.
3. Define the profile rule to match to unknown traffic and to forward samples for analysis based on:
   - **Direction of Traffic**—Forward files for analysis based the transmission direction of the file (**Upload**, **Download**, or **Upload and Download**). For example, select **Upload and Download** to forward all unknown PDFs for analysis, regardless of the transmission direction.
   - **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.
   - Select the destination for traffic to be forwarded for Analysis.
     - Select **Public Cloud** so that all traffic matched to the rule is forwarded to the Advanced WildFire public cloud for analysis.
     - Select **Private Cloud** so that all traffic matched to the rule is forwarded to the WildFire appliance for analysis.
     - **Save** the WildFire analysis forwarding rule when finished.
4. **Save** the WildFire and Antivirus security profile.

STEP 7 | Enable the WildFire and Antivirus Security Profile.

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

STEP 8 | Push configuration changes.

STEP 9 | (Optional) Enable Advanced WildFire Inline ML

STEP 10 | Choose what to do next...

- Verify WildFire Submissions to confirm that the firewall is successfully forwarding files for analysis.
- Monitor WildFire Activity to assess alerts and details reported for malware.

PAN-OS & Panorama

STEP 1 | (PA-7000 Series Firewalls Only) To enable a PA-7000 Series firewall to forward samples for 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 samples.

STEP 2 | Specify the Advanced 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.

Advanced 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`**
   - Switzerland: **`ch.wildfire.paloaltonetworks.com`**
   - Poland: **`pl.wildfire.paloaltonetworks.com`**
   - Indonesia: **`id.wildfire.paloaltonetworks.com`**
   - Taiwan: **`tw.wildfire.paloaltonetworks.com`**
   - France: **`fr.wildfire.paloaltonetworks.com`**
   - Qatar: **`qatar.wildfire.paloaltonetworks.com`**
   - South Korea: **`kr.wildfire.paloaltonetworks.com`**
   - Israel: **`il.wildfire.paloaltonetworks.com`**
   - Saudi Arabia: **`sa.wildfire.paloaltonetworks.com`**
   - Spain: **`es.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.

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

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

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

> *It is a Advanced WildFire Best Practices 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 verdict of benign.
- Select **Report Grayware Files** to allow logging for files that receive a 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.

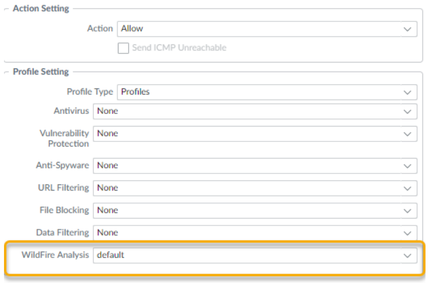
STEP 5 | Define traffic to forward for analysis.

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 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. Click **OK** to save the WildFire analysis profile.

STEP 6 | 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 firewalls 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



Action Setting

Action: Allow

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: None

Vulnerability Protection: None

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: default

STEP 7 | Make sure to enable the firewall to also Forward Decrypted SSL Traffic for Advanced WildFire Analysis.

This is a recommended best practice.

STEP 8 | (Optional) Enable Advanced WildFire Inline ML

STEP 9 | (Optional) Enable Hold Mode for Real-Time Signature Lookup

STEP 10 | Review and implement Advanced WildFire Best Practices.

STEP 11 | Click **Commit** to apply the updated settings.

STEP 12 | (Optional) Install a Device Certificate to update to the latest version of the certificate used by the firewall to communicate with Palo Alto Networks cloud services.

STEP 13 | (Optional) Configure the Content Cloud FQDN Settings.

STEP 14 | Choose what to do next...

- Verify WildFire Submissions to confirm that the firewall is successfully forwarding files for analysis.
- Monitor WildFire Activity to assess alerts and details reported for malware.

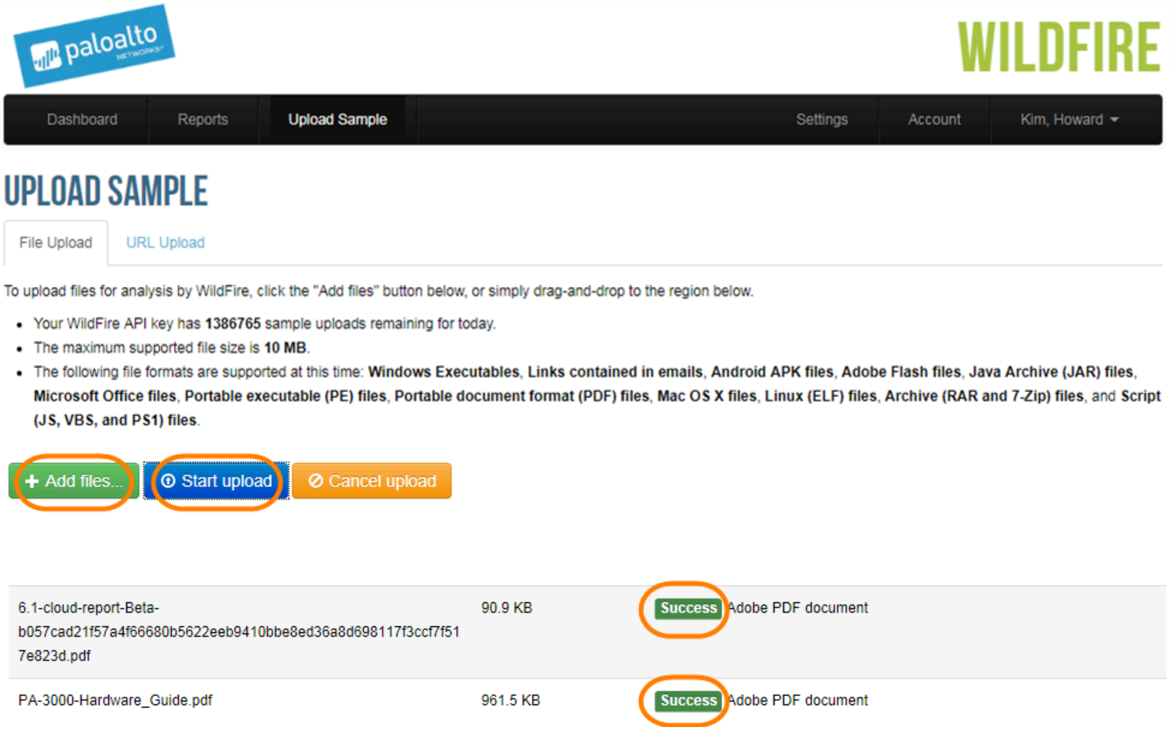
Manually Upload Files to the WildFire Portal

Where Can I Use This?	What Do I Need?
- Prisma Access (Managed by Strata Cloud Manager) - Prisma Access (Managed by Panorama) - NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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 analysis. If you have an Advanced WildFire or 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 analysis.Click **Start** to begin analysis of a single file, or click **Start Upload** to submit all the files you added for analysis.
   - To submit a URL for analysis, click **URL Upload**, enter a URL, and **Submit** for analysis.



UPLOAD SAMPLE

To upload files for analysis by WildFire, click the "Add files" button below, or simply drag-and-drop to the region below.

- Your WildFire API key has **1386765** sample uploads remaining for today.
- The maximum supported file size is **10 MB**.
- The following file formats are supported at this time: **Windows Executables**, **Links contained in emails**, **Android APK files**, **Adobe Flash files**, **Java Archive (JAR) files**, **Microsoft Office files**, **Portable executable (PE) files**, **Portable document format (PDF) files**, **Mac OS X files**, **Linux (ELF) files**, **Archive (RAR and 7-Zip) files**, and **Script (JS, VBS, and PS1) files**.

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 verdict and analysis results for the file.

Please wait at least five minutes for Advanced 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.

Forward Decrypted SSL Traffic for Advanced WildFire Analysis

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Enable the firewall to forward decrypted SSL traffic for Advanced 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 analysis before the firewall re-encrypts it. Only a super user can enable this option.

Forwarding decrypted SSL traffic for analysis is a Advanced WildFire Best Practices.

- 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 Advanced 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 Advanced WildFire Analysis.
  2. Select **Device** > **Virtual Systems**, click the virtual system you want to modify, and **Allow Forwarding of Decrypted Content**.

- For Prisma Access, this is configured as part of your **WildFire and Antivirus** security profile settings. For more information, refer to Forward Files for Advanced WildFire Analysis for Prisma Access.

Enable Advanced WildFire Inline Cloud Analysis

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

Palo Alto Networks Advanced WildFire operates a series of cloud-based ML detection engines that provide inline analysis of PE (portable executable) files traversing your network to detect and prevent advanced malware in real-time. As with other malicious content that WildFire detects, threats detected by Advanced WildFire Inline Cloud Analysis generate a signature that is then disseminated to customers through an update package, providing a future defense for all Palo Alto Networks customers.

The cloud-based engines enable the detection of never-before-seen malware (e.g., a Palo Alto Networks zero-day - malware previously unseen in the wild or by Palo Alto Networks) and block it from entering your environment. Advanced WildFire Inline Cloud Analysis uses a lightweight forwarding mechanism on the firewall to minimize performance impact. The cloud-based ML models are updated seamlessly, to address the ever-changing threat landscape without requiring content updates or feature release support.

Advanced WildFire Inline Cloud Analysis is enabled and configured through the WildFire Analysis profile and requires PAN-OS 11.1 or later with an active Advanced WildFire license.

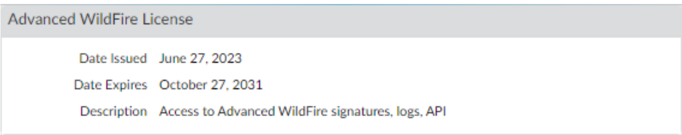
STEP 1 | Install an updated firewall device certificate used to authenticate to the Advanced WildFire cloud analysis service. Repeat for all firewalls enabled for inline cloud analysis.

This step is not necessary if you already installed the current version of the device certificate on your firewall.

STEP 2 | Log in to the PAN-OS web interface.

STEP 3 | To enable Advanced WildFire Inline Cloud Analysis, you must have an active Advanced WildFire subscription. For more information, refer to: Licensing, Registration, and Activation.

To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses are available and have not expired.



Advanced WildFire License

Date Issued June 27, 2023

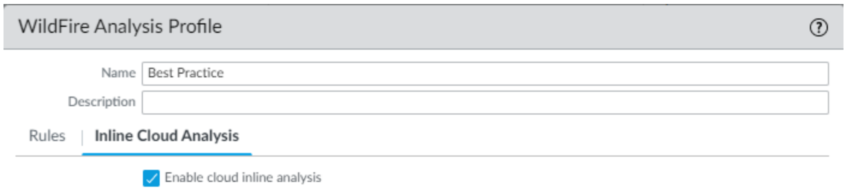
Date Expires October 27, 2031

Description Access to Advanced WildFire signatures, logs, API

If your current WildFire license has expired and you are installing an Advanced WildFire license, you must first remove the WildFire license from the NGFW before installing the Advanced WildFire license.

STEP 4 | Update or create a new WildFire Analysis Security profile to enable Advanced WildFire Inline Cloud Analysis.

1. Select an existing **WildFire Analysis Profile** or **Add** a new one (**Objects** > **Security Profiles** > **WildFire Analysis**).
2. Select your WildFire analysis profile and then go to **Inline Cloud Analysis** and **Enable cloud inline analysis**.



WildFire Analysis Profile

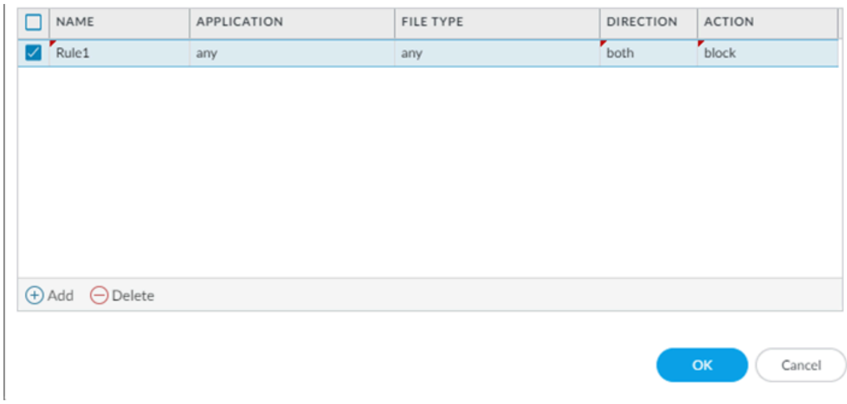
Name: Best Practice

Description:

Rules | Inline Cloud Analysis

☑ Enable cloud inline analysis

3. Specify a rule defining an action to take when Advanced WildFire Inline Cloud Analysis detects advanced malware.



□	NAME	APPLICATION	FILE TYPE	DIRECTION	ACTION
☑	Rule1	any	any	both	block

- Name—Enter a descriptive Name for any rules you add to the profile (up to 31 characters).
- Application—Add application traffic to match against for which the rules defining the Inline Cloud ML actions are governed.
- File Type—Select a File Type to be analyzed at the defined analysis destination for the rule.

  Only PE (portable executable) are supported at this time.

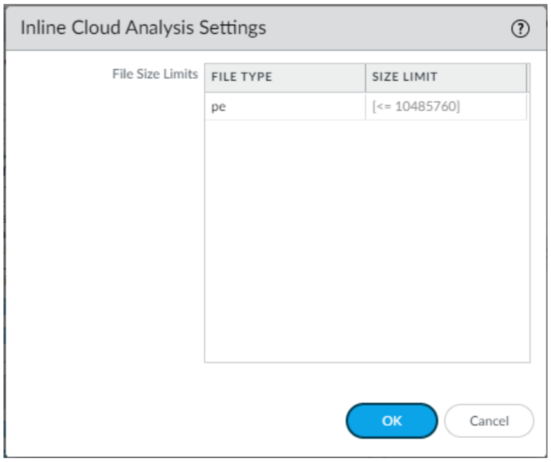
- Direction—Apply the rule to traffic depending on the transmission Direction. You can apply the rule to **download** traffic.
- Action—Configure the action to take when a threat is detected using Advanced WildFire Inline Cloud Analysis. You can **allow** the application traffic to continue to the destination or **block** traffic from either a source or a source-destination.

  Palo Alto Networks recommends setting the action to block for optimal security.

4. Click **OK** to exit the WildFire Analysis Profile configuration dialog.

STEP 5 | Review the maximum file size that can be forwarded for analysis using Advanced WildFire Inline Cloud Analysis.

Advanced WildFire Inline Cloud Analysis provides a fast WildFire verdict, however, a full report for a malicious sample is only available after the sample undergoes full dynamic analysis, which can take up to 30 minutes.

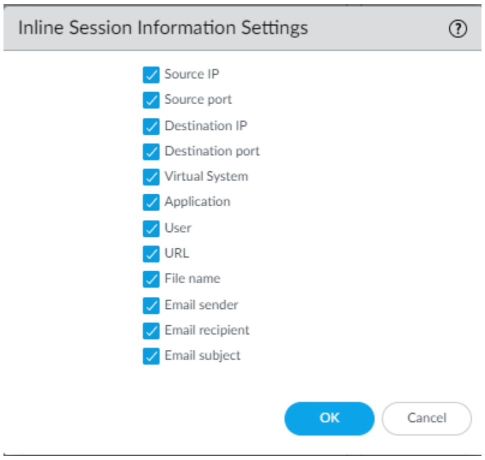


File Size Limits

FILE TYPE	SIZE LIMIT
pe	[<= 10485760]

1. Select **Device** > **Setup** > **WildFire** > **Inline Cloud Analysis Settings** and review the file size limits.
2. Click **OK** to confirm your changes.

STEP 6 | Specify the network session information that the firewall forwards about a given 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. These options are enabled by default.

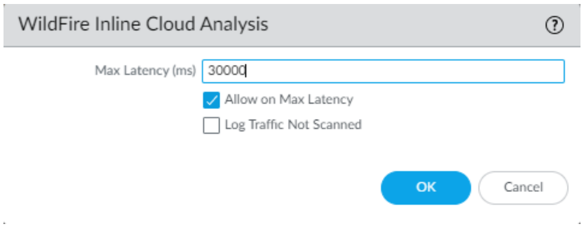


Inline Session Information Settings

☑ Source IP
☑ Source port
☑ Destination IP
☑ Destination port
☑ Virtual System
☑ Application
☑ User
☑ URL
☑ File name
☑ Email sender
☑ Email recipient
☑ Email subject

1. Select **Device** > **Setup** > **WildFire** > **Inline Session Information Settings** and select or clear the options as necessary.
   - **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).
2. Click **OK** to confirm your changes.

STEP 7 | Configure the timeout latency and action to take when the request exceeds the max latency.



Max Latency (ms) 30000

☑ Allow on Max Latency

□ Log Traffic Not Scanned

1. Specify the action to take when latency limits are reached for Advanced WildFire Inline Cloud Analysis requests:
   - Max Latency (ms)—Specify the maximum acceptable processing time, in seconds, for Advanced WildFire Inline Cloud Analysis to return a result.
   - Allow on Max Latency—Enables the firewall to take the action of allow, when the maximum latency is reached. De-selecting this option sets the firewall action to block.
   - Log Traffic Not Scanned— Enables the firewall to log Advanced WildFire Inline Cloud Analysis requests that exhibit the presence of advanced malware, but have not been processed by the Advanced WildFire cloud.
2. Click **OK** to confirm your changes.

STEP 8 | (Recommended) Configure the firewall to disable the client from fetching part of a file and subsequently starting a new session to fetch the rest of a file after the firewall terminates the original session due to detected malicious activity. This occurs when a web browser implements the HTTP Range option. While enabling **Allow HTTP partial response** provides maximum availability, it can also increase the risk of a successful cyberattack. Palo Alto Networks recommends disabling **Allow HTTP partial response** for maximum security.

__Allow HTTP partial response__ is a global setting and affects HTTP-based data transfers which use the RANGE header, which may cause service anomalies for certain applications. After you disable __Allow HTTP partial response__, validate the operation of your business-critical applications.

1. Select **Device** > **Setup** > **Content-ID** > **Content-ID Settings**.
2. De-select **Allow HTTP partial response** and click **OK**.

STEP 9 | **Commit** your changes.

STEP 10 | (Optional) Configure the Content Cloud FQDN Settings.

Enable Advanced WildFire Inline ML

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

You can prevent malicious variants of portable executables and PowerShell scripts from entering your network in real-time using machine learning (ML) based analytics on the firewall dataplane. By utilizing WildFire® Cloud analysis technology on your security platform, Advanced 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. Advanced 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.

To enable Advanced WildFire Inline ML, you must have an active Advanced WildFire or WildFire subscription, create (or modify) an Antivirus (or WildFire and Antivirus for Prisma Access) security profile to configure and enable the service, and then attach the Antivirus profile to a security policy rule.

Advanced WildFire Inline ML is not currently supported on the VM-50 or VM50L virtual appliance.

- Cloud Management
- PAN-OS & Panorama

PAN-OS & Panorama

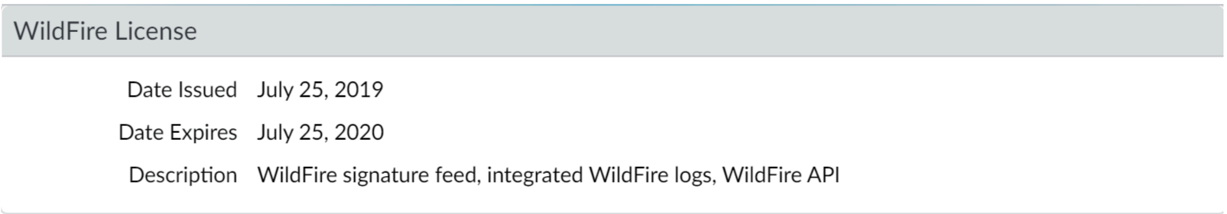
To enable your WildFire inline ML configuration, attach the Antivirus profile configured with the inline ML settings to a security policy rule.

To bypass Advanced WildFire Inline ML, you must set the **Action Setting** to **disable (for all protocols)** on a per-model basis or create a WildFire Inline ML file exception using the partial hash. Do not configure your antivirus profile with signature exceptions based off of WildFire Inline ML Threat IDs. This will cause the firewall to block all traffic from your network to the IP address.

WildFire inline ML is not currently supported on the VM-50 or VM50L virtual appliance.

STEP 1 | To take advantage of WildFire inline ML, you must have an active WildFire subscription to analyze Windows executables.

Verify that you have a WildFire subscription. To verify which subscriptions that you currently have licenses for, select **Device** > **Licenses** and verify that the appropriate licenses display and have not expired.



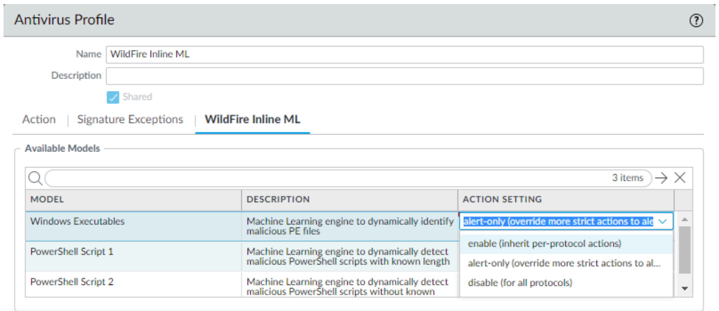
WildFire License

Date Issued	July 25, 2019
Date Expires	July 25, 2020
Description	WildFire signature feed, integrated WildFire logs, WildFire API

STEP 2 | Create a new or update your existing Antivirus security profile(s) to use the real-time WildFire inline ML models.

1. Select an existing **Antivirus Profile** or create a new one (select **Objects** > **Security Profiles** > **Antivirus** and **Add** a new profile.
2. Configure your Antivirus profile.
3. Select the **WildFire Inline ML** tab and apply an **Action Setting** for each WildFire Inline ML model. This enforces the WildFire Inline ML Actions settings configured for each protocol on a per model basis. The following classification engines available:

   - Windows Executables
   - PowerShell Scripts 1
   - PowerShell Scripts 2
   - Executable Linked Format (available with installation of PAN-OS content release 8367 and later)
   - MSOffice (available with installation of PAN-OS content release 8434 and later)
   - Shell Scripts (available with installation of PAN-OS content release 8543 and later)
   - OOXML (available with installation of PAN-OS 11.1.3 and later and PAN-OS content release 8825 and later)


Antivirus Profile
?
Action
Signature Exceptions
WildFire Inline ML
Available Models
3 items
enable (inherit per-protocol actions)
alert-only (override more strict actions to al...
disable (for all protocols)

Name WildFire Inline ML
Description
☑ Shared

MODEL	DESCRIPTION	ACTION SETTING
Windows Executables	Machine Learning engine to dynamically identify malicious PE files	alert-only (override more strict actions to ale
PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length	
PowerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts without known	

   The following action settings are available:

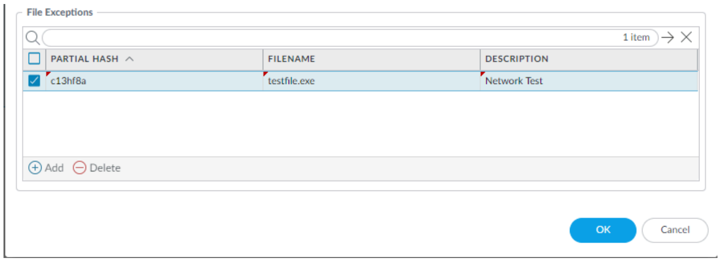
   - **enable (inherit per-protocol actions)**—WildFire inspects traffic according to your selections in the WildFire Inline ML Action column in the decoders section of the **Action** tab.
   - **alert-only (override more strict actions to alert)**—WildFire inspects traffic according to your selections in the WildFire Inline ML Action column in the decoders section of the **Action** tab and overrides any action with a severity level higher than `alert` (`drop`, `reset-client`, `reset-server`, `reset-both`) `alert`, which allows traffic to pass while still generating and saving an alert in the threat logs.
   - **disable (for all protocols)**—WildFire allows traffic to pass without any policy action.

4. Click **OK** to exit the Antivirus Profile configuration window and **Commit** your new settings.

STEP 3 | (Optional) Add file exceptions to your Antivirus security profile if you encounter false-positives. This is typically done for users who are not forwarding files to WildFire for analysis. You can add the file exception details directly to the exception list or by specifying a file from the threat logs.

If your WildFire Analysis security profile is configured to forward the filetypes analyzed using WildFire inline ML, false-positives are automatically corrected as they are received. If you continue to see ml-virus alerts for files that have been classified as benign by WildFire Analysis, please contact Palo Alto Networks Support.

- Add file exceptions directly to the exception list.
  1. Select **Objects** > **Security Profiles** > **Antivirus**.
  2. Select an Antivirus profile for which you want to exclude specific files and then select **WildFire Inline ML**.
  3. Add the hash, filename, and description of the file that you want to exclude from enforcement.

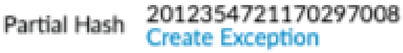


File Exceptions

1 item

☐	PARTIAL HASH	FILENAME	DESCRIPTION
☑	c13hf8a	testfile.exe	Network Test

  4. Click **OK** to save the Antivirus profile and then **Commit** your updates.
- Add file exceptions from threat logs entries.
  1. Select **Monitor** > **Logs** > **Threat** and filter the logs for the **ml-virus** threat type. Select a threat log for a file that you wish to create a file exception for.
  2. Go to the **Detailed Log View** and scroll down to the **Details** pane then select **Create Exception**.



Partial Hash 2012354721170297008

  3. Add a **Description** and click **OK** to add the file exception.
  4. The new file exception can be found **File Exceptions** list under **Objects** > **Security Profiles** > **Antivirus** > **WildFire Inline ML**.

STEP 4 | (Optional) Verify the status of your firewall's connectivity to the Inline ML cloud service.

Use the following CLI command on the firewall to view the connection status.

```
show mlav cloud-status
```

For example:

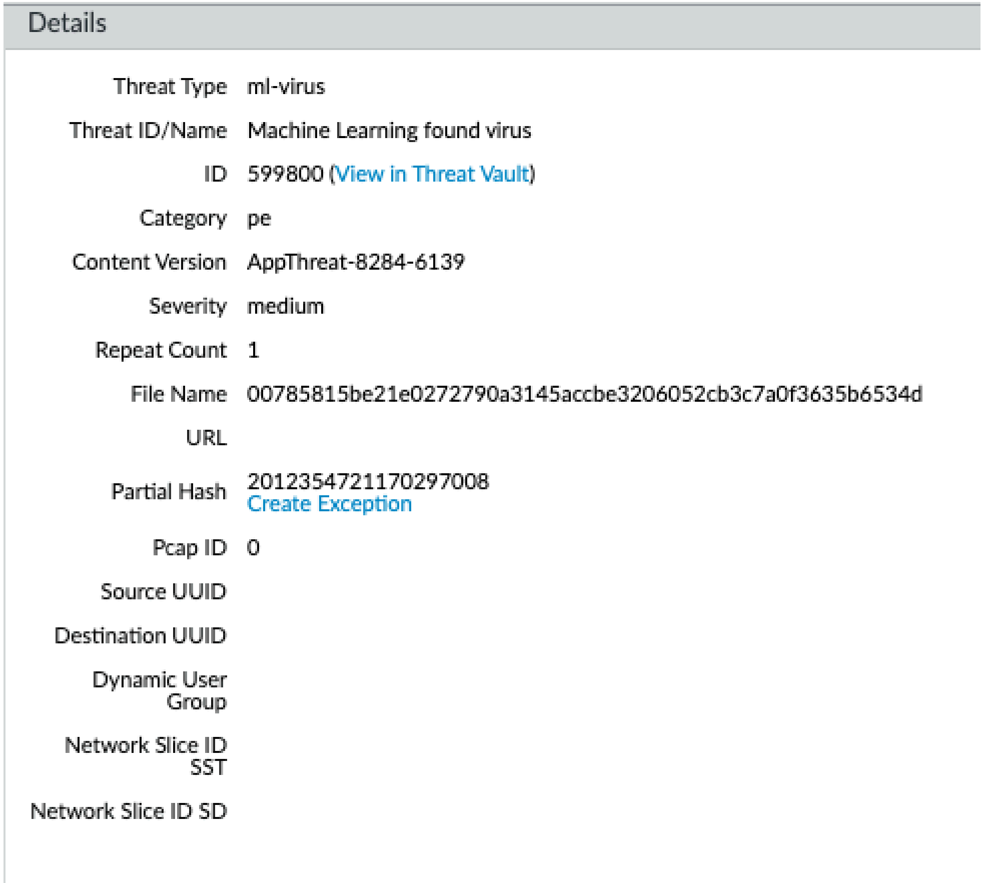
```
show mlav cloud-status

MLAV cloud
Current cloud server:          ml.service.paloaltonetworks.com
```

```
Cloud connection:                  connected
```

If you are unable to connect to the Inline ML cloud service, verify that the following domain is not being blocked: ml.service.paloaltonetworks.com.

STEP 5 | (Optional) Configure the Content Cloud FQDN Settings.

To view information about files that have been detected using WildFire Inline ML, examine the threat logs (**Monitor > Logs > Threat**, then select the log type from the list). Files that have been analyzed using WildFire inline ML are labeled with the threat type **ml-virus**:



Details

Threat Type: ml-virus
Threat ID/Name: Machine Learning found virus
ID: 599800 (View in Threat Vault)
Category: pe
Content Version: AppThreat-8284-6139
Severity: medium
Repeat Count: 1
File Name: 00785815be21e0272790a3145accbe3206052cb3c7a0f3635b6534d
URL:
Partial Hash: 2012354721170297008 Create Exception
Pcap ID: 0
Source UUID:
Destination UUID:
Dynamic User Group:
Network Slice ID SST:
Network Slice ID SD:

Cloud Management

If you're using Panorama to manage Prisma Access:

*Toggle over to the **PAN-OS** tab and follow the guidance there.*

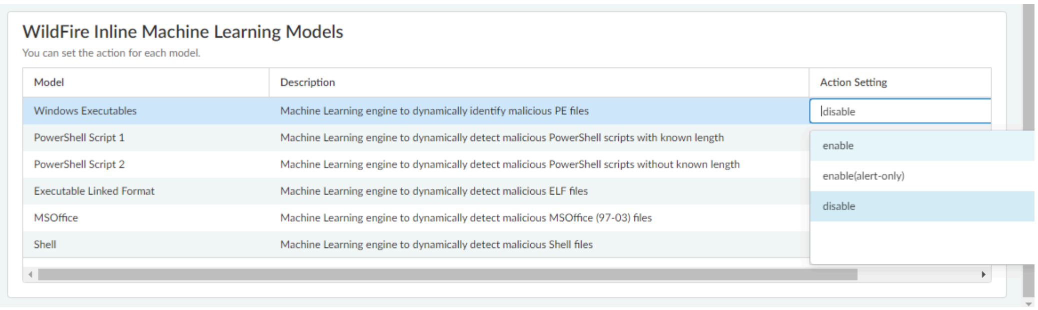
If you're using Prisma Access Cloud Management, continue here.

STEP 1 | To take advantage of WildFire Inline ML, you must have an active WildFire subscription as part of your Prisma Access subscription.

Verify that you have a valid and unexpired WildFire subscription.

STEP 2 | Create a new or update your existing **WildFire and Antivirus** security profile to use the real-time WildFire inline ML models.

1. Select an existing **WildFire and Antivirus** security profile or create a new one (select **Manage** > **Configuration** > **NGFW and Prisma Access** > **Security Services** > **WildFire and Antivirus** and **Add Profile**.
2. Configure your WildFire and Antivirus profile to forward samples for analysis.
3. Select **WildFire Inline Machine Learning Models** and apply an **Action Setting** for each WildFire Inline ML model. This enforces the WildFire Inline ML Actions settings configured for each protocol on a per model basis.



WildFire Inline Machine Learning Models

You can set the action for each model.

Model	Description	Action Setting
Windows Executables	Machine Learning engine to dynamically identify malicious PE files	disable
PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length	
PowerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts without known length	
Executable Linked Format	Machine Learning engine to dynamically detect malicious ELF files	
MSOffice	Machine Learning engine to dynamically detect malicious MSOffice (97-03) files	
Shell	Machine Learning engine to dynamically detect malicious Shell files	

The following classification engines available:

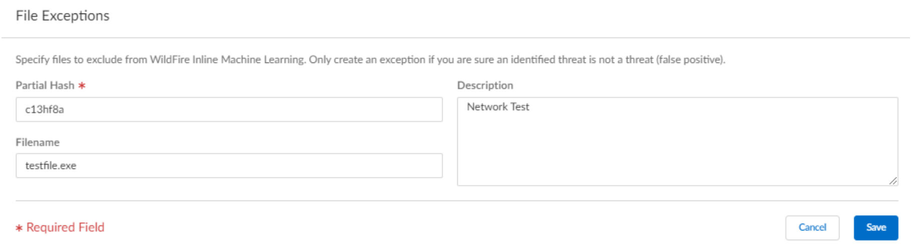
- Windows Executables
- PowerShell Scripts 1
- PowerShell Scripts 2
- Executable Linked Format
- MSOffice
- Shell Scripts
- **enable**—WildFire inspects traffic according to your selections in the WildFire Inline ML Action column in the decoders section of the **Action** tab.
- **enable(alert-only)**—WildFire inspects traffic according to your selections in the WildFire Inline ML Action column in the decoders section of the **Action** tab and overrides any action with a severity level higher than `alert` (`drop`, `reset-client`, `reset-server`, `reset-both`) `alert`, which allows traffic to pass while still generating and saving an alert in the threat logs.
- **disable**—WildFire allows traffic to pass without any policy action.

STEP 3 | (Optional) Add file exceptions to your WildFire and Antivirus security profile if you encounter false-positives. This is typically done for users who are not forwarding files to

WildFire for analysis. You can add the file exception details directly to the exception list or by specifying a file from the threat logs.

> *If your WildFire Analysis security profile is configured to forward the filetypes analyzed using WildFire inline ML, false-positives are automatically corrected as they are received. If you continue to see ml-virus alerts for files that have been classified as benign by WildFire Analysis, please contact Palo Alto Networks Support.*

- Add file exceptions directly to the exception list.
  1. Select **Advanced Settings** and **Add Exception** in the **File Exceptions** pane.
  2. Add the hash, filename, and description of the file that you want to exclude from enforcement.



File Exceptions

Specify files to exclude from WildFire Inline Machine Learning. Only create an exception if you are sure an identified threat is not a threat (false positive).

Partial Hash * : c13hf8a

Filename: testfile.exe

Description: Network Test

* Required Field

  3. When finished, **Save** your file exceptions.

STEP 4 | **Save** your WildFire and Antivirus profile configuration and push configuration changes.

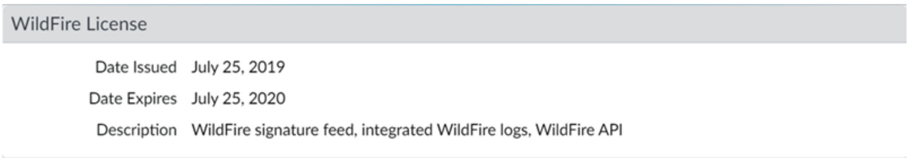
Enable Hold Mode for Real-Time Signature Lookup

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

You can configure the NGFW to hold the transfer of a sample while the real-time signature cloud performs a signature lookup. When the lookup is completed, the file is released to the requesting client (or blocked), based on your organization's security policy for specific WildFire verdicts, preventing the initial transfer of known malware. You can configure hold mode on a per antivirus profile basis and apply a global setting for the signature lookup timeout and the associated action.

This feature is available to all users with an active WildFire or Advanced WildFire license running PAN-OS 11.0.2 or later.

STEP 1 | To enable hold mode for WildFire real-time signature lookups, you must have either a WildFire or Advanced WildFire subscription service license. Make sure to activate the license on the firewall if you have not done so already. To verify subscriptions for which you have currently-active licenses, select **Device** > **Licenses** and verify that the appropriate licenses display and are not expired. The example below shows the description for the standard WildFire license.



WildFire License

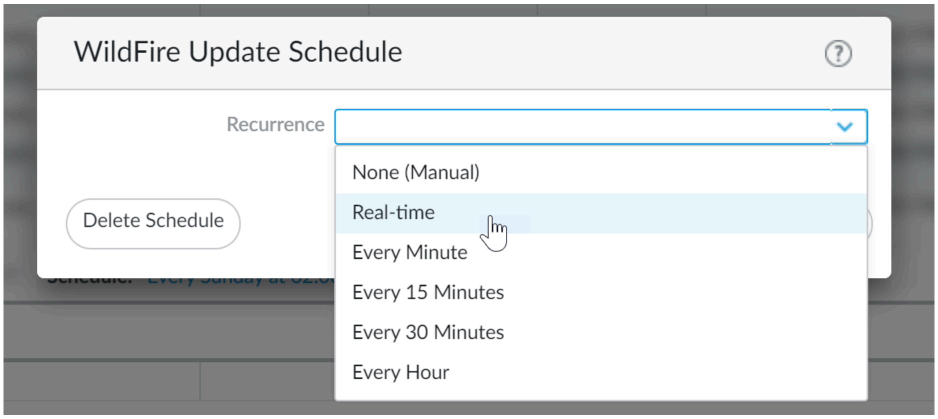
Date Issued July 25, 2019

Date Expires July 25, 2020

Description WildFire signature feed, integrated WildFire logs, WildFire API

STEP 2 | Set the schedule for the firewall to retrieve WildFire signatures in real-time.

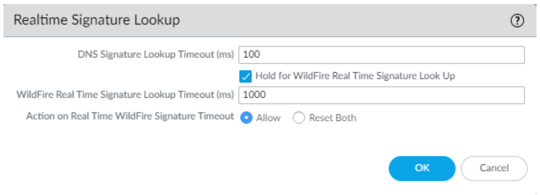
Even when the firewall is configured to use real-time signatures, supplemental signature packages are still installed on a regular basis. This provides an up-to-date signature source when you experience connectivity issues, as well as a speed benefit, where signatures are available locally.



1. Select **Device** > **Dynamic Updates**.
2. Select the **Schedule** for WildFire updates.
3. Set the **Recurrence** (how often the firewall checks the Palo Alto Networks update server for new signatures) for **Real-time** updates.
4. Click **OK** to save the WildFire update schedule and then **Commit** your changes.

STEP 3 | Configure the timeout setting and action when the request exceeds the timeout.

You must enable hold mode globally before you enable hold mode for WildFire real-time signature lookups on a per-Antivirus profile basis.


Realtime Signature Lookup

DNS Signature Lookup Timeout (ms) 100

☑ Hold for WildFire Real Time Signature Look Up

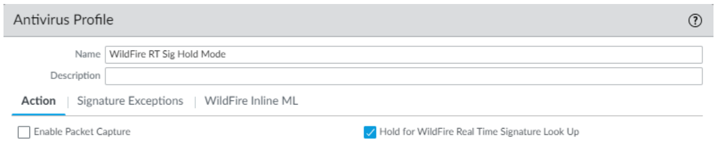
WildFire Real Time Signature Lookup Timeout (ms) 1000

Action on Real Time WildFire Signature Timeout ● Allow ○ Reset Both

1. Select **Device Setup** > **ContentID** > **Realtime Signature Lookup**
2. Enable **Hold for WildFire Real Time Signature Look Up**.
3. Specify the **WildFire Real Time Signature Lookup Timeout (ms)** in milliseconds (the default value is 1000).

   Palo Alto Networks recommends using the default value of 1000ms unless you experience repeated timeouts during testing.
4. Specify the **Action On Real Time WildFire Signature Timeout**. The default value is **Allow**, however, Palo Alto Networks recommends setting this to **Reset-Both** when hold mode is enabled. The options include the following:
   - Allow—The NGFW allows packets through when the hold timeout threshold is reached.
   - Reset Both—The NGFW resets the connection on both the client and server ends when the hold timeout threshold is reached.
5. Select **OK** when finished.

STEP 4 | Update or create a new Antivirus Security profile to enable hold mode for WildFire real-time signature lookups.



Antivirus Profile

Name WildFire RT Sig Hold Mode

Description

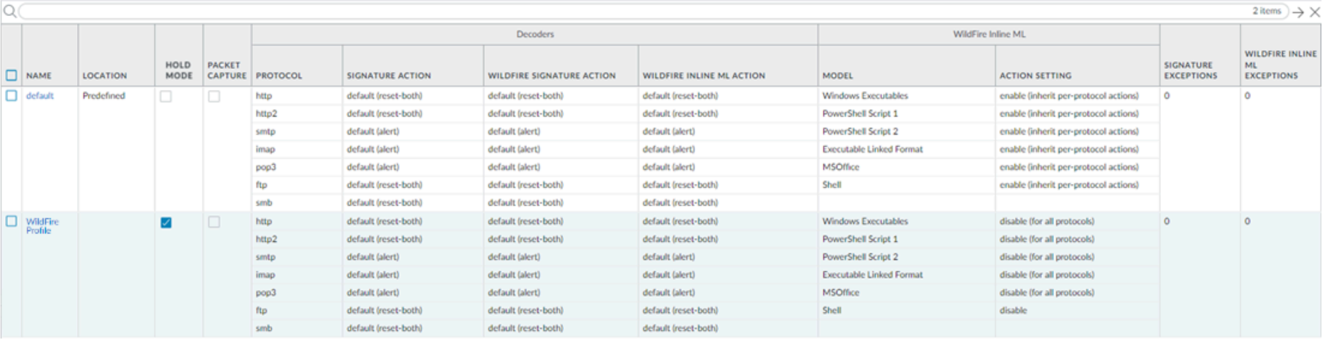
□ Enable Packet Capture

☑ Hold for WildFire Real Time Signature Look Up

1. Select an existing antivirus security profile or **Add** a new one (**Objects** > **Security Profiles** > **Antivirus**).
2. Select your antivirus security profile and then go to **Action**.
3. Select **Hold for WildFire Real Time Signature Look Up**.
4. Repeat steps 4.1-4.3 for all active antivirus profiles for which you want to enable hold mode for WildFire real-time signature lookups.

STEP 5 | **Commit** your changes.

STEP 6 | (Optional) You can view a summary of your antivirus security profile settings, including hold mode enablement, on the antivirus summary view page.



					Decoders				WildFire Inline ML			
□	NAME	LOCATION	HOLD MODE	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING	SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
□	default	Predefined	□	□	http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
					http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
					smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
					imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
					pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
					ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
					smb	default (reset-both)	default (reset-both)	default (reset-both)				
□	WildFire Profile		☑	□	http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
					http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
					smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
					imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
					pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
					ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
					smb	default (reset-both)	default (reset-both)	default (reset-both)				

Configure the Content Cloud FQDN Settings

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

You can specify the cloud content Fully Qualified Domain Name (FQDN) used by the NGFW to handle Advanced WildFire service requests. The default FQDN connects to hawkeye.services-edge.paloaltonetworks.com and then resolves to the closest cloud services server. You can override the automatic server selection by specifying a regional cloud content server that best meets your data residency and performance requirements. Keep in mind, the cloud content FQDN is a globally used resource and affects how other services that rely on this connection sends traffic payloads.

In some cases, the cloud content FQDN might not fully support the functionality of a particular Palo Alto Networks product in certain regions. Verify that the product is fully supported before changing the cloud content FQDN.

Depending on which services you use, the cloud content FQDN facilitates analysis service requests, including traffic payloads, which sends data to the servers in the selected region. If you specify a content cloud FQDN that is outside of your region (for example, if you are in the EU region but you specify the APAC region FQDN), you may be in violation of your organization's privacy and legal regulations. Please refer to the specific product documentation for information about how the cloud content FQDN is used by your Palo Alto Networks products.

If you are experience service connectivity issues, verify that the configured cloud content FQDN is not being blocked.

STEP 1 | Log in to the PAN-OS web interface.

STEP 2 | Select (**Device** > **Setup** > **Content-ID** > **Content Cloud Settings**) and change the FQDN as desired:

- Default—**`hawkeye.services-edge.paloaltonetworks.com`**
- US Central (Iowa, US)—**`us.hawkeye.services-edge.paloaltonetworks.com`**
- Europe (Frankfurt, Germany)—**`eu.hawkeye.services-edge.paloaltonetworks.com`**
- APAC (Singapore)—**`apac.hawkeye.services-edge.paloaltonetworks.com`**
- India (Mumbai)—**`in.hawkeye.services-edge.paloaltonetworks.com`**
- UK (London, England)—**`uk.hawkeye.services-edge.paloaltonetworks.com`**
- France (Paris, France)—**`fr.hawkeye.services-edge.paloaltonetworks.com`**
- Japan (Tokyo, Japan)—**`jp.hawkeye.services-edge.paloaltonetworks.com`**
- Australia (Sydney, Australia)—**`au.hawkeye.services-edge.paloaltonetworks.com`**
- Canada (Montréal, Canada)—**`ca.hawkeye.services-edge.paloaltonetworks.com`**
- Switzerland—**`ch.hawkeye.services-edge.paloaltonetworks.com`**
- Netherlands—**`nl.hawkeye.services-edge.paloaltonetworks.com`**
- Indonesia—**`id.hawkeye.services-edge.paloaltonetworks.com`**
- Qatar—**`qa.hawkeye.services-edge.paloaltonetworks.com`**
- Taiwan—**`tw.hawkeye.services-edge.paloaltonetworks.com`**
- Poland—**`pl.hawkeye.services-edge.paloaltonetworks.com`**
- South Korea (Seoul, South Korea)—**`kr.hawkeye.services-edge.paloaltonetworks.com`**
- Saudi Arabia—**`sa.hawkeye.services-edge.paloaltonetworks.com`**
- Italy—**`it.hawkeye.services-edge.paloaltonetworks.com`**

STEP 3 | Click **OK**.

Verify Sample Submissions

Where Can I Use This?	What Do I Need?
- NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	□ Advanced WildFire License

Test your deployment 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

Where Can I Use This?	What Do I Need?
- NGFW (Managed by PAN-OS or Panorama) - VM-Series - CN-Series	□ Advanced WildFire or WildFire License

Palo Alto Networks provides sample malware files that you can use to test an Advanced WildFire configuration. Take the following steps to download the malware sample file, verify that the file is forwarded for Advanced 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

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire or WildFire License

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

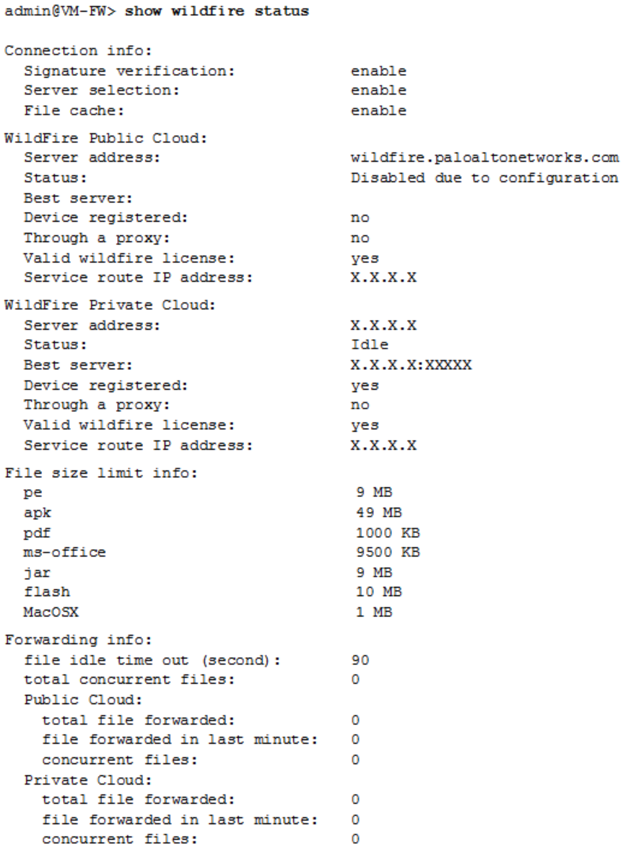
Several of the options to verify that a firewall is forwarding samples for analysis are CLI commands; for details on getting started with and using the CLI, refer to the PAN-OS CLI Quick Start Guide.

- Verify the status of the firewall connection to the Advanced WildFire public and/or WildFire 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 Advanced WildFire public and/or WildFire private cloud to which the firewall is connected. The status `Idle` indicates that the Advanced 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 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 `show wildfire 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 Advanced 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 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 Advanced WildFire public or WildFire private cloud:

  - The command displays the output of a working firewall and shows counters for each file type that the firewall forwards for 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 an Advanced WildFire public or WildFire private cloud.
  - `FWD_CNT_LOCAL_FILE`— Indicates the total number of email links uploaded to an Advanced WildFire public or WildFire private cloud.

- 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:

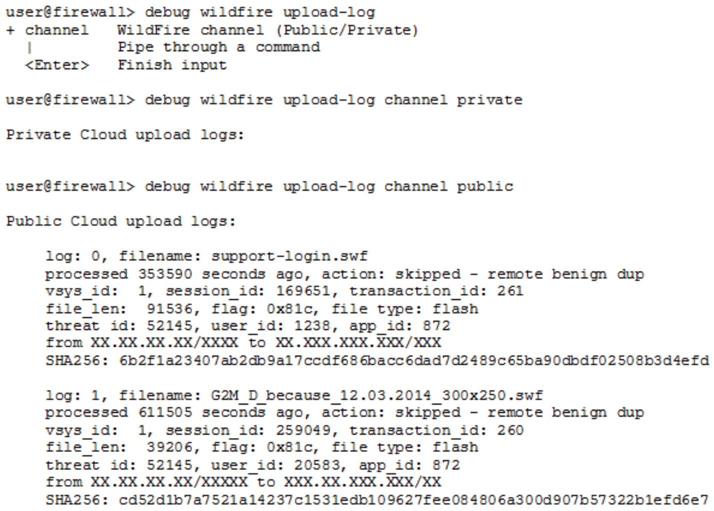
  - Confirm that samples that have not yet received a verdict were correctly forwarded by the firewall. Because **WildFire Submissions** are logged on the firewall only when analysis is complete and the sample has received a verdict, use this option to verify the firewall forwarded a sample that is currently undergoing 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 analysis.
- Check that a firewall in a hybrid cloud deployment is forwarding the correct file types and email links to either the Advanced WildFire public cloud or a WildFire private cloud.

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

- View all samples forwarded by the firewall with the CLI command **`debug wildfire upload-log`**.
- View only samples forwarded to the Advanced 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 an Advanced 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/XXXX 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 analysis.

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

- Check the 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 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. This is useful when deploying a hybrid cloud.

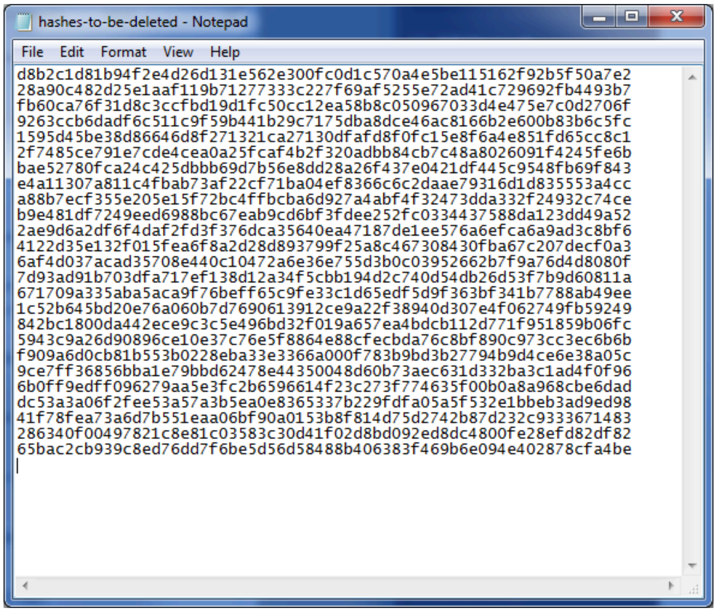
Sample Removal Request

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Unique samples sent to the Advanced 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.

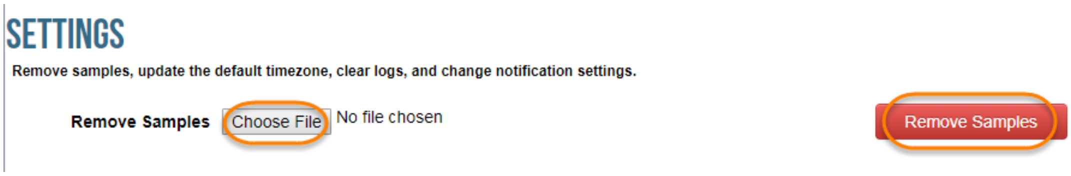


```
d8b2c1d81b94f2e4d26d131e562e300fc0d1c570a4e5be115162f92b5f50a7e2
28a90c482d25e1aaf119b71277333c227f69af5255e72ad41c729692fb4493b7
fb60ca76f31d8c3ccfbd19d1fc50cc12ea58b8c050967033d4e475e7c0d2706f
9263ccb6dadf6c511c9f59b441b29c7175dba8dce46ac8166b2e600b83b6c5fc
1595d45be38d86646d8f271321ca27130dfafd8f0fc15e8f6a4e851fd65cc8c1
2f7485ce791e7cde4cea0a25fcaf4b2f320adbb84cb7c48a8026091f4245fe6b
bae52780fca24c425dbbb69d7b56e8dd28a26f437e0421df445c9548fb69f843
e4a11307a811c4fbab73af22cf71ba04ef8366c6c2daae79316d1d835553a4cc
a88b7ecf355e205e15f72bc4ffbcba6d927a4abf4f32473dda332f24932c74ce
b9e481df7249eed6988bc67eab9cd6bf3fdee252fc0334437588da123dd49a52
2ae9d6a2df6f4daf2fd3f376dca35640ea47187de1ee576a6efca6a9ad3c8bf6
4122d35e132f015fea6f8a2d28d893799f25a8c467308430fba67c207decf0a3
6af4d037acad35708e440c10472a6e36e755d3b0c03952662b7f9a76d4d8080f
7d93ad91b703dfa717ef138d12a34f5cbb194d2c740d54db26d53f7b9d60811a
671709a335aba5aca9f76beff65c9fe33c1d65edf5d9f363bf341b7788ab49ee
1c52b645bd20e76a060b7d7690613912ce9a22f38940d307e4f062749fb59249
842bc1800da442ece9c3c5e496bd32f019a657ea4bdcb112d771f951859b06fc
5943c9a26d90896ce10e37c76e5f8864e88cfecbda76c8bf890c973cc3ec6b6b
f909a6d0cb81b553b0228eba33e3366a000f783b9bd3b27794b9d4ce6e38a05c
9ce7ff36856bba1e79bbd62478e44350048d60b73aec631d332ba3c1ad4f0f96
6b0ff9edff096279aa5e3fc2b6596614f23c273f774635f00b0a8a968cbe6dad
dc53a3a06f2fee53a57a3b5ea0e8365337b229fdfa05a5f532e1bbeb3ad9ed98
41f78fea73a6d7b551eaa06bf90a0153b8f814d75d2742b87d232c933367148 3
286340f00497821c8e81c03583c30d41f02d8bd092ed8dc4800fe28efd82df82
65bac2cb939c8ed76dd7f6be5d56d58488b406383f469b6e094e402878cfa4be
```

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

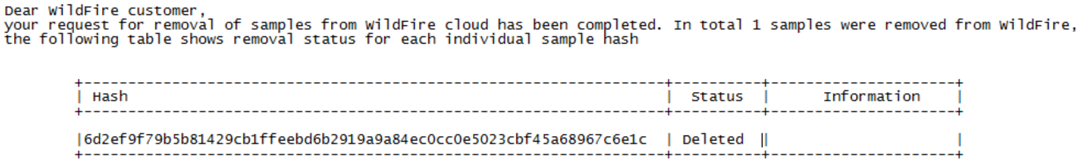
STEP 3 | Select **Settings** on the menu bar.

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
Choose File
No file chosen
Remove Samples

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

        |6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c  | 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

Where Can I Use This?	What Do I Need?
- NGFW (Managed by PAN-OS or Panorama) - VM-Series	□ Advanced WildFire License

File-forwarding capacity is the maximum rate per minute at which each Palo Alto Networks firewall model can submit files to the Advanced WildFire® cloud 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 the Advanced WildFire cloud 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-3400 Series	100	500MB

Platform	Maximum Files Per Minute	Reserved Drive Space
PA-5200 Series	250	1500MB
PA-5400 Series	250	1500MB
PA-7000 Series	300	1GB

Monitor Activity

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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.

You can also view how Advanced WildFire integrates with other Palo Alto Networks applications and security services to protect your organization from threats, as well as get a high-level view of the overall operational health of your deployment, through The Strata Cloud Manager Command Center. The command center functions as your NetSec homepage and provides a comprehensive summary of the health, security, and efficiency of your network, in an interactive visual dashboard with multiple data facets for easy, at-a-glace assessment.

Depending on the product platform, you can access high-level dashboards that provide Advanced WildFire malware detection statistics and usage trends, including context into network activity in the form of analysis insights and more.

Palo Alto Networks provides several methods to monitor the Advanced WildFire activity:

- The Strata Cloud Manager Command Center
- Advanced WildFire Dashboard
- About WildFire Logs and Reporting
- Configure WildFire Submission Log Settings
- Use the WildFire Portal to Monitor Malware
- WildFire Analysis Reports—Close Up
- Set Up Alerts for Malware

About WildFire Logs and Reporting

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

You can Monitor Activityon the firewall, with the WildFire portal, Strata Cloud Manager, 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. 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.
- On Strata Cloud Manager—All samples submitted by Prisma Access for WildFire analysis are logged as WildFire logs and can be perused through the Strata Cloud Manager Log Viewer. You can view the traffic details, context, and other relevant details, include information about how the sample progressed through your network.
- With the WildFire API—Retrieve WildFire analysis reports from a WildFire appliance or from the WildFire public cloud.

Advanced WildFire Analysis Reports—Close Up

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama)	□ Advanced WildFire License

Where Can I Use This?	What Do I Need?
• VM-Series • CN-Series	

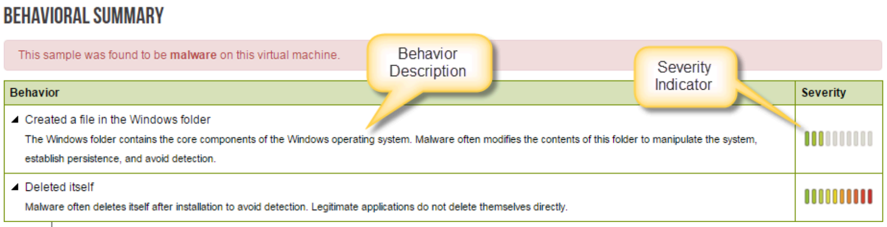
Access Advanced WildFire analysis reports on the firewall, the WildFire portal, and the WildFire API.

Advanced 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. Advanced 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 an Advanced 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	• **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: • **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.

Report Heading	Description
Coverage Status	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. 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 will also be displayed in this section. Because this information is retrieved dynamically, it will not appear in the PDF report. The following coverage information is provided for active signatures: • **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	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**. The following options are available: • Source IP • Source Port • Destination IP • Destination Port • Virtual System (If multi-vsys is configured on the firewall) • Application • User (If User-ID is configured on the firewall) • URL • Filename

Report Heading	Description
	- Email sender - Email recipient - Email subject By default, session information includes the field Status, which indicates if the firewall allowed or blocked the sample.
Dynamic Analysis	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 analysis. When dynamic 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 4 tab might show an analysis environment operating Windows 7, Adobe Reader 11, Flash 11, and Office 2010. *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.*
Behavior Summary	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. 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.  BEHAVIORAL SUMMARY This sample was found to be **malware** on this virtual machine. Behavior | Severity ◢ 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. ◢ Deleted itself Malware often deletes itself after installation to avoid detection. Legitimate applications do not delete themselves directly. The following describes the various behaviors that are analyzed:

Report Heading	Description
	• **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. • **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. *The activity timeline information is only available in the PDF export of the WildFire reports.*
Submit Malware	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.
Report an Incorrect Verdict	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.

Configure WildFire Submission Log Settings

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

A WildFire submissions log is an automatically generated, time-stamped file that provides an audit trail to track events when a Palo Alto Networks network security platform forwards samples (files and emails links) to the WildFire cloud for analysis based on WildFire Analysis profile settings (Objects > Security Profiles > WildFire Analysis). WildFire Submissions log entries are generated for each sample forwarded to the WildFire cloud that has completed static and/or dynamic analysis of the sample. WildFire Submissions log entries include the Action taken on the sample (allow or block), the WildFire verdict for the submitted sample as determined through WildFire analysis, the severity level of the sample, and other details.

By default, WildFire submissions logs are created for Benign and Malicious samples; while Grayware and Benign samples generate no logs. You can change the WildFire submission log settings to include Grayware and Benign samples as well as additional session information contained in email links.

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

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

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

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

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.

Set Up Alerts for Malware

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License

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.

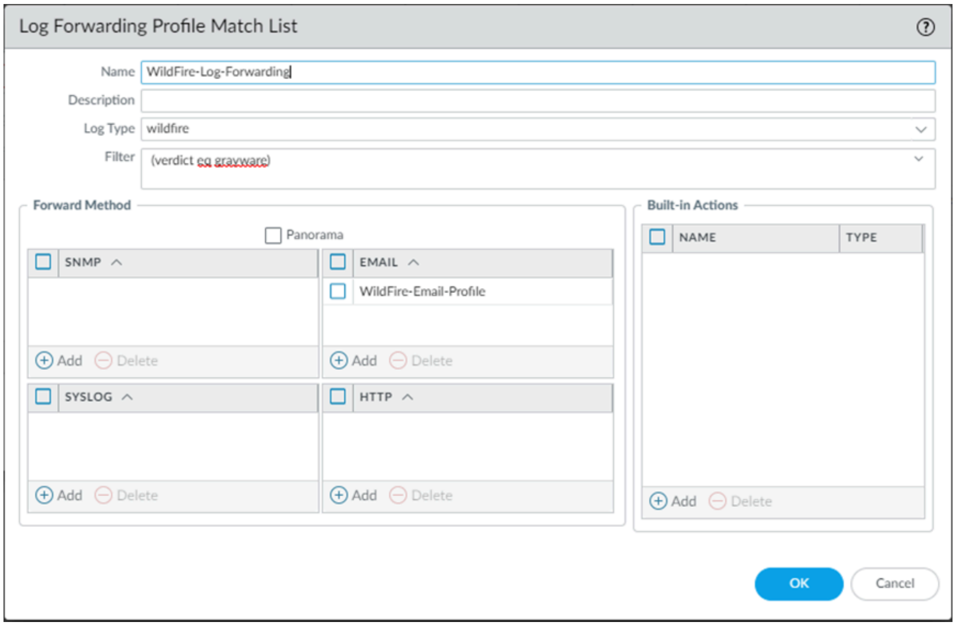
1. Select **Monitor** > **PDF Reports** > **Email Scheduler**.
2. Click **Add** and select the new email profile from the **Email Profile** drop-down.
3. Click the **Send test email** button and a test email should be sent to the recipients defined in the email profile.

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.



Log Forwarding Profile Match List

Name: WildFire-Log-Forwarding

Description:

Log Type: wildfire

Filter: (verdict eq grayware)

Forward Method

□ Panorama

□	SNMP

□	EMAIL
□	WildFire-Email-Profile

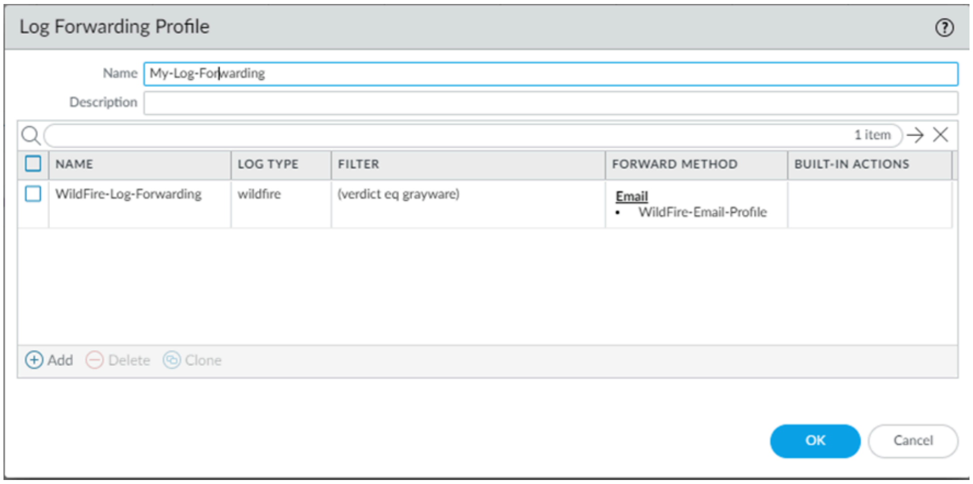
□	SYSLOG

□	HTTP

Built-in Actions

□	NAME	TYPE

   1. Provide a name for the **Log Fowarding 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.


Log Forwarding Profile

Name My-Log-Forwarding

Description

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
WildFire-Log-Forwarding	wildfire	(verdict eq grayware)	Email • WildFire-Email-Profile	

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 Advanced WildFire analysis. To set up a WildFire analysis profile and attach it to a security policy rule, see Forward Files for Advanced 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.

View WildFire Logs and Analysis Reports

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

WildFire logs contain information on samples (files and email links) uploaded to the WildFire cloud for analysis. It includes artifacts, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker as well as WildFire-specific qualities, such as high-level analysis results including categorization of the sample as malware, phishing, grayware, or benign and details sample information. Reviewing the WildFire Submissions logs can also indicate whether a user in your networks downloaded a suspicious file. The WildFire analysis report displays 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. It informs you if the file is malicious, if it modified registry keys, read/wrote into files, created new files, opened network communication channels, caused application crashes, spawned processes, downloaded files, or exhibited other malicious behavior.

WildFire logs are displayed as WildFire submissions logs on NGFW firewalls, while on Cloud Management platforms, you must first configure log forwarding to upload relevant logs to CDL (Cortex Data Lake), which will then show the WildFire logs as threat logs (type WildFire).

- Cloud Management
- PAN-OS & Panorama

PAN-OS & Panorama

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 Advanced WildFire Analysis.

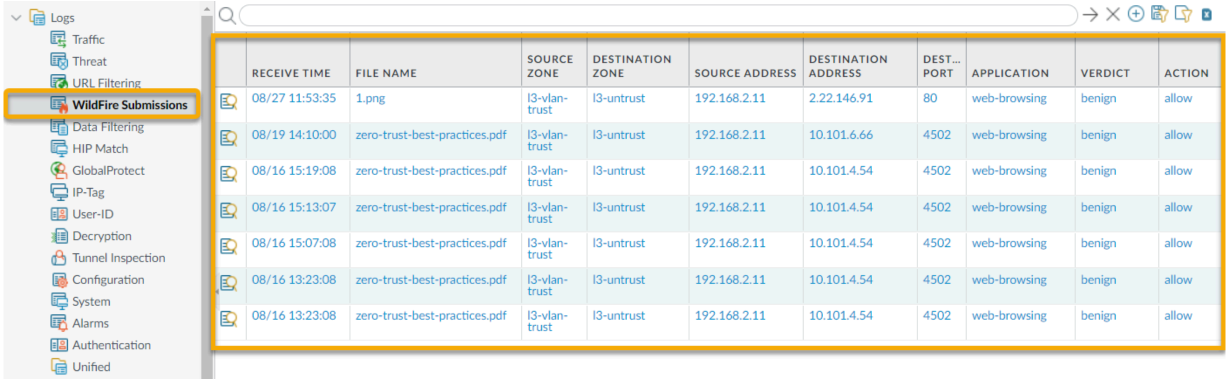
STEP 2 | Configure WildFire Submissions Log Settings.

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.

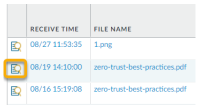
The values for the following severity levels are determined by a combination of verdict and action values.

- *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.*



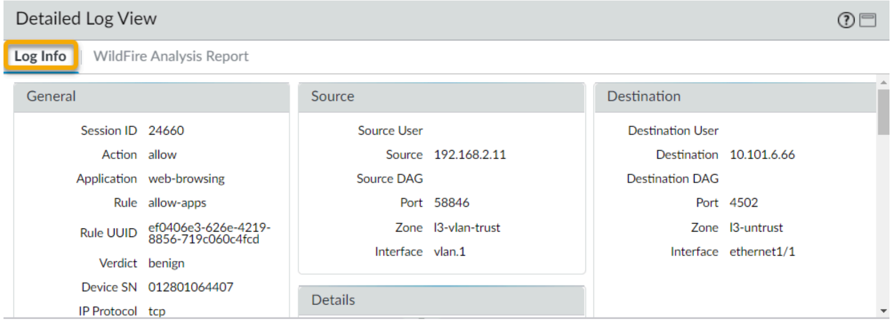
RECEIVE TIME	FILE NAME	SOURCE ZONE	DESTINATION ZONE	SOURCE ADDRESS	DESTINATION ADDRESS	DEST... PORT	APPLICATION	VERDICT	ACTION
08/27 11:53:35	1.png	l3-vlan-trust	l3-untrust	192.168.2.11	2.22.146.91	80	web-browsing	benign	allow
08/19 14:10:00	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.6.66	4502	web-browsing	benign	allow
08/16 15:19:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:13:07	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 15:07:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-untrust	192.168.2.11	10.101.4.54	4502	web-browsing	benign	allow
08/16 13:23:08	zero-trust-best-practices.pdf	l3-vlan-trust	l3-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.



General

Session ID	24660
Action	allow
Application	web-browsing
Rule	allow-apps
Rule UUID	ef0406e3-626e-4219-8856-719c060c4fcd
Verdict	benign
Device SN	012801064407
IP Protocol	tcp

Source

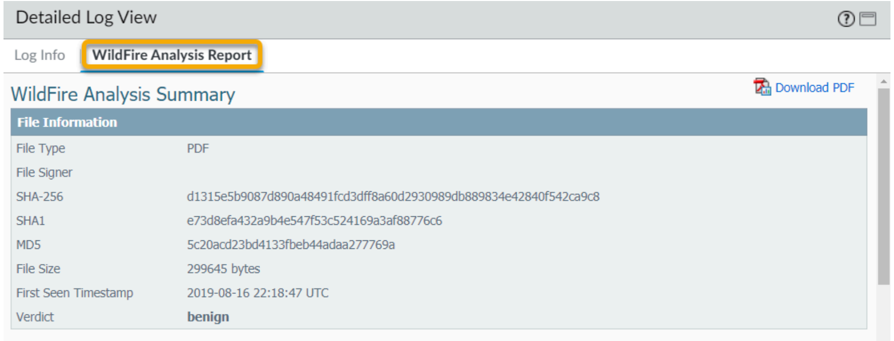
Source User	
Source	192.168.2.11
Source DAG	
Port	58846
Zone	l3-vlan-trust
Interface	vlan.1

Destination

Destination User	
Destination	10.101.6.66
Destination DAG	
Port	4502
Zone	l3-untrust
Interface	ethernet1/1

Details

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.



File Information	
File Type	PDF
File Signer	
SHA-256	d1315e5b9087d890a48491fcd3dff8a60d2930989db889834e42840f542ca9c8
SHA1	e73d8efa432a9b4e547f53c524169a3af88776c6
MD5	5c20acd23bd4133fbeb44adaa277769a
File Size	299645 bytes
First Seen Timestamp	2019-08-16 22:18:47 UTC
Verdict	**benign**

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

Cloud Management

*If you're using Panorama to manage Prisma Access,, you can follow the process below to access content in Prisma Access or toggle over to the **PAN-OS** tab and follow the guidance there.*

STEP 1 | Use the credentials associated with your Palo Alto Networks support account and log in to the Strata Cloud Manager application on the hub.

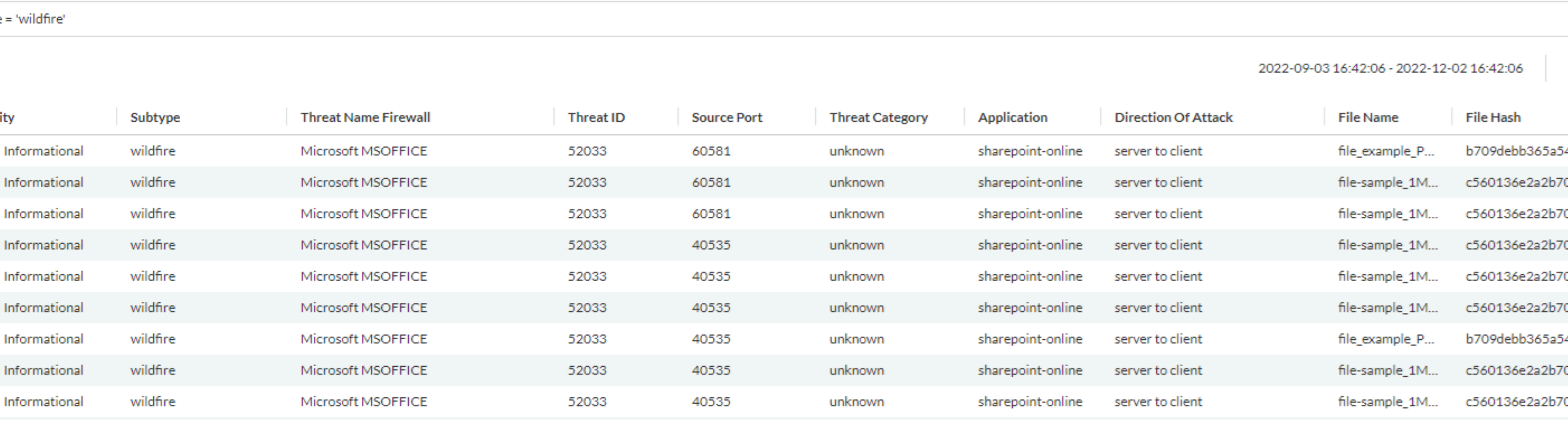
For more information on using Activity, refer to the Log Viewer.

STEP 2 | Filter threat logs to display your WildFire sample submissions in Prisma Access.

1. Select **Incidents and Alerts** > **Log Viewer**.
2. Change the log type to be searched to **Threat**.
3. Create a search filter using the WildFire subtype used to indicate a WildFire sample submission using the query builder. For example, you can use `sub_type.value = 'wildfire'` to view your WildFire logs. Adjust the search criteria as necessary for

your search, including additional query parameters (such as the severity level and action) along with a date range.

To view the WildFire analysis report, you must log in to the WildFire portal and use the hash value or file name to retrieve the report file. For more information, refer to View Reports on the WildFire Portal.

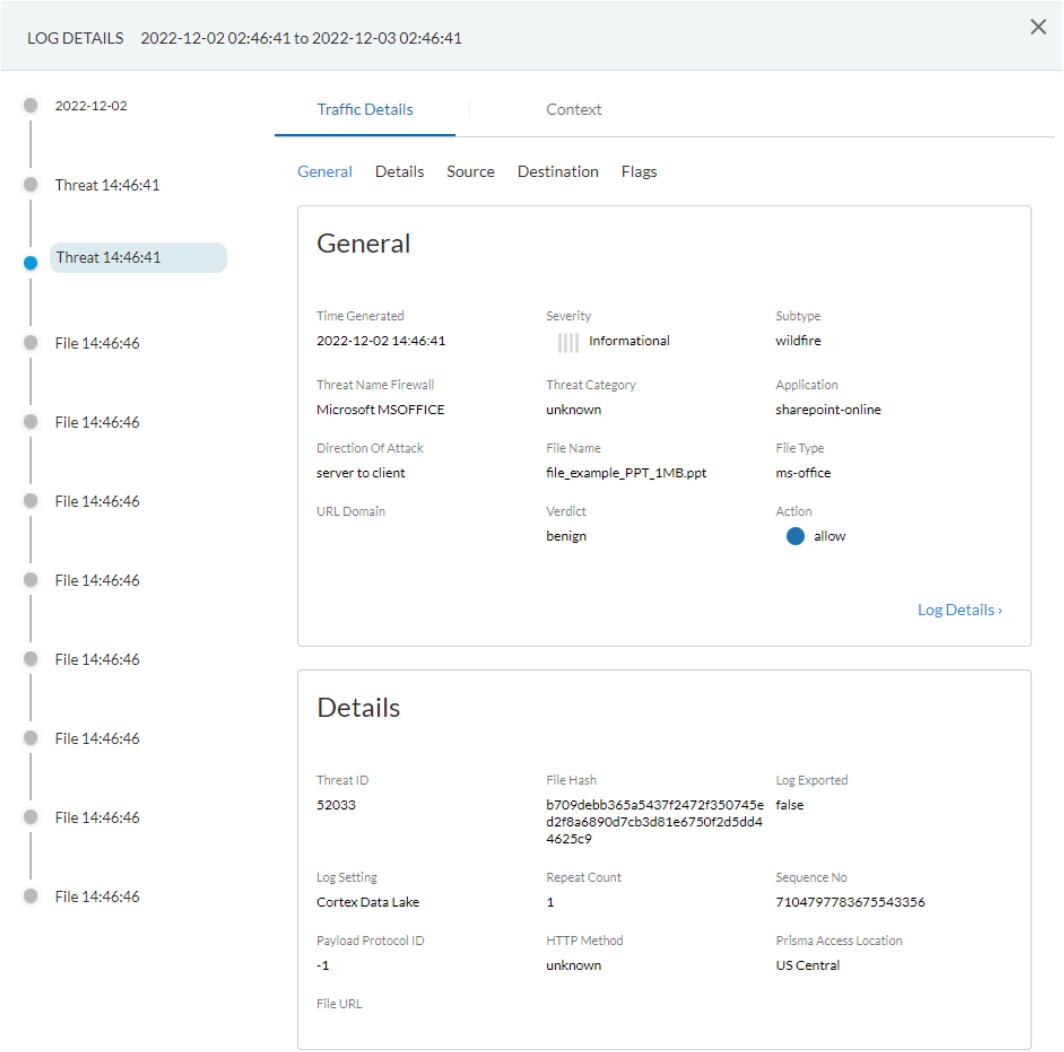


e = 'wildfire'

2022-09-03 16:42:06 - 2022-12-02 16:42:06

ity	Subtype	Threat Name Firewall	Threat ID	Source Port	Threat Category	Application	Direction Of Attack	File Name	File Hash
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70

4. Run the query after you have finished assembling your filter.
5. Select a log entry from the results to view the log details.
6. The threat log **Subtype** is displayed in the **General** pane along with other information about the sample. Other relevant details about the threat are displayed in their corresponding windows.



LOG DETAILS 2022-12-02 02:46:41 to 2022-12-03 02:46:41

General

Time Generated	Severity	Subtype
2022-12-02 14:46:41	Informational	wildfire
Threat Name Firewall	Threat Category	Application
Microsoft MSOFFICE	unknown	sharepoint-online
Direction Of Attack	File Name	File Type
server to client	file_example_PPT_1MB.ppt	ms-office
URL Domain	Verdict	Action
	benign	● allow

Details

Threat ID	File Hash	Log Exported
52033	b709debb365a5437f2472f350745e d2f8a6890d7cb3d81e6750f2d5dd4 4625c9	false
Log Setting	Repeat Count	Sequence No
Cortex Data Lake	1	7104797783675543356
Payload Protocol ID	HTTP Method	Prisma Access Location
-1	unknown	US Central
File URL		

Use the WildFire Portal to Monitor Malware

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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 portal.
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

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

Where Can I Use This?	What Do I Need?
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	

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

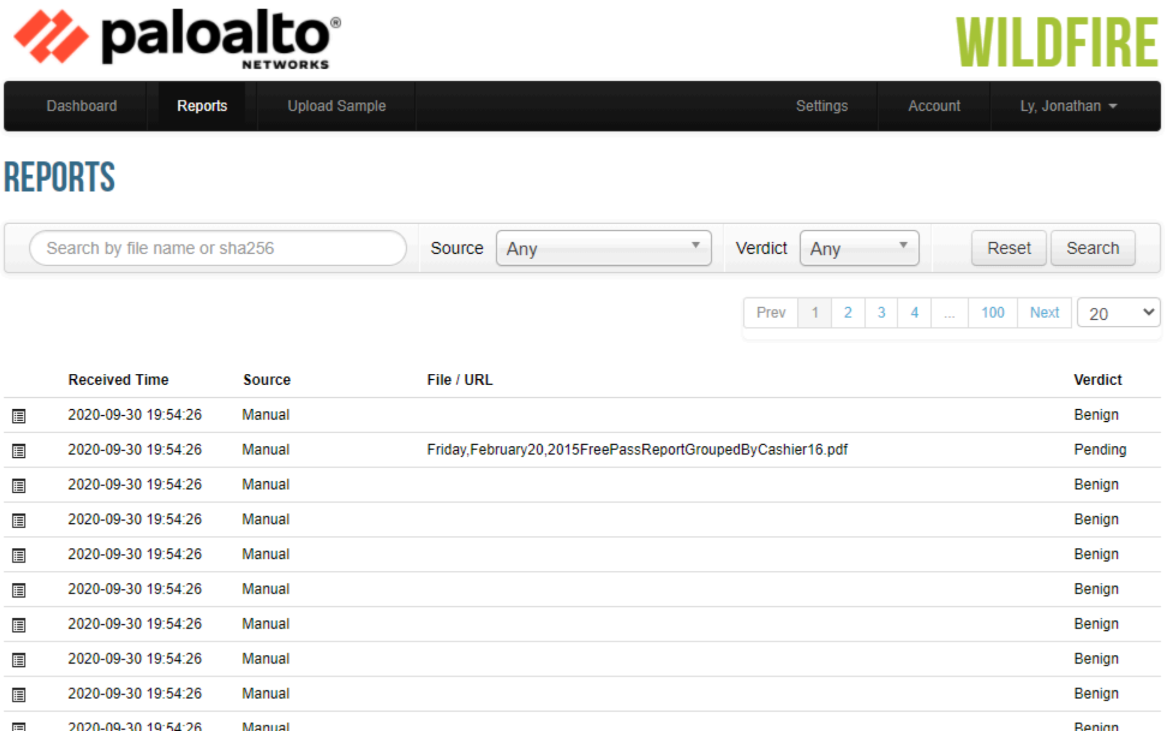
Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	□ Advanced WildFire License *For Prisma Access, this is usually included with your Prisma Access license.*

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:



	Received Time	Source	File / URL	Verdict
▤	2020-09-30 19:54:26	Manual		Benign
▤	2020-09-30 19:54:26	Manual	Friday,February20,2015FreePassReportGroupedByCashier16.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