Best Practices

FortiPAM 1.9.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 4, 2026
FortiPAM 1.9.0 Best Practices
74-180-1245223-20260504

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-05-04	Initial release.

Getting started

FortiPAM is a privileged access management solution.

FortiPAM provides privileged access management, control, and monitoring of elevated and privileged accounts, processes, and critical systems across the entire IT environment.

For more information on FortiPAM and its features, see the latest *FortiPAM Administration Guide*.

The following are the first steps to take when preparing a new FortiPAM device for deployment:

Registration

The FortiPAM, and then its service contract, must be registered to have full access to FortiCare portal, and FortiGuard services.

The FortiPAM can be registered in either the FortiPAM GUI or the FortiCare portal. The service contract can be registered from the FortiCare portal.

To verify the license status on the FortiPAM, go to *System > FortiGuard License* and check the *License Information* table.

> There can be a delay of a few hours between when you register your device and when the license information on the FortiPAM is updated.

The *License Information* table can be used to confirm that the FortiPAM is receiving the latest updates.

Expand a service in the table and hover over a version to see the day it was last updated. Some services have daily updates, but others will remain unchanged for a longer period of time. For example, the AV engine can stay unchanged for months, while the AV signature database can receive multiple updates a day.

> If you are not receiving updates, ensure FortiPAM communication with FortiGuard is uninterrupted.
>
> See the latest *FortiPAM Ports Guide*.

For more information on FortiGuard, see *FortiGuard Distribution Network* in the latest *FortiPAM Administration Guide*.

Basic configuration

As the first step of a new deployment, review default settings such as administrator password, certificates for GUI, and open administrative ports on interfaces.

As soon as FortiPAM is connected to the Internet, it is exposed to external risks, such as unauthorized access, man-in-the-middle attacks, spoofing, DoS attacks, and other malicious activities from malicious actors. Manually reconfigure the default settings to tighten the security from the beginning.

- **Firmware**
  If the shipped firmware is not the firmware that you will be running, load the required firmware before doing any configuration.

  > Always ensure that the FortiPAM firmware is regularly updated to receive the latest features, bug fixes, and security updates.

- **Hostname**
  Use a meaningful hostname. It is used in the CLI prompt, as the SNMP system name, as the FortiPAM Cloud device name, and as the device name in an HA configuration.
- **System time**
  Several FortiPAM features rely on an accurate system time, such as logging and certificate related functions. It is recommended that you use a Network Time Protocol (NTP) server to set the system time. If necessary, the system time can be set manually.
- **Administrator password**
  The administrator password must be set when you first log in to the FortiPAM. Ensure that the password is unique and has adequate complexity.
- **Management interface**
  Configure only the required administrative access services (SSH, SNMP) on the interface.

Resources

Fortinet provides many resources to help you configure FortiPAM.

FortiPAM product documentation https://docs.fortinet.com/product/fortipam/	Access FortiPAM documentation, including administration guides, reference manuals, release notes, and QuickStart guides.
FortiPAM Community page https://community.fortinet.com/t5/FortiPAM/tkb-p/TKB52	A central repository of technical notes, tips, troubleshooting and debugging, and instructions primarily provided by the technical support team.

FortiGuard Labs https://www.fortiguard.com	Information on the latest internet threats, security advisories, hot bulletins, and malware through the threat encyclopedia. This database has more than four million records and provides access to the signature database. The FortiGuard network resources helps you keep up to date with the security landscape through Advisories & Reports, FortiGuard services, and a Resource library.
FortiCare portal https://support.fortinet.com/	Start a chat, open a ticket, or call in for immediate service. Be aware of your support SLA with regards to receiving assistance based on the issue severity and Return Merchandise Authorization (RMA) replacement times.
Professional Services https://www.fortinet.com/support/support-services/professional-services	Assistance with configuring your FortiPAM, and other Fortinet products.
Fortinet Training Institute https://training.fortinet.com	Sign up for computer based or instructor led training and hands on labs.

Administrator access

On FortiPAM, the GUI portal is opened to all users. Different user roles control what a user can do when logged into FortiPAM.

See *Role* in the latest *FortiPAM Administration Guide*.

When access to the FortiPAM is insecure, so is the traffic that it passes.

The following information can help you prevent unwanted access to your FortiPAM:

User authentication

Who can access FortiPAM

Users can log in to the FortiPAM by authenticating locally with the FortiPAM, or with a remote access server that is integrated with the FortiPAM, such as LDAP or RADIUS servers.

For improved security, disable the known administrator account.

Assign the *Super Administrator* access profile to a user to manage and monitor the FortiPAM device.

Set security policies, e.g., a login schedule, trusted hosts, automatic password changing, ZTNA protection, to protect the super admin user.

To avoid potential lockouts, do not configure any MFA for the default *Super Administrator*.

Instead, configure restricted/trusted hosts to secure the default *Super Administrator*.

For local accounts on the FortiPAM, define a password policy to ensure a minimum complexity level.

Remote authentication servers enforce their own password policies. They also provide more configuration options. For example, you can use pre-defined security groups to enable access to a group of users. If an administrator's access needs to be removed, when their account is disabled in the remote access server, they are no longer able to log in to the FortiPAM.

Do not use shared accounts to access the FortiPAM. Shared accounts are more likely to be compromised, are more difficult to maintain as password updates must be disseminated to all users, and make it impossible to audit access to the FortiPAM.

In addition to accounts for GUI and CLI administration, the FortiPAM can be managed with API calls by API users who are required to generate authorization tokens for REST API messages.

You can enable ZTNA control on FortiPAM so that users can only connect to FortiPAM and launch secrets from the endpoint PC with allowed ZTNA tags.

See *ZTNA user control* in the latest *FortiPAM Administration Guide*.

What can administrators access

The features that an administrator can access should be limited to the scope of that administrator's work to reduce possible attack vectors. The access profile tied to the user account defines the areas on the FortiPAM that the administrator can access, and what they can do in those areas. The list of users with access should be audited regularly to ensure that it is current.

How can users access FortiPAM

Trusted hosts can be used to specify the IP addresses or subnets that can log in to the FortiPAM.

When authenticating to the FortiPAM, implement multi-factor authentication (MFA). This makes it significantly more difficult for an attacker to gain access to the FortiPAM.

Administrative settings

The following general administrative settings are recommended:

- Set the idle timeout time for administrators to a low value, preferably less that ten minutes.

  The idle timeout can be set using the *GUI Session Timeout* option in the *Other General Settings* pane in *System > Settings*.

  See the latest *FortiPAM Administration Guide*.
- Use non-standard HTTPS and SSH ports for administrative access.
- Disable weak encryption protocols.
- Replace the certificate that is offered for HTTPS access with a trusted certificate that has the FQDN or IP address of the FortiPAM.

Day to day operations

Using secrets

When setting up secrets, you should:

- Enable *AntiVirus Scan* and apply an antivirus profile.
- Enable *DLP Status* and apply a DLP profile.
- Enable *SSH Filter* and apply an SSH filter profile.
- Enable *Requires Checkout* to get exclusive access to a secret for a limited time.
- Enable *Requires Approval to Launch Secret* and apply an approval profile.
  This ensures that the user sends out a request to approvers to get access to the secret.
- In the *Permission* tab, ensure that the permissions are set to the minimum before sharing the secret, e.g., set the permission to *View* before you share the secret.

Kerberos authentication for RDP sessions

- Create a secret using the *Target Only* secret template with target computer FQDN as the host information.
  Associate the secret with the corresponding *Windows Domain Account* secret, and launch the RDP session using the associated secret credentials.
- Create a secret using *Windows Domain Account* secret template.
  When launching an RDP session, enter the target FQDN in the *Enter Target* field.

See *Creating a secret* in the latest *FortiPAM Administration Guide*.

Logging and reporting

Logging generates system event, traffic, user login, and many other types of records that can be used for alerts, analysis, and troubleshooting. The records can be stored locally (data at rest) or remotely (data in motion). Due to the sensitivity of the log data, it is important to encrypt data in motion through the logging transmission channel. Communication with FortiAnalyzer is encrypted by default. When logging to third party devices, make sure that the channel is secure. If it is not secure, it is recommended that you form a VPN to the remote logging device before transmitting logs to it.

Logging options include FortiAnalyzer and a local disk. Logging to FortiAnalyzer stores the logs and provides log analysis. If a security fabric is established, you can create rules to trigger actions based on the logs. For example, sending an email if the FortiPAM configuration is changed, or running a CLI script if a host is compromised. If you are

using a standalone logging server, integrating an analyzer application or server allows you to parse the raw logs into meaningful data.

FortiSIEM (security information and event management) and FortiSOAR (security orchestration, automation, and response) both aggregate security data from various sources into alerts. The FortiSOAR can also automate responses to different alerts.

Identity and access management

Secure authentication is paramount in the implementation of an effective security policy. Many of the most damaging security breaches are due to compromised user accounts. By identifying and authenticating users, a significantly more granular control can be implemented to ensure that the right users are accessing the right network resources.

FortiPAM supports identifying users in many different ways, including but not limited to:

- **Local**: The user name and password are stored on FortiPAM.

  For local users, set up a password policy.

  See *User Password Policy* pane in *System > Settings* in the latest *FortiPAM Administration Guide*.

- **Remote**: The user name and password are stored on a remote server, such as LDAP, SAML, or RADIUS, that the FortiPAM queries.

  For remote users, set up password policy on the remote authentication server.

  For remote LDAP server, ensure that *Server Identity Check* is enabled to verify the server domain/IP address against the server certificate.

  The option is enabled by default.

  See *LDAP servers* in the latest *FortiPAM Administration Guide*.

  For SAML configuration, ensure that the IdP and SP settings are aligned.

  If FQDNs are used, the IdP and SP side must use FQDNs consistently. Similarly, if IP addresses are used, the IdP and SP side must use IP addresses consistently.

Configure trusted IPv4 addresses from which the user can connect to the FortiPAM.

See *Configure Trusted Hosts* in the latest *FortiPAM Administration Guide*.

Configure a schedule when the user can connect to FortiPAM.

See *Configure the schedule for which the user can connect to the FortiPAM* in the latest *FortiPAM Administration Guide*.

The most effective authentication includes more than one of the following:

- Something that the user knows: a username and password
- Something that the user has: a one time password (OTP) in the form of a token or code either sent to the user over email or SMS, or generated by a hardware token or authenticator app.

Single sign-on (SSO) can be used to reduce user fatigue by allowing users to only authenticate one time to gain access to all permitted resources.

FortiClient provides a solution to user and device identification, and can function as an SSO agent. It is also part of the Zero Trust Network Access (ZTNA) solution, allowing security posture checks along with authentication.

Note that, when implementing MFA on the FortiPAM, a FortiToken can only be registered to one FortiPAM at a time. If you use a remote authentication server for MFA, then each FortiPAM points to the server. FortiAuthenticator and FortiToken Cloud are remote authentication servers that can manage the FortiTokens for multiple FortiPAM devices at the same time. This allows you to use one token per user across multiple FortiPAM devices.

See the following in the latest *FortiPAM Administration Guide*:

- *2FA with FortiToken*
- *2FA with FortiToken Cloud*

See the following in the latest *FortiPAM Examples*:

- *2FA on FortiPAM for RADIUS users using FortiAuthenticator*
- *2FA on FortiPAM for SAML users using FortiAuthenticator*

Certificates

Certificates serve three primary purposes:

1. **Authentication**
   The Common Name (CN) and/or Subject Alternative Name (SAN) fields are used to identify the device that the certificate is representing.
2. **Encryption and decryption**
   Private and public key pairs are used to encrypt and decrypt traffic.
3. **Integrity**
   Messages are hashed using a secret key known to both the sender and the receiver. The receiver uses the key to check the hash value and confirm the message's data integrity and authenticity.

Certificate based authentication has several advantages over password based authentication. While password based authentication relies on secrets that are defined and managed by a user, certificate based authentication uses secrets that are issued and managed by the certificate authority. Certificates are more secure than passwords, because the private key in the certificate has high cryptographic strength, which a user defined password does not usually have.

The CA vouches for the certificates that it signs. If the endpoint has the CA root certificate installed, then it trusts the CA and anything that the CA signs. There are three types of CAs:

Replace the certificate for HTTPS access.

- **Public CA**
  Public, or well-known, CAs charge a fee to sign your certificate. Many systems come with these CA root certificates pre-installed.
- **Let's Encrypt**
  Let's Encrypt is a free, automated, and open CA. FortiPAM includes an Automated Certificate Management Environment (ACME) to directly interact with Let's Encrypt. Some legacy systems might not have the Let's Encrypt CA root certificate installed.
- **Private CA**
  Private CAs are created by an organization that creates its own local CA instead of using an external CA. It functions the same as a public CA, but the root certificate is not pre-installed on anything. FortiAuthenticator, Microsoft Server, OpenSSL, and XCA can all function as CAs.

Regardless of what kind of CA is used, involved devices must have the CA root certificate installed in order to trust the certificate that it signs.

Certificate usage

FortiPAM leverages certificates in multiple areas, such as administrative access, ZTNA, SAML authentication, and LDAPs.

The default Fortinet factory self-signed certificates are provided to simplify initial installation and testing. Replace any used certificates with certificates that are signed by a trusted CA and specific to that FortiPAM.

Certificates can be uploaded to the FortiPAM in multiple ways:

- Automated Certificate Management Environment (ACME),
- Uploading a certificate in the GUI or CLI,
- Creating a Certificate Signing Request (CSR), having it signed by a CA, then uploading the certificate.

Security profiles

Security profiles define what to inspect in the traffic that the FortiPAM is passing. When traffic matches the profile, it is either allowed, blocked, or monitored (allowed and logged).

The protection that a profile provides, and the information that it monitors, can be configured to your requirements, but increased inspection uses more of the FortiPAM resources. Assess your policies' traffic matching, and then apply the necessary level of protection.

Security profiles can use flow or proxy mode inspection. Apply flow mode inspection to policies that prioritize traffic throughput, and proxy mode when thoroughness is more important than performance. Under normal traffic conditions, the throughput difference between the two modes is insignificant. For resource optimization, using one mode uniformly across all of the policies is recommended.

Each security profile generates its own log type that contains some log fields that are not present in other logs. This can be important when reviewing or analyzing the logs to assess or troubleshoot user traffic. For example, if no web filtering is applied, then you will not have insight or control of users' browsing information.

The following table lists some basic examples of how a security profile could be used on an edge FortiPAM, where inbound traffic goes from the internet to an internal resource using a VIP, and outbound traffic goes from your network to an internet resource:

Security profile	Inbound traffic	Outbound traffic
AntiVirus	Protect external resources from malware, such as HTTP PUT requests or FTP uploads.	Scan requested user traffic for malware.
Web filter	Not usually applied to inbound traffic.	Monitor and block user web traffic based on categories and domains.
Video filter	Not usually applied to inbound traffic.	Monitor and restrict YouTube videos based on categories or channels.
DNS filter	Not usually applied to inbound traffic.	Monitor and filter DNS lookups based on domain ratings. Block requests for known compromised domains.
Application control	Make sure that specific protocols are used to access specific ports. For example, only allow SSH traffic to be sent and received over port 22.	Monitor and filter applications on any port.
Intrusion prevention	Protect external services from known exploits and protocol anomalies.	Block connections to botnet sites.
File filter	Prevent uploading files based on the file type and the protocol that is used.	Prevent downloading files based on the file type and the protocol that is used.

Security profile	Inbound traffic	Outbound traffic
Data leak prevention	Prevent sensitive data from entering your network.	Prevent sensitive data, such as credit card numbers or SSNs, from leaving your network.
ICAP	Offload tasks to separate, specialized servers.	Offload tasks to separate, specialized servers.

SSL/TLS deep inspection

TLS encryption is used to secure traffic, but the encrypted traffic can be used to get around your network's normal defenses. SSL/TLS deep inspection allows the FortiPAM to inspect traffic even when they are encrypted. When you use deep inspection, the FortiPAM serves as the intermediary to connect to the SSL server, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content with a certificate that is signed by the FortiPAM, and sends it to the real recipient.

The FortiPAM acts as a subordinate CA to sign the certificate on the fly, as it re-encrypts traffic. The FortiPAM usually uses a subordinate CA certificate that is signed by the company's private CA, such as a FortiAuthenticator or a Windows server with certificate services.

For information about uploading a CA certificate and private key for deep inspection, see *Certificates* in the latest *FortiPAM Administration Guide*.

To implement seamless deep inspection, users must trust the certificate that is signed by the FortiPAM, and there must be certificate chain back to the trusted root CA that is installed on the user's endpoint. If the root certificate is not installed, the user receives a certificate warning every time they access a website that is scanned by the FortiPAM using deep inspection. Administrators should provide the CA certificate to the end users if deep inspection will be used.

Users should be made aware that their communication is subject to these security measures, and that their privacy while protected by a FortiPAM that is performing deep inspection cannot be guaranteed. Performing deep inspection might be undesirable when users are accessing certain web categories, such banking or personal health related sites. When creating SSL/SSH inspection profiles that use full SSL inspection, the Finance and Banking, Health and Wellness, and Personal Privacy categories are exempt from inspection by default. Administrators can customize these categories, enable Reputable websites, and add individual addresses to the SSL exemptions as required.

High availability and redundancy

Downtime due to an unexpected network failure negatively impacts business operations. For some companies, some downtime is acceptable; for others, any downtime is unacceptable. Determine your uptime requirements, and ensure that your network has the resilience to meet those requirements.

Building a resilient network costs more initially, as it can include HA, cold standby spares, multiple internet circuits, premium supports contracts, and more.

High availability

HA provides resilience not only in the event of a cluster member failing, but also allows for firmware updates without any downtime.

FortiPAM can operate in Active-Passive HA mode.

See *High availability* in the latest *FortiPAM Administration Guide*.

Disaster recovery

It is important to plan what to do in the event that a disaster occurs. Disaster recovery starts with a business continuity plan. This plan should be all-encompassing, and include your FortiPAM.

FortiPAM disaster recovery should include:

- A tested plan:
  - Without testing the plan, you cannot be sure that it will work.
  - Testing helps to uncover oversights and refine the process.
- Configuration backups:
  - Backups should be made on a schedule, and after any changes have been made to the configuration.
  - It is good practice to evaluate if any unexpected changes occur between backups.
- Remote site assistance:
  - Who will load the configuration backup to the FortiPAM?
  - In the event of an RMA, who will install the replacement FortiPAM?
  - Do all of the people who will require it have access to the FortiPAM?
- Replacement hardware:
  - If the device is covered under warranty, what level of support has been purchased?
  - What is the agreed expectation for a replacement?
  - How will the backup configuration be loaded onto the new device?

After a disaster, review the recovery to asses what worked, what did not work, and what can be improved. Unfortunately, sometimes a disaster helps get approval for a more robust solution, such as HA or a premium support contract with better SLAs.

To set up disaster recovery on FortiPAM, see *Disaster recovery* in the latest *FortiPAM Administration Guide*.

Network security

Many factors affect how you design your network, the topology that you use, and the placement of your FortiPAM in the network, such as:

- The size of your business and the number of users that you are protecting.
- Your business type and industry - service provider, education, healthcare, retail, hospitality, operational technologies, and so on.
- Who is being protected - employees, customers, students, remote workers, healthcare workers, and so on.
- What is being protected - web servers, office computers, cloud devices, industrial devices, POS terminals, and so on.

For example, a mid-sized retail company might have a corporate headquarters, multiple branches, and physical and cloud-based datacenters, with one or more FortiPAM devices and other Fortinet products deployed at each location.

When designing the network, consider the functionality that you are providing at each location, what you are protecting, and who is allowed access to protected resources. The branches likely have similar or identical setups, and headquarters and the datacenters have setups specific to those locations' requirements. Considering the network design factors helps you define the FortiPAM's role, where it is placed in the network, and how to incorporated it and other network solutions into your environment.

The Fortinet solutions page, https://www.fortinet.com/solutions, provides information about products and solutions for different business sizes and industries.

Hardening

System hardening reduces security risk by eliminating potential attack vectors and shrinking the system's attack surface.

Some of the best practices described previously in this document contribute to the hardening of the FortiPAM with additional hardening steps listed here.

RAID on host

Configure RAID on the VM host to protect the system data in case of a drive failure.

Physical security

Install FortiPAM in a physically secure location. Physical access to the FortiPAM can allow it to be bypassed, or other firmware could be loaded after a manual reboot.

Vulnerability - monitoring PSIRT

Product Security Incident Response Team (PSIRT) continually tests and gathers information about Fortinet hardware and software products, looking for vulnerabilities and weaknesses. The findings are sent to the Fortinet development

teams, and serious issues are described, along with protective solutions, in advisories listed at https://www.fortiguard.com/psirt.

Firmware

Keep the FortiPAM firmware up to date. The latest patch release has the most fixed bugs and vulnerabilities, and should be the most stable. Firmware is periodically updated to add new features and resolve important issues.

- Read the release notes. The known issues may include issues that affect your business.
  The *Release Notes* are available on the *FortiPAM Docs* page.
- Do not use out of support firmware. Review the product lifecycle and plan to upgrade before the firmware expires.

Encrypted protocols

Use encrypted protocols, wherever possible, for example:

- LDAPS instead of LDAP
- SNMPv3 instead of SNMPn
- SCP instead of FTP or TFTP
- NTP authentication
- Encrypted logging instead of TCP

FortiGuard databases

Ensure that FortiGuard databases, such as AS, IPS, and AV, are updated punctually. Optionally, send an alert if they are out of date.

Penetration testing

Test your FortiPAM to try to gain unauthorized access, or hire a penetration testing company to verify your work.

Secure password storage

The passwords, and private keys used in certificates, that are stored on the FortiPAM are encrypted using a predefined private key, and encoded when displayed in the CLI and configuration file.

Passwords cannot be decrypted without the private key and are not shown anywhere in clear text. The private key is required on other FortiPAM to restore the system from a configuration file. In an HA cluster, the same key should be used on all of the units.

To enhance password security, specify a custom private key for the encryption process. This ensures that the key is only known by you.

FortiPAM models with a Trusted Platform Module (TPM) can store the primary encryption password, which is used to generate the primary encryption key, on the TPM. For more information, see FortiPAM with TPM .

To configure the private encryption key:

1. In the CLI console, enter the following commands:

```
config system global
  set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

See *Verify the private-data-encryption feature* in the latest *FortiPAM Administration Guide*.

Configuration backup

The FortiPAM configuration file has important information that should always be kept secured, including details about your network, users, credentials, passwords, and keys. There are many reasons to back up your configuration, such as disaster recovery, preparing for migrating to another device, and troubleshooting. Evaluate the risk involved if your configurations were exposed, and manage your risk accordingly.

When backing up your configuration, consider the following steps to safeguard the file:

- Enable *Encryption* when backing up the configuration.
- Store the configuration file in a secure location.
- Delete old configuration files that are no longer needed.

If a configuration file must be shared with a third party for auditing, troubleshooting, or any other reasons, consider only providing a section of the file and not the entire file. Otherwise, consider the following steps:

- Enable *Encryption* when backing up the configuration and only share the password with the intended party.
- Manually replace the passwords in the backed up configuration file.
- Request that the configuration file be deleted after the intended purpose has been satisfied.

Email notifications

Setting up email notifications helps notify administrators about FortiPAM device events, e.g., glass breaking or license expiry, allowing quick response to issues.

See *Email alert settings* in the latest *FortiPAM Administration Guide*.

vTPM

For improved secret credentials protection, enable vTPM on FortiPAM.

See *FortiPAM with TPM* in the latest *FortiPAM Administration Guide*.

Log and video disk encryption

Turning on disk encryption on log and video disks is akin to putting a solid lock on a chest of sensitive information. This keeps all the data safe by making it unreadable to anyone without a unique key or password. If someone tries to steal or get into the storage devices without permission, they cannot open and access the disk content. This is a crucial defence against any potential leaks or breaches.

See *Configuring log and video disk encryption* in the latest *FortiPAM Administration Guide*.

Login disclaimer

By setting up login disclaimer in FortiPAM, not only can you warn users about unauthorized use, you can also see the last successful/failed login time.

See *Login Disclaimer* in the *Other General Settings* pane in *System > Settings* in the latest *FortiPAM Administration Guide*.

Firmware change management

Consider the following points when performing firmware upgrades, not only in FortiPAM but as general rules for any change you have to make in a production environment.

Understanding the new version

Before attempting any changes in production, first make sure you set up a laboratory where you can freely play with the new features and understand them without pressure and time constraints. Read the release notes, manuals, and other documentation, such as presentations, videos, or podcasts about the new version.

You are ready to explain the need for an upgrade once you understand:

- The differences and enhancements between the new version and the previous versions.
- The impact of the upgrade on customers and the users of the operating platform.
- The known limitations that might affect your environment.
- The potential risks when performing the upgrade.
- The licensing changes that may apply.

> ⚠ Never attempt to upgrade to a version that you do not fully understand, in terms of both features and known limitations, and on which you have no operational experience.

Reasons to upgrade

You should have a valid reason for upgrading the firmware. The reason cannot be only because you want the latest version. The reason has to be explained in terms of business, technical, or operational improvement.

Affirmative answers to the following questions are valid reasons to upgrade:

- Does the new version have a feature that helps to ensure compliance?
- Does the new version have an enhancement that allows a 40% decrease on the time it takes to perform a certain operation?
- Does a new feature correct a known defect or bug found on a previous version that affects the company business or operations?
- Will the new version allow your organization to deploy new services that will help to gain new customers or increase loyalty of existing customers?
- Is the vendor cutting support for the version your organization is currently using?

If the best reason to upgrade is because the new features seem to be cool or because you want the latest version, some more understanding and planning may be necessary.

Preparing an upgrade plan

If you choose to upgrade for a valid reason, make sure you create a plan that covers business, technical, and operational aspects of the upgrade.

Business aspects of the upgrade

Proper planning and justification for an upgrade should be proportional to how critical the system is to the business.

- Make sure you can clearly articulate the benefits of the upgrade in business terms, such as time, money, and efficiency.
- Understand the business processes that will be affected by the change.
- Make sure the upgrade maintenance window is not close to a business-critical process, such as quarterly or monthly business closure.
- Obtain executive and operational approval for the maintenance window. The approval must come from the owners of all the system and information affected by the upgrade, not only from those that own the system being upgraded. The approval must be done formally through written statement or e-mail.

Technical and operational aspects of the upgrade

A plan must be created to account for technical and operational inputs.

- Re-read the release notes for the technology that you are upgrading. Supported hardware models, upgrade paths, and known limitations should be clearly understood.
- Make sure your upgrade maintenance window does not overlap with any other maintenance window on your infrastructure.
- If you have any premium support offer, such as TAM Premium Support, do a capacity planning exercise to ensure the new firmware or software version does not take more hardware resources than you currently have.
- Create a backup, whether or not you already have scheduled backups.
- Obtain offline copies of both the currently installed firmware and the new version.
- Create a list of systems with inter-dependencies to the system you are upgrading. For example, if you are upgrading a FortiPAM, understand the impact other devices that you have on your environment.
- Ensure you have a list of adjacent devices to the upgrading platform and have administrative access to them, in case you need to do some troubleshooting.
- Have a step-by-step plan on how to perform and test the upgrade. You want to make sure you think of the worst situation before it happens, and have predefined courses of action, instead of thinking under pressure when something has already gone wrong.
- Define a set of tests (that include critical business applications that should be working) to make sure the upgrade was successful. If any test does not go well, define which ones mandate a rollback and which ones can be tolerated for further troubleshooting. This set of tests should be run before and after the upgrade to compare results. The tests performed before and after the upgrade should be the same.
- Define a clear rollback plan. If something goes wrong with the upgrade or the tests, the rollback plan will help you get your environment back to a known and operational status. The plan must clearly state the conditions under which the rollback will be started.

- Declare configuration freezes shortly before and after the upgrade. This reduces the amount of variables to take into consideration if something goes wrong.
- Perform a quality assurance upgrade. Load a copy of the production configuration on a non-production box and execute the upgrade to see if there are any issues on the process. Adjust your plan according to the results you obtain.
- Have a list of information elements to be gathered if something goes wrong. This ensures that, even if the upgrade fails, you will collect enough information to troubleshoot the issue without needing to repeat the problem. Get help from Fortinet Support if you need to confirm what could be missing from your list.
- Define a test monitoring period after the change was completed. Even if the upgrade went smoothly, something could still go wrong. Make sure that you monitor the upgraded system for at least one business cycle. Business cycles may be a week, month, or quarter depending on your organization's business priorities.

Executing the upgrade plan

Execution of an upgrade is just as key as planning. Once you are performing the upgrade, the pressure will rise and stress might peak. This is why you should stick to the plan you created with a cool head.

Resist the temptation to make decisions while performing the upgrade, as your judgment will be clouded by the stress of the moment, even if a new decision seems to be an obvious improvement in the moment. If your plan says you should rollback, then execute the rollback despite the potential quick fix mentality.

While performing the upgrade, make sure all the involved components are permanently monitored before, during, and after the upgrade, either through monitoring systems, SNMP alerts, or with a ping. Critical resources like CPU, memory, network, and disk utilization must also be constantly monitored.

To avoid misunderstandings, when performing the tests for each critical application defined in the planning, make sure there are formal notifications on the results for each user area, service, system, and application tested.

Regardless if you have to rollback or not, if a problem occurs, make sure you gather as much information about the problem as possible, so you can later place a support ticket to find a solution.

Finally, document the upgrade:

- Enable your terminal emulation program to leave trace of all the commands executed and all the output generated. If you are performing steps through the GUI, consider using a video capture tool to document it.
- Document any command or change performed over the adjacent and interdependent systems. Make sure they are acknowledged by the relevant administrators.
- Document any deviations performed over the upgrade plan. This is the planned-versus-actual.

Learning more about change management

Change management and change control are huge knowledge areas in the fields of Information Systems, and Computer and Network Security.

This document is by no means a comprehensive list on what you should do when performing an upgrade, with either Fortinet or any other technology. It is merely a list of important things you should take into consideration when performing upgrades. It is the result of years of experience dealing with changes on critical environments, as it is common that security devices are protecting critical applications and processes.

There are vast resources on the topic of change management and change control, including books, public whitepapers, blog entries, and so on. If you search the internet for the "Change Control Best Practices" or "Change Management Best Practices," you will find many helpful results.

Changes on production IT infrastructure are critical to the business. Make sure they play in your favor and not against you.

For details on upgrading FortiPAM firmware, see *Firmware* in the latest *FortiPAM Administration Guide*.

www.fortinet.com