Legal Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/. 
1 Securing Privileged Account Manager at the Operating System 5
  1.1 Enabling FIPS ................................................................. 5
    1.1.1 Settings to Enable and Disable TLS Algorithms ................. 6

2 Securing Privileged Account Manager 7
  2.1 Securing Access to the Framework Manager Console .................. 7
    2.1.1 Requesting a Certificate for the Framework Manager Console .... 7
  2.2 Deployment Considerations ............................................... 8
  2.3 Configuring Privileged Account Manager Against Attacks ............. 10
    2.3.1 SSL Renegotiation DOS Attack Protection ......................... 10
    2.3.2 Enabling FIPS Mode .................................................. 11

3 Securing Privileged Account Manager at Application Level 13
  3.1 Using Audit Settings ...................................................... 14
  3.2 Using the Encryption Settings .......................................... 14
  3.3 Enabling the FIPS Mode .................................................. 15
  3.4 Disabling the CBC Mode .................................................. 15

4 Securing Network Settings and Strengthening Deployment Settings 17
  4.1 Opening Firewall Ports .................................................. 17
  4.2 Protecting Privileged Account Manager through Firewall ............. 17

5 Securing Access to the Privileged Account Manager Console 21
  5.1 Requesting a Certificate for the Framework Manager Console ....... 22
    5.1.1 Installing a Certificate .............................................. 22
  5.2 Securing the PAM Manager ............................................... 23
  5.3 Privileged Account Manager and Agent Communication ................. 23
  5.4 Privileged Account Manager Communication with External Services .... 23
  5.5 Credential Vault ......................................................... 23

6 Getting the Latest Security Patches 25
Privileged Account Manager offers enhanced protection against security threats and compliance with the United States federal government standards by supporting Federal Information Processing Standards (FIPS). Privileged Account Manager leverages the FIPS 140-2 compliant features to meet the security requirements of the United States federal agencies and customers with highly secure environments. Enabling FIPS mode in Privileged Account Manager allows the product components such as PAM Manager, Privileged Account Manager Agent, Privileged Account Manager Administration Console, Privileged Account Manager User Console, and target applications to communicate using FIPS 140-2 certified encryption algorithms.

This table lists all the required steps to secure Privileged Account Manager at the Operating System level:

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable FIPS at Operating System Level.</td>
<td>See, Enabling FIPS Mode.</td>
</tr>
<tr>
<td>Ensure that you update the security patches and service packs.</td>
<td>See, Privileged Account Manager 4.2 Release Notes.</td>
</tr>
<tr>
<td>Ensure that the time is in sync.</td>
<td>Privileged Account Manager agent and manager communication, data synchronization, and certificate renewal require that the systems are time synchronized. Ensure that time is synchronized using standard means such as, Network Time Protocol.</td>
</tr>
</tbody>
</table>

### 1.1 Enabling FIPS

**IMPORTANT:**

- You cannot disable FIPS after you have enabled it.
  - The FIPS mode is enabled immediately on all the managers that have the registry module.
  - The primary registry manager is enabled first, followed by the other registry managers, and then the associated agents. Automatic re-registration of agents happens once in two days. Therefore, it might take up to two days for FIPS to be enabled automatically on all the agents because FIPS is enabled when agents re-register with a manager.
  - For agents in Offline state, FIPS is enabled only after the status changes to Online and the agents are re-registered with the manager.

**Prerequisites:**

- Ensure that all the packages are upgraded to the latest version on all Privileged Account Manager agents and managers.
• Enable FIPS on the operating systems hosting the managers and the agents.

You can enable the FIPS mode in Privileged Account Manager for both managers and agents only on Windows and Linux. This mode is not supported on Unix. For a complete list of the supported Windows and Linux operating systems, see Privileged Account Manager 4.4 System Requirements and Sizing Guidelines.

To enable FIPS on Privileged Account Manager:

1. Log in to the Privileged Account Manager Administration Console.
2. Click Hosts > Host Status > Enable.
3. (Conditional) To enable FIPS immediately on agents, re-register agents manually. For more information about re-registering agents manually, see the Privileged Account Manager Administration Guide.
4. You must also enable FIPS on the target machines for the following components:
   • (Conditional) RDP relay
   • (Conditional) Credential checkout of applications and databases: Enable FIPS mode on Java that is installed on the system hosting the application.

1.1.1 Settings to Enable and Disable TLS Algorithms

Privileged Account Manager communicates only on TLS 1.2 and the vulnerable encryption methods are disabled to ensure the following:

• Prevent the SWEET32 Attack
• Handle enabling Perfect Forward Secrecy
• Disable SSL renegotiation

NOTE: Due to Cipher Block Chaining (CBC), using TLSv1.0 or earlier makes the environment vulnerable to the BEAST attack. For more information, see Managing and Monitoring Hosts and SSL Renegotiation DOS Attack Protection.
Securing Privileged Account Manager

Administration Console contains configuration information for Privileged Account Manager. If you federate your users with other servers, it stores configuration information about these users. You must protect Administration Console so that unauthorized users cannot change configuration settings or gain access to the information in the configuration store.

When using Privileged Account Manager on cloud, you must consider the following security recommendations:

- The operating system packages must be updated. If you are using SUSE or Red Hat, ensure that the operating system is updated with the latest patch update.
- It is recommended to not use keys of sizes less than 1024 bits on port 22.
- It is recommended to install Privileged Account Manager on a private subnet to restrict the access to configuration data store.

When you develop a security plan for Privileged Account Manager, consider the following considerations:

- Section 2.1, “Securing Access to the Framework Manager Console,” on page 7
- Section 2.2, “Deployment Considerations,” on page 8
- Section 2.3, “Configuring Privileged Account Manager Against Attacks,” on page 10

2.1 Securing Access to the Framework Manager Console

The following options enhance the security of the communication between the browsers and the Framework Manager console. These configuration options do not affect the communications between the Framework managers and the Framework agents.

2.1.1 Requesting a Certificate for the Framework Manager Console

For added security, you can install a certificate to use when accessing the Framework Manager console. To access this option, you need to select the Administration Manager (admin) package on the host that you want to protect. You must then complete a certificate request form, send it to your chosen certification authority, and then install the certificate that you receive.

NOTE: By default, OpenSSL accepts DNS, email, URI, RID, IP, dirName as a Subject Alternative Name (SAN). Privileged Account Manager uses OpenSSL to generate a Certificate Signing Request (CSR). When requesting a certificate in Privileged Account Manager, use the Alternative Names in the console as the “DNS” attribute.
Syntax for Alternative Names is:

- DNS:example.com, DNS:www.example.com
- DNS:example.com, DNS:www.example.com, IP:127.0.0.1

1. On the home page of the console, click Hosts.
2. In the navigation pane, select the host that you want to protect with a certificate.
3. In the details pane, click Packages and select the Administration Manager (admin) for the Framework Manager console.
4. Click Request Certificate in the task pane.
5. Specify the necessary details as described in your chosen certification authority documentation.
6. Click Finish.
   The text for your certificate request is displayed in the text area.
7. Copy the certificate request into an e-mail and send it to your chosen certification authority.
8. When you receive the certificate from your certification authority, install it as described in “Installing a Certificate” on page 8.

### 2.1.1 Installing a Certificate

When you have received the requested certificate from your certification authority:

1. Copy the certificate to the machine you use to access the Framework Manager console.
2. On the home page of the console, click Hosts.
3. In the navigation pane, select the host where you want to install the certificate.
4. In the details pane, click Packages and select the Administration Manager (admin) package for which you have requested the certificate.
5. Click Install Certificate in the task pane.
6. Paste the certificate into the text area.
7. Click Finish.

### 2.2 Deployment Considerations

**Protecting Privileged Account Manager through Firewall**

Use Privileged Account Manager with firewalls. Following figure illustrates a firewall setup for a basic Privileged Account Manager configuration.
Figure 2-1 Privileged Account manager Components between Firewalls
2.3 Configuring Privileged Account Manager Against Attacks

2.3.1 SSL Renegotiation DOS Attack Protection

Clients can attack the SSL server by sending many renegotiation (SSL handshake) requests to it. This can overload the server and it might go down. To prevent such attacks, you can enable DOS attack protection.

To enable SSL renegotiation DOS attack protection:

1. In the `<Installation Path>/config/unifi.xml` file, edit the following line:

   `<SSL reneg_dos_protection="0"/>`

   `reneg_dos_protection`: Set the value to 1 to enable DOS attack protection. The default value is 0.

2. Save the file.
2.3.2 Enabling FIPS Mode

Privileged Account Manager offers enhanced protection against security threats and compliance with United States federal government standards by supporting Federal Information Processing Standards (FIPS). Privileged Account Manager leverages the FIPS 140-2 compliant features to meet the security requirements of United States federal agencies and customers with highly secure environments. Enabling FIPS mode in Privileged Account Manager allows the product components such as PAM Manager, Privileged Account Manager Agent, Privileged Account Manager Administration Console, Privileged Account Manager User Console, and target applications to communicate using FIPS 140-2 certified encryption algorithms.

IMPORTANT: • You cannot disable FIPS after you have enabled it.

• When you enable FIPS:
  • FIPS mode is enabled immediately on all the managers that have the registry module.
  • The primary registry manager is enabled first, followed by the other registry managers, and then the associated agents. Automatic re-registration of agents happens once in two days. Therefore, it may take up to two days for FIPS to be enabled automatically on all the agents because FIPS is enabled when agents re-register with a manager.
  • For agents in Offline state, FIPS will be enabled only after the status changes to Online and the agents are re-registered with the manager.

Prerequisites:

• Ensure that all the packages are upgraded to the latest version on all Privileged Account Manager agents and managers.

• Enable FIPS on the operating systems hosting the managers and the agents.

FIPS mode in Privileged Account Manager can be enabled only on Windows and Linux operating systems, for both managers and agents. FIPS mode in Privileged Account Manager is not supported on Unix operating systems. For a complete list of the supported Windows and Linux operating systems, see Privileged Account Manager 4.4 System Requirements and Sizing Guidelines.

To enable FIPS:

1 Enable FIPS on Privileged Account Manager:
   1a Log in to the Privileged Account Manager Administration Console.
   1b Click Hosts > Host Status > Enable.
   1c (Conditional) To enable FIPS immediately on agents, re-register agents manually. For more information about re-registering agents manually, see the Privileged Account Manager Administration Guide.

2 Enable FIPS on the target machines for the following:
   • (Conditional) RDP relay
   • (Conditional) Credential checkout of applications and databases: Enable FIPS mode on Java that is installed on the system hosting the application.
Securing Privileged Account Manager at Application Level

The following sections outline security considerations for Privileged Account Manager at Application Layer level:

NOTE:

- Privileged Account Manager has TLS 1.2 enabled by default.
- For Password Management, ensure to use ports 5985 and 5986.
- Privileged Account Manager bundles FIPS-capable OpenSSL 1.0.2 and for encrypting all communication channels for all communication channels with internal and external services. It also uses OpenSSL 1.0.2 for the encryption of data in details such as, Credential Vault, confidential configuration data.

Ensure to use the privileged access approach while accessing the product. For more information, see Configuring Privileged Access.

The following are recommended access policies:

- Allow/Deny commands instead of the complete session access. For more information, see Application Command List.
- Just-In-Time Access Framework. For more information, see Just In Time Access Framework.
- Configured user roles added in the Administrator group instead of complete access. For more information, see Configuring a User Role.
- Configuring Command Risk. For more information, see Setting the Command Risk.
- Section 3.1, “Using Audit Settings,” on page 14
- Section 3.2, “Using the Encryption Settings,” on page 14
- Section 3.3, “Enabling the FIPS Mode,” on page 15
- Section 3.4, “Disabling the CBC Mode,” on page 15
3.1 Using Audit Settings

The default configuration does not encrypt or roll over the audit databases. If your security model requires you to keep audit records available for years, you need to configure the rollover options and move the rolled-over files to an archive location.

To set the Audit configuration:

1. Click Reports > Settings > Audit Settings on the home page of the Privileged Account Manager console.
2. Specify the details for each audit database file, set the rollover parameters. Rolled-over databases are kept as SQLite databases.

3. Click Finish.

3.2 Using the Encryption Settings

Use this page to configure database encryption when the randomly generated encryption key is changed.

1. Click Reports > Settings on the home page of the console.
2. Click Encryption Settings in the task pane.
3 The **NULL Cipher (clear text)** key is enabled at Reports Settings > Encryption Settings by default. If you want to encrypt the databases then you must first disable the null cipher and then change the database to encryption and save. Privileged Account Manager encrypts all the databases, which has the Protection set to Encrypted in Reports Settings > Audit Settings, with the latest key. This can be very time-intensive and can affect performance until it is completed.

4 To specify how frequently the key is changed, move the Key Rollover slider to the right and specify a Key Rollover interval by selecting the type of interval (years, months, weeks, or days).

5 (Optional) In the Encryption Keys list, disable or enable keys by moving the slider to the right or left against the respective Key ID. Each time a new key is generated, it is added to the list. If you disable a previous key, Privileged Account Manager re-encrypts all databases with the old key to the latest key. This can be very time-intensive and can affect performance until it is completed.

If you disable the null cipher key, Privileged Account Manager encrypts all the databases, which has the Protection set to Encrypted in Reports Settings > Audit Settings, with the latest key. This can be very time-intensive and can affect performance until it is completed.

6 Click Finish.

### 3.3 Enabling the FIPS Mode

For information, see Section 3.3, “Enabling the FIPS Mode,” on page 15.

### 3.4 Disabling the CBC Mode

In Privileged Account Manager, Cipher Block Chaining (CBC) mode is enabled by default. Disabling this mode, ensures that the CBC mode is not used for communication by product components such as PAM Manager, Privileged Account Manager Agent, Privileged Account Manager Administration Console, Privileged Account Manager User Console, and target applications.

**IMPORTANT:**

- When you disable CBC Mode:
  - It is disabled immediately on all the managers that have the registry module.
  - The primary registry manager is disabled first, followed by the other registry managers, and then the associated agents. Automatic re-registration of agents happens once in two days. Therefore, it may take up to two days for CBC Mode to be disabled automatically on all the agents.
  - For agents in Offline state, CBC Mode will be disabled only after the status changes to Online and the agents are re-registered with the manager.

**Prerequisites:**

Ensure that all the packages are upgraded to the latest version on all Privileged Account Manager agents and managers.
To disable CBC mode:

1. Log in to the Privileged Account Manager Administration Console.
2. Click **Hosts > Host Status**, and then click **Disable** next to **CBC Mode**.
3. (Conditional) To disable CBC mode immediately on agents, re-register agents manually. For more information about re-registering agents manually, see the *Privileged Account Manager Administration Guide*. 
Securing Network Settings and Strengthening Deployment Settings

The following sections outline the security considerations for Privileged Account Manager at Network system or deployment level:

- Section 4.1, “Opening Firewall Ports,” on page 17
- Section 4.2, “Protecting Privileged Account Manager through Firewall,” on page 17

4.1 Opening Firewall Ports

The Firewall port 29120 is used for all the communication among the Framework managers and the agents. Port 29120 is also used for communications among the Framework agents.

If firewalls separate your Privileged Account Manager machines, 29120 port must be opened to traffic in both directions for Privileged Account Manager to work properly.

The port is specified when the agent is registered with the Framework Manager. If you need to specify a different port if the port 29120 is already in use, 29120 port must be opened in the firewall settings for communication.

NOTE: For RHEL 8.x, you can use:

- **firewalld**: Use the `firewalld` utility for simple firewall use cases.
- **nftables**: Use the `nftables` utility to set up complex and performance critical firewalls, such as for a whole network.
- **iptables**: The `iptables` utility on Red Hat Enterprise Linux 8 uses the `nf_tables` kernel API instead of the legacy backend.

The `nf_tables` API provides backward compatibility so that the scripts that use `iptables` commands still work on Red Hat Enterprise Linux 8. For new firewall scripts, Red Hat recommends to use `nftables`.

For information about Database ports for Database Monitoring, see Setting the Command Risk.

4.2 Protecting Privileged Account Manager through Firewall

You can protect the Privileged Account Manager with firewalls. The following is an illustration of a firewall setup for a basic Privileged Account Manager configuration.
The following ports are used by Privileged Account Manager Agent and Manager:
<table>
<thead>
<tr>
<th>Platform</th>
<th>Network Ports</th>
<th>Purpose of the Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>443</td>
<td>For administration and user Web console access over HTTPS protocol.</td>
</tr>
<tr>
<td></td>
<td>2222</td>
<td>SSH proxy for privileged access.</td>
</tr>
<tr>
<td></td>
<td>13389</td>
<td>RDP proxy for privileged access.</td>
</tr>
<tr>
<td>Manager</td>
<td>Database Access Through Privileged Account Manager Proxy</td>
<td>For database monitoring functionality</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>For administrator and user Web console access over HTTPS protocol.</td>
</tr>
<tr>
<td>Privileged Account Manager Windows</td>
<td>13389</td>
<td>RDP proxy for privileged access.</td>
</tr>
<tr>
<td></td>
<td>29120</td>
<td>For agent and manager TLS communication.</td>
</tr>
<tr>
<td>Agent</td>
<td>Linux, Unix, and Windows</td>
<td>29120 For agent and manager TLS communication.</td>
</tr>
</tbody>
</table>

Securing Access to the Privileged Account Manager Console

The following options enhance the security of the communication between browsers and the product console. These configuration options do not affect the communications between the manager and the agent.

<table>
<thead>
<tr>
<th>Task</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Login Session Timeout helps secure the product while monitoring sessions timing.</td>
<td>See, Adding a User.</td>
</tr>
<tr>
<td>♦ Types of authentication for local, LDAP, RADIUS, OAuth users, Advanced Authentication. Recommends to use along with multi-factor authentication. MFA is supported with AA, RADIUS and OAuth. Most secure option recommended is the OAuth authentication.</td>
<td>See, OAuth2.</td>
</tr>
<tr>
<td>Using the password restrictions on LDAP Servers</td>
<td>See, Configuring LDAP Server Settings.</td>
</tr>
<tr>
<td>Second factor authentication with Advanced Authentication and RADIUS.</td>
<td>See, Advanced Authentication</td>
</tr>
<tr>
<td>Backup Administrator User Creation</td>
<td>See, Managing Users and Groups.</td>
</tr>
<tr>
<td>Wildcard and third-party certification for HTTPS.</td>
<td>See, Exporting the Certificate From the Active Directory Server.</td>
</tr>
<tr>
<td>Using tokens instead of username and password for the following:</td>
<td>See, Enabling Users to Generate API Tokens.</td>
</tr>
<tr>
<td>♦ Password Checkin and Checkout using APIs. For more information, see Application to Application Password Management and Password Management</td>
<td></td>
</tr>
<tr>
<td>♦ Authentication of SSH Relay</td>
<td></td>
</tr>
</tbody>
</table>

♦ Section 5.1, “Requesting a Certificate for the Framework Manager Console,” on page 22
♦ Section 5.2, “Securing the PAM Manager,” on page 23
♦ Section 5.3, “Privileged Account Manager and Agent Communication,” on page 23
♦ Section 5.4, “Privileged Account Manager Communication with External Services,” on page 23
♦ Section 5.5, “Credential Vault,” on page 23
5.1 Requesting a Certificate for the Framework Manager Console

For added security, you can install a certificate to use when accessing the Framework Manager console. To access this security option, you need to select the Administration Manager (admin) package on the host that you want to protect. You must then complete a certificate request form, send it to your chosen certification authority, and then install the certificate that you receive from the certificate authority.

**NOTE:** By default, OpenSSL accepts DNS, email, URI, RID, IP, dirName as a Subject Alternative Name (SAN). Privileged Account Manager uses OpenSSL to generate a Certificate Signing Request (CSR). When requesting a certificate in Privileged Account Manager, use the Alternative Names in the console as the "DNS" attribute.

Syntax for Alternative Names is:

- DNS:example.com, DNS:www.example.com
- DNS:example.com, DNS:www.example.com, IP:127.0.0.1

1. On the home page of the console, click **Hosts**.
2. In the navigation pane, select the host that you want to protect with a certificate.
3. In the details pane, click **Packages** and select the Administration Manager (admin) for the Framework Manager console.
4. Click **Request Certificate** in the task pane.
5. Specify the necessary details as described in your chosen certification authority documentation.
6. Click **Finish**.
   
   The text for your certificate request is displayed in the text area.
7. Copy the certificate request into an e-mail and send it to your chosen certification authority.
8. Install the certificate that you receive from certificate authority.

5.1.1 Installing a Certificate

After you receive the requested certificate from your certificate authority:

1. Copy the certificate to the machine you use to access the Framework Manager console.
2. On the home page of the console, click **Hosts**.
3. In the navigation pane, select the host where you want to install the certificate.
4. In the details pane, click **Packages** and select the Administration Manager (admin) package for which you have requested the certificate.
5. Click **Install Certificate** in the task pane.
6. Paste the certificate into the text area.
7. Click **Finish**.
5.2 Securing the PAM Manager

The following table helps you understand how you can secure the PAM manager.

<table>
<thead>
<tr>
<th>Task</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Relay</td>
<td>You can disable weak MAC Algorithms on a Secure Shell Server. Configured in ssh_config and ssdh_config settings from Developer help or pages of ssh_config and ssdh_config</td>
</tr>
<tr>
<td>Module level DB Encryption</td>
<td>See, Modifying a Host</td>
</tr>
<tr>
<td>Audit database Encryption</td>
<td>See, Using Audit Settings</td>
</tr>
<tr>
<td>Oracle database specific SSL and TLS configuration</td>
<td>Although, Privileged Account Manager supports SSLv3 for older servers and clients, but the recommendation is to use the most current TLS version.</td>
</tr>
</tbody>
</table>

5.3 Privileged Account Manager and Agent Communication

The PAM manager and Agent certificates are renewed every 2 days for more secure communication.

5.4 Privileged Account Manager Communication with External Services

For securing connections with external services such as, Advanced Authentication, LDAP, RADIUS, Mail, PowerShell etc, see Integration with External Services.

5.5 Credential Vault

All the confidential data, such as passwords and SSH keys, of each account of all the resources are encrypted using AES-256-CBC and stored in the Credential Vault module of the Privileged Account Manager. For more information, see Credential Vault.
Getting the Latest Security Patches

After installing Privileged Account Manager, download the software and the license from the Software License and Download (https://sld.microfocus.com/) portal. For information about how to download the product from this portal, watch the following video.

http://www.youtube.com/watch?v=esy4PTVi4wY