# HP Security Manager
Release Notes v3.6.1

## Table of contents

- **Overview** 2
- **Key Features** 2
- **What’s New in Security Manager 3.6.1?** 3
  - Features and Usability Improvement 3
  - New Policy Items and policy changes 5
  - New Devices Supported 5
  - Fixes 5
- **Software Notes and Known Issues** 6
- **Installation** 8
  - Installation Notes 9
- **Supported Operating Systems and Databases** 10
- **Hardware Requirements** 10
- **VMware and Hypervisor Support** 10
- **Solutions** 10
- **Network Port Assignments** 11
- **Ports diagram** 13
- **Appendix A** 14
  - Release History 14
- **Appendix B** 33
  - Other HP Security Manager Whitepapers and Manuals 33
Overview

Announcing HP Security Manager 3.6.1, the latest release of the industry’s first policy-based solution that helps you increase security, strengthen compliance, and reduce risk across your imaging and printing fleet. With Security Manager, you can gain control of your fleet by enabling an effective, policy-based approach to securing HP imaging and printing devices. Through the intuitive and intelligent security policy editor, you can easily create a custom and comprehensive device security policy that is suited for your specific environment.

A Security Manager Base Policy template is provided as a great place to begin creation of a custom security policy or to use as is, if appropriate, as a baseline security policy for your environment. You can schedule the Assess and Remediate task to execute on a daily, weekly or monthly basis to monitor the print environment for settings that do not comply with the chosen security policy, and then automatically return those settings to the policy-specific state. In addition, the Security Manager Instant-On Security feature can place your HP imaging and printing device into the desired security state, as soon as it is attached to the network. The Instant-On Security feature is also invoked when the device is cold-reset or changes IP addresses.

Security Manager also offers a Fleet Certificate Management solution. This feature eliminates the manually deployed, singular device, network certificate implementation process and replaces it with an automatic, fleet based, security policy centered method of certificate management. By using this feature, you can easily replace the default device self-signed certificate with an authorized Certificate Authority (CA) signed certificate and manage it for validity, expiration, and revocation. Implemented as an extension of the Security Manager policy editor, this solution handles network certificate management as a background task like any other Security Manager assessment and remediation.

Key Features

- The Security Manager Instant-On Security feature allows supported devices to automatically locate the Security Manager server and receive your company approved device security policy as soon as the device is attached to the network. Instant-On Security then maintains policy-based compliance during device resets and address changes.

- The Security Manager Policy Editor allows print administrators with minimal security knowledge, as well as experienced security administrators, to build a valid, comprehensive security policy to deploy across the HP imaging and printing fleet. The Policy Editor provides security setting intelligence through basic definition, recommendations, validations and constraints to ensure creation of a valid policy. A Security Manager Base Policy template is provided as a great place to begin creation of a custom policy or to use as is, if appropriate, as a baseline policy for your environment.

- Security Manager can be scheduled to assess and remediate devices on a daily, weekly or monthly occurrence. When configured in this fashion, Security Manager automatically assesses your fleet for its current setting and returns non-compliant settings to the desired state of the security policy used in the assessment. Unlike other management tools, Security Manager only fixes what is out of compliance, then it reports on exactly what was out of compliance that had to be remediated. This is valuable in understanding where vulnerabilities exist in your environment.

- The Security Manager Certificate Management solution replaces a manual, highly interactive network certificate deployment process with an automated policy-based solution that deploys and manages network certificates like any other assessed and remediated Security Manager device security setting. Automated fleet deployment of Certificate Authority (CA) signed certificates to accommodate encrypted printing, 802.1x protected network authentication and other print environment related encryption/authentication needs is now possible with this solution.
What’s New in Security Manager 3.6.1?

Features and Usability Improvement

Several configuration options have been added in this release to improve performance and to prevent that devices are ending up in Credentials Error. In order to validate if a configuration changes, is making a positive impact, you must first get a baseline of your current HPSM implementation. This means check for a couple of days how much time HPSM needs to perform a task (assessment only, or assessment and remediation) on all devices, how much time does HPSM need to perform a Verify on all devices, how many devices will end up with credentials error after any of this? After collecting this kind of data, change one of the new parameters and validate that the change has a positive impact in your environment. Then start with the next parameter, until you found an optimal performance for your HPSM installation.

New configuration setting which can impact performance:

- Added configuration option `usePassWordCheck` in `EapDeviceLib.config`. Changing this setting to true should improve the performance while performing assessment and remediation tasks.
- Added the configuration options `MaxOldRecommendationRecordsToDelete` and `MaxDeviceRecordsToDelete` in the `HPSM_service.exe.config` with the default value of ten thousand (10000). The higher the number, the more records can be deleted during the nightly maintenance in a single transaction. In previous HPSM versions the value was hardcoded to ten thousand. When the value for these configuration options are increased (for example till 100k), then the `MaintenanceTaskQueryTimeout` has to increased as well (for example to 1200). After making the changes the HPSM service has to be restarted and the `hpsm_service.log` file should be checked to make sure that no timeout occurred after increasing the maximum number of records to delete.

In HPSM 3.6 the following configuration settings which can impact performance had been added:

- Added configuration option `httpTimeout` in `EapNetworkLib.dll.config`. By default this is set to 60 seconds. Tuning this option can improve performance with devices in inconclusive state (devices which are temporarily unreachable over port 7627/web services and which end up with device status “Credentials Not Validated or Incorrect” from HPSM 3.6 onwards). For every config item which is using web services, the default time out of 60 seconds will be used. Recommendation is to change this timeout to 20 seconds and monitor if this brings indeed faster assessment and remediation. Due to this new lower timeout, you might run into more remediation issues for devices which are reachable on the network.
- The configuration option `AllowRepetitiveInstantOnPolicyAfter` has been added in the `hpsm_service.exe.config` file (see the installation and setup guide). This setting can be used to improve performance, without running the risk of adversely impacting the system performance. With a value of 0:0:15 duplicated instant on processing within a timespan of 15 minutes can be prevented. A higher value can help to improve performance, but introduces the risk of missing an instant-on message.

Note: after making changes to the EAP*.config files, the HPSM service has to be restarted in order to use the new values.

New configuration settings which can impact number of devices in 'Credentials Error' and performance:

By default HPSM is trying to use the device specific credentials, if that fails, then HPSM will use the global credentials and if that fails HPSM will be using the default credentials (which means blank EWS password and SNMPv1/v2 community name of public). With the new options this behavior can be changed.

- Added configuration option `eapAdminCredentialRetryDelay` a in `HPSM_service.exe.config` file. When (temporarily) a network connection over web services (port 7627) cannot be established, then the EWS password cannot be validated. By default HPSM will try to use the global credentials after trying the device specific EWS password which is stored in HPSM, even if the password could not be
validated. In order to retry the same device specific password, you need to configure eapAdminCredentialRetryDelay. Internal testing showed improvements with a delay value of 500. By default this is set to -1, which means that the device password will always be tried once.

- Added configuration option CredentialRetryWhenInconclusive in HPSM_service.exe.config file. When (temporarily) a network connection over web services (port 7627) cannot be established, then the EWS password cannot be validated. By default HPSM will only try to use the global credentials after trying the EWS password which is stored for the device in HPSM, if the device password and global password are different. Even if the password could not be validated. In order to retry with the global password when it's the same password as the device password and when the device EWS password could not be validated (inconclusive), you need to configure CredentialRetryWhenInconclusive with the value true.

- Added configuration option UseDefaultCredentials in HPSM_service.exe.config file. By default this is set to true. When changing this to no, HPSM will no longer try with the default credentials. Such a change can have two effects. 1. It can increase performance when all devices on the network are configured with a password. 2. It can prevent that a device is ending up with Credentials Error after failing with device password, global password and default password. Instead it could display a more device specific password error as default credentials are no longer used.

Note: after making changes to the HPSM_service.exe.config files, the HPSM service has to be restarted in order to use the new values.

New devices statuses are now available. This means you can now have one the following device credential statuses:
- Good
- Credential Error
- Credentials not Validated or Incorrect (introduced in 3.6.0)
- EWS not Verified (introduced in 3.6.1)
- SNMP Credential Error (introduced in 3.6.1)

After automatically stopping the nightly maintenance task, HPSM will now display if the maintenance task was finished. The following statuses can be seen for the maintenance task:
- Maintenance task has not been completed on <date> <time>
- Maintenance task completed successfully on <date> <time>
- Maintenance task is in progress and performance might be degraded.

Note: the maintenance task consists of several components. One of them is to clear the old recommendations. This part of the maintenance task is by default limited to 30 minutes with the configuration option ClearOldRecommendationTasksMaxDuration in the HPSM_service.exe.config file.

In order to prevent heavy load on the database during the nightly maintenance performance, it’s now possible to configure HPSM to queue new instant on announcements during the nightly maintenance, and to queue new (assessment and remediation) task during the nightly maintenance instead of executing them immediately. The queued items will be processed after the maintenance task has been completed. By default instant on messages and new tasks will be processed during the nightly maintenance, but if desired this can be changed by setting the configuration option AllowScheduledTasksDuringMaintenanceTaskRun to false in the HPSM_service.exe.config and restarting the HPSM service.

The following table shows the HPSM behavior with the different values for this new parameter:
The word “Jetadvantage” has been removed from the product name, which has become HP Security Manager. Name changes in the HPSM installer will be done in a later release.

**New Policy Items and policy changes**

No new policy items added in 3.6.1.

**New Devices Supported**

No new devices supported in 3.6.1.

**Fixes**

- HPSM-749 All ECDH ciphers are available in existing policies after upgrading from 3.5 or older to HPSM 3.6.1
- HPSM-668 HPMS is now correctly recognizing a revoked certificate (using the URL of the CRL)
- HPSM-536 Textual explanation for CSR source has been improved
- HPSM-451 HPMS is now showing Credential not Validated or Incorrect when port 7626 is blocked during device verification
- HPSM-628 When **OverwriteDevicesWhenIPsMatches** is set to true, duplicate IPs will now be prevented
- HPSM-611 HPMS will now poll the SCEP server, while the SCEP server is creating the certificate and the SCEP server responded with a status of 3 (wait) to the download request from HPMS. Comodo SCEP are using this wait response if needed.
- HPSM-729 Devices are no longer being removed from manual groups during nightly maintenance when at least one device is in Network Communication Error after running a task or verify operation on the manual group
- HPSM-470 HPMS can now also configure access control rights when solutions are installed as an IPA agent. Previously HPMS could only configure access control rights when solutions were installed as an OPA agent (and the solution was visible in the EWS under the section Solutions Installer from the General tab in the EWS.
- HPSM-791 The word failed is now spelled correctly in the log file
- HPSM-542 The "Group membership" column is no removed after several configuration steps
- HPSM-612 HPMS will now send automated email after finishing a remediation task when a cloud mail Server (no windows authentication) is used
- HPSM-743 To prevent lots of devices ending up with credential status as Credentials Not Validated or Incorrect, it’s now possible to configure the **CredentialRetryWhenInconclusive** to **true** with a corresponding **eapAdminCredentialsRetryDelay** (wait time) of for example 500 (ms). These changes have to be made in the HPMS_service.exe.config file and require a restart of the HP Jetadvantage Security Manager Service.
- HPSM-637 Device Status EWS Not Verified and SNMP Credential Error have been added (previously this was all displayed as Credential Error)
- HPSM-826 InstantOn message are no longer processed nor forwarded to a secondary listener when Allow Device Announcement Reflection is disabled
- HPSM-560 Host names which starts with a number are no longer changed (characters after the

---

<table>
<thead>
<tr>
<th>Versions</th>
<th>AllowScheduledTasksDuringMaintenance</th>
<th>Discovery</th>
<th>Verification</th>
<th>Assessment / A&amp;R</th>
<th>Instant on Discovery</th>
<th>Instant on Verification (no instant on policy)</th>
<th>Instant on / Autogroup A&amp;R</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPSM 3.6</td>
<td>NA</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
</tr>
<tr>
<td>HPSM 3.6.1</td>
<td>false</td>
<td>Queued</td>
<td>Queued</td>
<td>Queued</td>
<td>Running</td>
<td>Running</td>
<td>Queued</td>
</tr>
<tr>
<td>HPSM 3.6.1</td>
<td>true</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
</tr>
</tbody>
</table>

While maintenance task runs

<table>
<thead>
<tr>
<th>Versions</th>
<th>AllowScheduledTasksDuringMaintenance</th>
<th>Discovery</th>
<th>Verification</th>
<th>Assessment / A&amp;R</th>
<th>Instant on Discovery</th>
<th>Instant on Verification</th>
<th>Instant on / Autogroup A&amp;R</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPSM 3.6</td>
<td>NA</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
</tr>
<tr>
<td>HPSM 3.6.1</td>
<td>false</td>
<td>Queued</td>
<td>Queued</td>
<td>Queued</td>
<td>Running</td>
<td>Running</td>
<td>Queued</td>
</tr>
<tr>
<td>HPSM 3.6.1</td>
<td>true</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
<td>Running</td>
</tr>
</tbody>
</table>
numerical values were getting removed in HPSM UI after device verification

- HPSM-721 Device counts between device page and left group pane window are no longer getting out of sync
- HPSM-667 After the weekly maintenance (Sunday night), the error "Insufficient licenses. Licenses have expired..." issue is no longer happening
- HPSM-716 During de-installation of HPSM 3.6.1, which has been upgraded from HPSM 3.5 you will no longer get an error message about the HP Print License Service (which is no longer available from HPSM 3.6 onwards)
- HPSM-812 HPSM is now longer intermittently showing 'Failed to retrieve the data' license error
- HPSM-718 Telnet policy item is now also working correctly for HP LaserJet M110 and HP LaserJet M140
- HPSM-661 Device status is no longer changing continuously when clicking on Refresh when the task is still in progress.
- HPSM-823 When configuring SNMPv1/v2 policy you can no longer configure a community name (in line with current Futuresmart EWS behavior)
- HPSM-754 HPSM is displaying in the assessment details for Syslog Protocol ‘Match’ instead of ‘Not Supported by Device’.
- HPSM-726 Flexera has been upgraded
- HPSM-820 Whitepaper links are no longer static, and Help, About Whitepapers is now referring to generic download location
- HPSM-817 HPSM UI now shows if maintenance task was completed or not and maintenance task will now have configurable options for the number of records to be deleted in the hpsm_service.exe.config file.
- HPSM-783 New/fresh HPSM installation are now configured with AutoLogoutEnabled set to true. This can be changed after installation, see the install and setup guide.
- HPSM-638/769 Disk Encryption Status Policy now supports if multiple (internal) disks/USB devices available in the device
- HPSM-793 Product name change in UI: HP JetAdvantage security Manager has been renamed into HP Security Manager
- HPSM-449/112215 HPSM no longer shows status as ERROR when remediating an HP Futuresmart printer with a policy which includes disk encryption status after performing a partial clean on the device with USB drive inserted.

Software Notes and Known Issues

- If the nightly maintenance task is not completing within 30 minutes after upgrading, then it’s recommended to run the following script once:

```sql
USE HPIPSC ; -- HPSM database name
DECLARE @X INT=1;
DECLARE @DeleteOlderThan INT=10; -- Days. Records older than this day will be deleted
WAY:
SELECT TOP 10000 * into #NEWTABLE FROM
(SELECT rec.ID AS recID, rToret.KEY_ID as rToretID, rt.ID AS rtID, rvt.ID as rvtID, rTorv.ID AS rTorvID,
rTorat.KEY_ID AS rToratKEY_ID, rat.ID AS ratID, av.ID AS avID, raTop.ID AS raTopID
FROM dbo.RecommendationTable rec
LEFT OUTER JOIN dbo.RecToReasonsTable rToret ON rToret.KEY_ID = rec.ID
LEFT OUTER JOIN dbo.ReasonTable rt ON rt.ID = rToret.Reason
LEFT OUTER JOIN dbo.ReasonToReasonValuesTable rTorv ON  rTorv.ID = rt.ID
LEFT OUTER JOIN dbo.ReasonValueTable rvt ON rvt.ID = rTorv.ReasonValue_ID
LEFT OUTER JOIN dbo.RecToRecommendationActionsTable rTorat ON rTorat.KEY_ID = rec.ID
LEFT OUTER JOIN dbo.RecommendationActionTable rat ON rat.ID = rTorat.RecommendationAction
LEFT OUTER JOIN dbo.AssessmentValueTable av ON av.ID = rat.ActionValue_REF
LEFT OUTER JOIN dbo.RecActionsToParametersTable raTop ON raTop.ID = rat.ID)
```
where rec.Date < getdate() - @DeleteOlderThan Or rec.AssessmentAndPolicyUniqueID NOT IN ( select distinct dal.assessmentAndPolicyUniqueID as uniqueID from dbo.DeviceAssessmentLogTable dal where dal.State = 2 ) ) as Sub1

--select count (*) from #NEWTABLE

DELETE a FROM dbo.RecToRecommendationActionsTable a INNER JOIN #NEWTABLE B ON a.KEY_ID = B.rToratKEY_ID
DELETE a FROM dbo.RecToReasonsTable a INNER JOIN #NEWTABLE B ON a.KEY_ID = B.rToretID
DELETE a FROM dbo.RecommendationTable a INNER JOIN #NEWTABLE B ON a.ID = B.recID
DELETE a FROM dbo.ReasonToReasonValuesTable a INNER JOIN #NEWTABLE B ON a.ID = B.rTorvID
DELETE a FROM dbo.ReasonTable a INNER JOIN #NEWTABLE B ON a.ID = B.rtID
DELETE a FROM dbo.ReasonValueTable a INNER JOIN #NEWTABLE B ON a.ID = B.rvtID
DELETE a FROM dbo.RecActionsToParametersTable a INNER JOIN #NEWTABLE B ON a.ID = B.raTopID
DELETE a FROM dbo.RecommendationActionTable a INNER JOIN #NEWTABLE B ON a.ID = B.ratID
DELETE a FROM dbo.AssessmentValueTable a INNER JOIN #NEWTABLE B ON a.ID = B.avID

SET @X = (select count (*) from #NEWTABLE)

drop table #NEWTABLE

IF @X=10000 GOTO WAY;

• 111911 The groups pane on the left might show different number of devices for the same group which is listed in the main window/pane. While this can no longer happen with HPSM 3.6.1, it’s possible the counters where out of sync before upgrading to HPSM 3.6.1. In that case you need to run the following script on the HPSM database to remove the historical incorrect data:

use HPIPSC

--Delete unused DeviceNodeIndentity entries
Delete from dbo.DeviceToDeviceNodeIdenityTable where Device_ID not in (select ID from DeviceTable where state=2)

This has been fixed for some scenarios in 3.6. Other scenarios are under investigation.

• HPSM-450/107960 An assessment or assessment and remediation task for HP Designjet Z3200ps 24in Photo, HP DesignJet Z2600 PostScript, HP Designjet Z6600 and HP Designjet T7100 devices will fail even while the device is supported by HPSM. This issue is under investigation by HP.

• HPSM-778 SNMPv3 password Complexity cannot be configured for the following flexworker devices with the HP default flexworker policy: HP LaserJet Managed MFP E42540f, HP Color LaserJet Managed MFP E47528f, HP Color LaserJet Managed E45028dn, HP LaserJet Managed E40040dn. This will be fixed in Futuresmart 5.3.

• HPSM-884 Credential error when SNMPv3 has been disabled on the device via the EWS or WJA, and while SNMPv3 has been configured previously by HPSM.

Workaround: Remove the SNMPv3 credentials which have been stored in HPSM for this device and run restart the Verify/Task.

• 112029 Some HPSM Configuration values are not updated after upgrade. HPSM 3.5 introduced the following new default settings:

PolicyChangeNotification is now disabled
EAPRetry = 1
snmpRequestTimeout = 5000
timeBetweenEapRetry= 1000

During an upgrade the PolicyChangeNotification will always be disabled, regardless of it's value before the upgrade. If this doesn’t match the desired behavior, change the settings in the hpsm_service.exe.config file and restart the HPSM service.

• 112301 When user switch the language from non-English language to a different non-English language the fonts and styles are not loading properly.

Resolution: Refresh the browser or open HPSM in a new browser tab.

• 109548 The HPSM installer is using powerscript files (CheckIISInstalled.ps1 and IISInstall.ps1) to
install HPSM. HPSM installation will fail to correctly install HPSM if local security policies do not allow to run unsigned powerscript files.

**Resolution:** temporarily allow to run unsigned powerscript files during HPSM installation.

- 110914 Unable to install ID certificate on DesignJet T790 and Z6 when the device is set to a non-English language. The following error message will be visible: "The certificate request returned from the printer was empty". This is caused by a firmware limitation.

**Resolution:** Change the language of the device to English before installing the ID certificate with HPSM.

- HPSM-668 HPSM is not recognizing revoked certificate over LDAP. This will be fixed in a later release.
- Older versions of Web Jetadmin may not have assigned rights for Network Service to use its self-signed certificate. If so, Instant on Reflection will fail if attempting to add Instant On discovered devices to that Web Jetadmin installation. Manually assign rights for Network Service to use the self-signed certificate to resolve.
- Email Summary Remediation report sent via email claims devices are remediating successfully when they are powered down and cannot be remediating successfully.
- Upgrades from version 2.1.2 directly to version 3.1 or beyond are not supported and will result in tasks being unable to run. Upgrade to version 2.1.4 or 2.1.5 first from version 2.1.2 before upgrading to version 3.1 or beyond.
- A locked policy automatically becomes unlocked after 2 hours.
- For better representation of pages, maximum recommended zoom is 150%.
- For the Web Encryption Strength individual ciphers, a device status can display as Network Connection Error if the device is verified after applying a policy with RC4-SHA and RC4-MD5 ciphers enabled. In order to ensure communication between a server and client, both sides need to have the same set of supported ciphers. If a device is set to use RC4-SHA/RC4-MD5 as the active ciphers after remediation, but the operating system doesn't support these ciphers, a Network Connection Error will be displayed. RC4-SHA and RC4-MD5 are considered weak ciphers and are not supported in the operating system.
- DesignJet devices do not allow device guest permission to be configured from Security Manager under Role Based Access Control if the devices are not configured with an Admin password.
- If a Policy has Subject Alternate names (SANs) enabled with a Domain name entered to include the Universal Printer name (UPN) as a SAN, the UPN is sent as ‘username@domainName’ to DNS. This is not accepted by an OpenTrust CA.
- If browser security level is set to High, Security Manager will not be able to perform any file related operations in IE until the security level is set to any other stage.

**Installation**

The Security Manager software is provided as a universal installation executable that is compatible with all supported operating systems. Installation options include a full local install or a full local install with a remote database option. For proper Security Manager installation and operation, specific Microsoft software must be present.

The detailed requirements are listed in the install and setup guide. Required:

- Microsoft SQL Server Database
- Microsoft Internet Information Services (IIS) - (part of installation script)

If these are not present on the system, the installation process installs some of the required software. This includes the option to install the Microsoft SQL Server Express 2019 database which is bundled with the product.

**Note:** SQL Express 2019 is not supported on all operating systems. When using an operating system on which SQL 2019 is not supported, then you must install manually an older version of SQL (Express) before starting the HPSM installer.
Installation Notes

- The browser-based interface requires Internet Information Services (IIS) in order to operate. The installer will verify that IIS is enabled with the proper settings enabled and will offer to enable the proper settings if desired. The Installation Guide specifies the proper IIS setting to be enabled if it is desired to perform manually. If the installer fails to set some of the IIS settings, it may be necessary to configure them manually. Since the installer is attempting to enable IIS, it may prompt for a machine restart.
- The browser-based interface is set to use port 7637 by default during installation. Security Manager is launched in a browser as such: https://localhost:7637. If it is desired to change this port, it can be changed by editing the bindings for the HPSM web site under IIS Manager.
- The browser-based interface offers the ability to use an existing server certificate or to create a self-signed certificate during installation. The self-signed certificate allows the data to be encrypted between client and server, while an existing server certificate not only encrypts data but also provides trust that the server is who it says it is. IIS will always search and bind for the server certificate in the personal store of computer account. An identity certificate needs to be of the type “Server Authentication” in order to provide trust.
- The browser-based interface supports Microsoft Internet Explorer, Google Chrome and Microsoft Edge Chromium based. The following settings may need to be configured on certain machines or operating systems if Security Manager is having difficulty loading:
  - Internet Explorer may require the “Display intranet sites in Compatibility View” box to be unchecked under Compatibility View Settings if the login screen for Security Manager is not appearing.
  - Internet Explorer may require the “Bypass proxy server for local addresses” box to be checked under Internet Options, Connections, LAN Settings if the login screen for Security Manager is not appearing.
  - Windows 10 may require HTTP2 to be disabled in the browser if Security Manager continually logs out the user.
- Newer versions of Google Chrome may require the following technique to disable HTTP2:
  Launch chrome by disable http/2 through RUN cmd.
  Open RUN prompt and type “chrome.exe --disable-http-2”
  Open registry and add two new parameters:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\EnableHttp2Cleartext DWORD 0
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\EnableHttp2Tls DWORD 0
- Based on the system state, in some cases, installation/uninstallation prompts for a system restart. This is caused by the MS Installer seeing a particular value present in the registry. A workaround rather than rebooting is to change an entry available in registry:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperation
    This entry needs to be deleted if it exists.
- Users need to be re-added to the HPISPC group after software upgrade.
- Licenses need to be re-loaded if the operating system is upgraded.
- Licenses need to be re-added if the database is being restored from 2014 to 2016 SQL Express.
- The Security Manager service must have the proper permissions to access the Security Manager service database. If the service and database are installed on the same computer, the installation process manages the assignment of database permissions. If the service and the database are installed on separate computers, you must configure the correct permissions for the remote database. For complete Security Manager installation information, see the Security Manager Installation and Setup Guide at www.hp.com/go/securitymanager. Also see the whitepaper titled “HP Security Manager - Using Microsoft® SQL Server” for more information.
- If a firewall is installed on the computer on which the Security Manager service runs, and the service will be accessed from the user interface on a remote computer, the firewall must be set to allow access to the service. The older Security Manager service listens on port 8002, which must be opened in the firewall to allow remote access to the service. The new browser-based interface listens on port 7637 by default. If you do not want to allow remote access to the Security Manager web service for either version, then you can block the respective ports with a firewall.
- For complete uninstallation, all the HPSM installation files/folders should be closed before uninstalling.
**Supported Operating Systems and Databases**

See setup and install guide. As SQL databases are missing in the install and setup guide, they are temporarily listed here:

**Tested Databases**
- Microsoft SQL Server Express 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server Express 2019 (bundled with HPSM 3.6.1 installer)

HP Jet Advantage Security Manager requires a Microsoft SQL database to store data. For customers who do not have their own full SQL Server or do not want to use a SQL license, Security Manager bundles a recent version of SQL Server Express that can be installed and used if desired. Since organizations usually upgrade SQL Server less often than operating systems, older versions may be used for quite some time, especially if the applications accessing SQL don't use the features added to the new SQL versions. While Security Manager only tests the two most recent SQL versions at the time of release, there should be no issues using older or newer SQL versions as Security Manager uses basic calls into the SQL database that would be supported by virtually all SQL releases.

Backward and forward compatibility should be present, there just isn’t capacity to test the multitude of SQL versions offered over the years.

**Hardware Requirements**

See setup and install guide.

**VMware and Hypervisor Support**

See setup and install guide.

**Solutions**

When used with third party solutions or any print or management solution requiring access to the device, the Security Manager Base Policy template, or any template defined to meet the security standards for a company, might require changes to the security settings. See the solution documentation to determine whether policy changes are required to accommodate specific functionality. Care should be taken when creating policies as to not disrupt the operation of any solutions that may be installed on devices.

**NOTE:** Testing a small number of devices in a sandbox or test environment when solutions are present on devices is highly recommended before applying settings to a fleet as undesired behavior may occur with certain settings on certain solutions. Solutions may fail to install/operate, or potentially even worse behavior can occur on devices, when some settings are applied to devices with solutions present.

Security settings that have been known to affect either the installation or operation of solutions include:
- DNS server configured
- SNMP GET Community Name (Read Community Name) required for installation and configuration
- EWS password required for installation and configuration
- Command Load & Execute enabled
- PJL Access Commands enabled
- Remote Firmware Updates enabled
- Allow PJL Access enabled
- PJL Password not set
- Legacy Firmware Upgrades enabled (Current versions of firmware are signed with the SHA-256 hashing algorithm. Enabling this option allows installation of legacy firmware signed with the less secure SHA-1 algorithm)
- Control Panel Timeout

Please see the whitepaper titled “HP Security Manager - Policy Editor Settings” for more detailed information regarding settings for solutions.

## Network Port Assignments

This section lists the ports used by Security Manager.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client to Server</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7637 (version 3.0+)</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Port set during installation to be used to secure data between client and HPSM server via browser. This port may be changed to something else by editing bindings for the HPSM web site under IIS Manager. HPSM versions 3.0 and beyond.</td>
</tr>
<tr>
<td>8002 (version 2.1.5-)</td>
<td>TCP</td>
<td>WCF-NET.TCP</td>
<td>WCF with message encryption - port used from a remote client interface to the Security Center service. HPSM versions 2.1.5 and prior.</td>
</tr>
</tbody>
</table>

| **Server to Devices and cloud** |          |            |                                                                      |
| 80 and 8080 | TCP      | HTTP       | Port used for HTTP communication to devices only when SSL is not supported on the device. Also used to gather the latest firmware versions from the web if firmware assessments are enabled and configured to dynamically retrieve from web. |
| 443         | TCP      | HTTPS      | Port used for secure HTTP communication to devices, HTTP Web over SSL and to connect to the HP Cloud[11] |
| N/A         | ICMP     | PING       | Internet Control Message Protocol - port used to check if node is active. |
| 161         | UDP      | SNMP       | Simple Network Management Protocol - port used for many configuration items on devices as well as discovery of devices. |
| 7627        | TCP      | SOAP-HTTP  | Web service port used to manage communications on Futuresmart devices. |

| **Devices to Server** |          |            |                                                                      |
| 3329         | TCP      | HP Instant-On Security | Secure port (uses SSL) used from the device to the Security Manager service for Instant-On discovered devices. |

| **Server to SQL database** |          |            |                                                                      |
| 1433         | TCP      | MS SQL     | Standard DB Connection - port used from the Security Manager service to a remote SQL database with a default instance. Can be customized in a configuration file. |
| 1434         | UDP      | MS SQL Browser service | Standard connection to SQL browser service to retrieve the TCP port for the named SQL instance |
| dynamic      | TCP      | MS SQL     | Standard DB connection to a named SQL instance using dynamic ports |

| **Server to Email** |          |            |                                                                      |
| 25            | SMTP     | Simple Mail Transfer Protocol | Typical port used for communication to mail server if Automated Output feature is enabled. Port can be customized under File, Settings, Automated Output. |

| **Server to Certificate Authority** |          |            |                                                                      |
When configuring firewalls, an administrator can either open up ports used by the application (above table) or allow certain program executables access through the firewall. For the latter, Security Manager includes two separate services represented by three executables:

C:\Program Files (x86)\HP JetAdvantage Security Manager\HPSM_Service.exe
C:\Program Files (x86)\HP JetAdvantage Security Manager\HPQ.exe
C:\Program Files (x86)\HP JetAdvantage Security Manager\lmgrd.exe

1) The only time Security Manager could potentially traverse outside the company firewall for on-premises devices, is if “Check for Latest Firmware assessments” is enabled in a policy and Security Manager is instructed to dynamically pull the latest firmware list from the web (Firmware Index File Source set to Web). The Firmware Index File Source can also be configured so that a firmware index file can be uploaded into Security Manager (Firmware Index File Source set to file) rather than having Security Manager dynamically download the latest file from the web, if desired. The latter requires a user occasionally downloading the firmware index file separately from the web outside of Security Manager then importing the file into Security Manager.
Ports diagram

Lazerjet

OZ/FutureSmart devices

www.hp.com

Email server

SQL Server (remote)

CA Server

WIA server

HPSM Server

HPSM Service

Flexera service

HPSM Client

HPSM Client Incoming:
7037 TCP client communication of https

HPMSM outgoing for Lazerjet:
ICMP Ping (discovery process)
80 TCP (HTTP/WSS access)
161 UDP (SNMP)
443 TCP Web services communication for retrieving OVP details
7627 TCP Web services communication (FutureSmart devices only)
8888 TCP Services communication (OEM devices only)

HPSM incoming from Lazerjet:
3329 TCP Instant On

HPSM outgoing for cloud:
443 HTTPS, retrieve firmware versions, firmware vulnerabilities, information and service integrations

HPSM outgoing for email server:
25 SMTP, port is configurable

HPSM outgoing for Remote SQL:
1433 TCP default instance
1434 TCP MS SQL, Browser service for named instance & dynamic TCP port

ID Certificate Request:
3355 TCP DCOM/RPC
Randomly allocated TCP ports above 1024

Instant On forwarding:
3329 (default port) TCP

Note: DNS server is not added to this diagram, but a vital part for HPSM as well.
## Appendix A

### Release History

Version history of HP Security Manager releases

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 2.0.0     | Feb 2012     | • 76 HP Device Models Supported (See Supported Devices)  
• Instant-On Security  
• Intelligent Security Policy Editor  
• Background Security Compliance Monitoring |
| 2.0.5     | May 2012     | • Added support for HP LaserJet Enterprise 500 color MFP M575  
• Added support for HP LaserJet Enterprise 500 MFP M525  
• Added support for Microsoft SQL 2012 and Microsoft SQL 2012 Express |
| 2.0.7     | Nov 2012     | • Implemented Password Management Functionality  
• Enhanced Instant-On Security  
• Added support for Windows 8 & Windows Server 2012  
New devices supported:  
• HP LaserJet 700 M712  
• HP LaserJet color flow MFP M575  
• HP LaserJet flow MFP M525  
• HP LaserJet 700 color MFP M775  
• HP Jetdirect 640n and 695nw |
| 2.0.8     | April 2013   | • Device DNS alias resolve and discovery  
• Selectable SNMPv3/AES or SHA-1 credential/device communication  
New support for HP Officejet Pro devices:  
• 251dw printer  
• 276dw MFP  
• X451dw printer  
• X476dw MFP  
• X551dw printer  
• X576dw MFP  
New support for HP LaserJet Pro devices:  
• P2055 printer  
• 300 color MFP M375  
• 400 printer M401  
• 400 MFP M425  
• 400 color printer M451  
• 400 color MFP M475 |
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
|          |              | **500 MFP M521**  
|          |              | **500 color MFP M570**  
|          |              | **Additional HP LaserJet Enterprise support:**  
|          |              | **700 MFP M725**  |
| 2.0.9    | Nov 2013     | **New policy settings**  
|          |              | • Jetdirect NFC & Wireless Direct Print  
|          |              | • FIPS-140  
|          |              | • PJL Access Control  
|          |              | • Legacy Firmware Upgrade  
|          |              | **Enhanced policy settings**  
|          |              | • SNMPv3 (AES/SHA-1), Web Encryption Strength (TLS 1.1 & 1.2)  
|          |              | • Added Windows Authentication & LDAP support for Single Function Future Smart Devices  
|          |              | • Added the display of service connections to IPSC UI console.  
|          |              | **New device support:**  
|          |              | • HP LaserJet flow MFP M830  
|          |              | • HP LaserJet M806  
|          |              | • HP Color LaserJet flow MFP M880  
|          |              | • HP Color LaserJet M855  
|          |              | • HP Color LaserJet M750  
|          |              | • HP LaserJet MFP M435  
|          |              | • HP Jetdirect 2800w NFC/Wireless Direct Accessory  |
| 2.0.10   | April 2014   | **New device support:**  
|          |              | • HP Officejet Color MFP X585  
|          |              | • HP Officejet Color flow MFP X585  
|          |              | • HP Officejet Color X555  
|          |              | • HP Color LaserJet MFP M680  
|          |              | • HP Color LaserJet flow MFP M680  
|          |              | • HP Color LaserJet M651  
|          |              | • HP Color Laserjet MFP M476  
|          |              | • HP LaserJet M701/M706  |
| 2.1.0    | Nov 2014     | **New HP Device Support**  
| 2.1.0    | Nov 2014     | **New Fleet Certificate Management solution**  
|          |              | **Added/Updated Security Settings**  
|          |              | **Improved Reports**  
|          |              | **Data Export**  
<p>|          |              | <strong>TLS1.1/1.2 Communication</strong>  |</p>
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 2.1.1   | Mar 2015     | • Fixed mismatched region language settings issue  
• Unchecked SSL 3.0 by default in policy settings  
• Corrected error string for blank CSR  
• Adjusted timing reading certificate revocation list (CRL)  
• Solved mass SNMP Read/Write credential failures |
| 2.1.2   | Sep 2015     | • Complete rename to HP JetAdvantage Security Manager  
• Assessments on Limited Policy included by default  
• Automatic remediation summary output via email  
• Auto-Refresh of user interface during active tasks  
• Stored Data improvements  
• Group PINs - remediation  
• Enable Fax Receive policy item  
• Auto-discovery of devices  
• Multiple CA certificate management  
• Best Possible for CSR  
• Updated SQL Express to 2012 |

**New HP Device Support:**

- HP LaserJet Enterprise M604  
- HP LaserJet Enterprise M605  
- HP LaserJet Enterprise M606  
- HP Color LaserJet Pro M252  
- HP Color LaserJet Pro MFP M277  
- HP Color LaserJet Enterprise M552  
- HP Color LaserJet Enterprise M553  

- HP LaserJet M201  
- HP LaserJet M202  
- HP LaserJet MFP M225  
- HP LaserJet MFP M226  
- HP LaserJet MFP M630  
- HP LaserJet MFP flow M630  
- HP/TROY Device Support  

- HP Color LaserJet Pro MFP M477  
- HP Color LaserJet M452  
- HP LaserJet MFP M426  
- HP LaserJet M402  
- HP Color LaserJet MFP M577  
- HP Color LaserJet Flow MFP M577  

- HP LaserJet M527  
- HP LaserJet Flow MFP 527  
- HP LaserJet M506  
- HP Color LaserJet MFP M477  
- HP Color LaserJet M452  
- HP LaserJet MFP M426  
- HP LaserJet M402  
- HP Color LaserJet MFP M577  
- HP Color LaserJet Flow MFP M577
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 2.1.4   | Feb 2016     | - Improved credential management including global credential store  
|         |              | - Firmware assessments  
|         |              | - Assessment on new security features (Secure Boot, Intrusion Detection, Whitelisting)  
|         |              | - Ability to enter greater than 8 MB for Max Attach Size under E-mail settings  
|         |              | - Upgrade improvements when using a remote SQL database  
|         |              | - HP LaserJet M400 series devices now allow SNMPv3 remediation  
|         |              | - Fixed cases where Instant On discovered devices are not remediating  
|         |              | - Fixed cases where tasks are hanging and never completing  
|         |              | - Max Attach Size under E-mail settings no longer reports failure on assess when values match  
|         |              | - Security Manager no longer crashes when attempting to upload CA cert without a particular value present  
|         |              | - HP Color LaserJet M476 no longer claims Not Supported  
|         |              | - Auto-refresh is now turned off by default  
|         |              | - Updated bundled SQL to Microsoft SQL Server Express 2014  

**New HP Device Support**

- HP LaserJet Pro M501  
- HP Color LaserJet Pro MFP M377  
- HP PageWide Color 556  
- HP PageWide Color MFP M586  
- HP PageWide Color Flow MFP M586  
- HP PageWide Pro 452  
- HP PageWide Pro MFP 477  
- HP PageWide Pro 552  
- HP PageWide Pro MFP 577  
- HP PageWide XL 4500  
- HP PageWide XL 5000  
- HP PageWide XL 8000  
- HP DesignJet T1120 44In  
- HP DesignJet T1500/Postscript  
- HP DesignJet T2300/Postscript  
- HP DesignJet T2500/Postscript  
- HP DesignJet T770  
- HP DesignJet T790 44In  
- HP DesignJet T790PS 24In  
- HP DesignJet T790PS 44In  
- HP DesignJet T920/Postscript  
- HP DesignJet T1300  
- HP DesignJet T1300/Postscript  
- HP Designjet T3500  
- HP Designjet Z5400
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.5</td>
<td>June 2016</td>
<td><strong>New Policy Items</strong>&lt;br&gt;- Verify Certificate for IPP/IPPS Pull Printing&lt;br&gt;- Enable WINS Port&lt;br&gt;- WINS Registration&lt;br&gt;- Secure Disk Password&lt;br&gt;&lt;br&gt;<strong>Changes to Policy Items</strong>&lt;br&gt;- Subject Alternate Names (SANs) added to Identity certificates.&lt;br&gt;- 802.1x remediation&lt;br&gt;- Bootloader Password remediation&lt;br&gt;- Ability to remediate SSL 3.0&lt;br&gt;- Maximum Attachment Size for SMTP E-mail settings can be remediated to any custom value between (0-999).&lt;br&gt;- EWS Password Account Lockout settings&lt;br&gt;- Certificate Management of Pro devices&lt;br&gt;- Installed solutions can now set &quot;Local&quot; for many of the Authentication Manager settings&lt;br&gt;- Reports include Device Model column instead of Device Name for consistency across products&lt;br&gt;- Assessments reports now include an Export Data tab to export to .csv or .xml file on the fleet&lt;br&gt;- Serial number no longer has to be upper case for Instant On filtering&lt;br&gt;- The checkbox to E-mail results for remediation task now saves correctly in UI when editing task&lt;br&gt;- dbo_DeviceTable now removes records during nightly cleanup when device is deleted&lt;br&gt;- Database is no longer locked to a specific Security Manager server allowing for much easier failover techniques on the Security Manager server&lt;br&gt;&lt;br&gt;<strong>New HP Device Support</strong>&lt;br&gt;- HP LaserJet Pro M203&lt;br&gt;- HP LaserJet Pro MFP M227</td>
</tr>
<tr>
<td>3.0</td>
<td>April 2017</td>
<td>• Browser-based user interface&lt;br&gt;• Dashboard indicating status of fleet compliance&lt;br&gt;• Ability to login as guest or admin role&lt;br&gt;• Logging of user and service activity in syslog format for integration into SIEM tools&lt;br&gt;• Support for Symantec Certificate Authority&lt;br&gt;• Addition of User Principal Name (UPN) as Subject Alternate Name (SAN) in identity certificate to support Active Directory User accounts authentication onto 802.1x networks&lt;br&gt;• New policy items:&lt;br&gt;  a) Service Access Code&lt;br&gt;  b) Wi-Fi Direct</td>
</tr>
<tr>
<td>Version</td>
<td>Release Date</td>
<td>Features</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
|         |              | • Password Complexity joined the existing Account Lockout features for several credential types  
|         |              | • Firmware Downgrade  
|         |              | • Improvements to Authentication Manager policy configuration to support additional solutions as sign-in method  |

**Fixes:**

- PJL Password now supported for LJ 5200  
- Fixed two very unique possible causes for task hangs  

**New HP Device Support**

- HP Color LaserJet Enterprise M652  
- HP Color LaserJet Enterprise M653  
- HP Color LaserJet Enterprise MFP M681  
- HP Color LaserJet Enterprise MFP M682  
- HP Color LaserJet MFP E77822  
- HP Color LaserJet Flow MFP E77822  
- HP Color LaserJet MFP E77825  
- HP Color LaserJet Flow MFP E77825  
- HP Color LaserJet MFP E77830  
- HP Color LaserJet Flow MFP E77830  
- HP Color LaserJet MFP E87640  
- HP Color LaserJet Flow MFP E87640  
- HP Color LaserJet MFP E87650  
- HP Color LaserJet Flow MFP E87650  
- HP Color LaserJet MFP E87660  
- HP Color LaserJet Flow MFP E87660  
- HP LaserJet Enterprise M607  
- HP LaserJet Enterprise M608  
- HP LaserJet Enterprise M609  
- HP LaserJet Enterprise MFP M631  
- HP LaserJet Enterprise Flow MFP M631  
- HP LaserJet Enterprise MFP M632  
- HP LaserJet Enterprise Flow MFP M632  
- HP LaserJet Enterprise MFP M633  
- HP LaserJet Enterprise Flow MFP M633  
- HP LaserJet MFP E72525  
- HP LaserJet Flow MFP E72525  
- HP LaserJet MFP E72530  
- HP LaserJet Flow MFP E72530  
- HP LaserJet MFP E72535  
- HP LaserJet Flow MFP E72535  
- HP LaserJet MFP E82540  
- HP LaserJet Flow MFP E82540  
- HP LaserJet MFP E82550  
- HP LaserJet Flow MFP E82550  
- HP LaserJet MFP E82560  
- HP LaserJet Flow MFP E82560  
- HP PageWide Pro 750  
- HP PageWide Pro 755
## Version 3.0.1
### Release Date: July 2017
- Addressed Cross Site Scripting and AngularJS vulnerabilities found during penetration testing with the new web user interface.
- Switched to using a new library to perform HTTP operations on devices to eliminate potential task hangs on some servers that rejected the old MSHTML library.

## Version 3.1
### Release Date: December 2017
**New features**
- Scheduled reports to file or email
- Autogrouping
- Support for OpenTrust Certificate Authority
- Addition of System Name as Subject Alternate Name (SAN) in identity certificate
- SQL database scripts included during install
- Support for Secure by Default initiative on new 24.5 firmware

**New policy items:**
- Web Scan and Secure Web Scan
- Individual cipher suites under Web Encryption Settings
- Role Based Access Control
- Add Roles to User or Group
- EWS Roles under Authentication Manager
- HP Connection Inspector
- Cross Site Request Forgery (CSRF) Prevention
- IPSEC/Firewall
- 802.1x (wireless)

**Fixes:**
- Global credentials working properly
- Incorrect passwords stored in database remain in database if unsuccessful
- Time zone difference between client and server allows for running tasks immediately if desired
- Time zone displayed in proper 24-hour format if desired
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Features</strong></td>
</tr>
</tbody>
</table>
|         |              | • CA certificates are now deleted if checkbox is checked to remove certificates not in policy  
|         |              | • CA certificates are now successfully installed on devices set to non-English language  |
| 3.1.1   | March 2018   | • Fixed issue with Admin (EWS) Password always remediating even if matching policy  
|         |              | • Fixed SQL scripts included in HPSM folder  |
| 3.2     | July 2018    | **Features** |
|         |              | • Instant on Reflection  
|         |              | • Mac Address as column  
|         |              | • Firmware assessment added to Essential policy  
|         |              | • Changed label of Limited policy to Essential policy  
|         |              | • Default licenses increased from quantity 20 to 50  |

**New HP Device Support**

- HP Color LaserJet M254
- HP Color LaserJet MFP M281
- HP Color LaserJet E65050
- HP Color LaserJet E65060
- HP Color LaserJet E67550
- HP Color LaserJet E67560
- HP LaserJet E60055
- HP LaserJet E60065
- HP LaserJet E60075
- HP LaserJet MFP E62555
- HP LaserJet MFP E62565
- HP LaserJet MFP E62575
- HP LaserJet MFP E72545
- HP LaserJet Flow MFP E72545
- HP PageWide Enterprise Color 765dn
- HP PageWide Enterprise Color MFP 780
- HP PageWide Enterprise Color Flow MFP 785
- HP PageWide Color E55650
- HP PageWide Color MFP E58650
- HP PageWide Managed Color E75160
- HP PageWide Managed Color MFP E77650
- HP PageWide Managed Color MFP E77660
- HP PageWide P55250
- HP PageWide MFP P77740
- HP PageWide MFP P77750
- HP PageWide MFP P77760
- HP PageWide MFP P57750
- HP DesignJet T830 24-in MFP
- HP DesignJet T1700dr PostScript
- HP Digital Sender Flow 8500
- HP ScanJet Flow N9120 fn2
- Zebra ZTC ZT410-203dpi ZPL
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>New Policy Items:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CIFS (Shared Folder)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP Client</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• FTP Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• JetAdvantage Link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Extended Signature Verification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Control Panel Logout Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Fixes:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Order of operation causing Network Connection Error or Credentials Failed status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Autogroups limited to 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Autogroup filter for Hostname cannot be blank</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disk Encryption Status claims failed for SSD/eMMC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File Erase Mode fails when no disk is present</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Incorrect hover help for Certificate Authority Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can't install an intermediate CA cert on older devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Duplicate ID certificates installed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can't add IP Addresses to ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Installer uses ODBC to connect to SQL on third option for Connect to Existing DB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device replacing another at same IP Address does not update all attributes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secure Boot Presence fails for devices that don't support feature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SNMPv3 queries when v3 is disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>New Device Support</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide Managed Color P75250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide Managed Color MFP P77440</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet MFP E50045n</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet MFP E52545dn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Flow MFP E52545c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet MFP E55040dn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet MFP E57540dn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet Flow MFP E57540c</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Designjet T3500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Designjet Z5600</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Samsung Multifunction MultiXpress K7400, K7500, K7600, K7650, K703, K705, K706</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Samsung Multifunction MultiXpress X7400, X7500, X7600, X703, X704, X705, X706</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Samsung Multifunction ProXpress M4580, M4583</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Samsung Multifunction MultiXpress M4370, M5370, M5270</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Samsung Multifunction MultiXpress X4220, X4250, X4300, X400, X401, K4250, K4300, K4350, K401, K400</td>
</tr>
<tr>
<td>Version</td>
<td>Release Date</td>
<td>Features</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 3.2.1   | December 2018| **Features:**  
  - Firmware version is now an autogrouping filter.  
  - Added option to display Error if an assessment could not be performed instead of remaining at Passed assessment status from the last successful assessment. The Email Summary Remediation report now indicates the device was not remediaged.  
  - More than one range can be entered for a single IP Range discovery.  
  - Discoveries can now be scheduled to occur at some desired frequency.  
  - Added option to properly assess PJL Password if PJL Access is disabled by temporarily enabling PJL Access.  
  - Added support for Active Directory authentication to be used to remotely manage devices instead of Admin (EWS) Password.  
  - A new option is available to limit Assessment & Remediation history stored in the database to some desired amount of days.  
  - New Repetitive Remediation report includes devices being remediaged for the same items multiple times.  
  - Added support for Zebra devices with Link OS > =5.0  
  - HP SM support for CSRF with JEDI FS3 firmware  
  - Admin password policy item support for Zebra devices  
  - Added Fax Receive Owner option (Drop down values as Guest, Administrator, Network User) under Fax Receive Policy Item.  

**New Policy Items:**  
- SIP Server Settings (FOIP Support)  
- Postscript Security  
- Wireless Radio State  
- Information Hiding  

**Fixes:**  
- Vulnerabilities in Bootstrap library and AngularJS library resolved by patching code fixes from new versions.  
- Installation no longer fails with Create a New or Upgrade Existing DB option while upgrading after database scripts have already been used to upgrade database.  
- Write verification failed is no longer displayed while remediaging FTP firmware Update policy on some devices.  
- CA certificate now remediages on a CLJ CM4730mfp when server localization is non-English.  
- Invalid Identity Certificate is no longer observed in device status on verifying a device after remediagion of an identity certificate.  
- SNMP Read/write Community Name is now attempted in global credentials if public is enabled for SNMP Reads on the device.
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Duplicate identity certificates are no longer installed if an assessment finds a mismatch in the ID certificate. Certificate is replaced instead of appended.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CA certificate displays Issued To name instead of Issued By name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed CA certificates issue on older devices requiring checkbox to allow intermediate certs. Root and intermediate certificates now install successfully.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Web Encryption Strength no longer fails on older devices that don’t support individual ciphers if a Read Community Name is present on the device and public is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed ID certificates issue where SANs are assessed incorrectly, and a new certificate is always installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Secure Boot Presence / Whitelisting / Intrusion Detection now correctly indicate Not Supported for models that do not support them and no longer fail in reports when Ignore is selected or unsupported devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed ID certificates issue where Common Name not Formed in CSR is displayed when the CA is set to manually approve requests instead of automatically generating certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed issue where PJL Password was not being pulled from the Global Credential Store during assessments/remediations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Jetdirect XML Services now assesses properly on some older Jetdirect nics.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added certificate management support for T1700 DesignJet Device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the issue where secure by default in FS 4.5 was breaking instant on remediation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed model name sorting issue on older devices that display with lower case.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Resolved the issue with downgrade for HPSM where a lower version was allowed to be installed on a higher version.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the behavior with Send FAX Policy. Now this policy can be enabled/disabled in Policy Editor UI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the SAN behavior for non-unified devices where FQDN was not displayed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the issue where Zebra devices were not getting discovered using auto-discovery IP range option.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the behavior where a not reachable device was showing as “credential failed”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the behavior where PJL password was not remediating on multiple older devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed FTP Firmware update behavior on LJ M631.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the issue with CLJ CP4520 where SNMPv3 was not remediating before.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the certificate behavior on CLJ 3600 and LJ 300 M375 devices. Now CA and ID certificate shows as not supported.</td>
</tr>
<tr>
<td>Version</td>
<td>Release Date</td>
<td>Features</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>New Device Support</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide Color MFP 779</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide Color MFP 775</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide Color MFP 751</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet M653</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet MFP M681</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet MFP M609</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet MFP M633</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Zebra ZQ320</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Zebra ZQ620</td>
</tr>
</tbody>
</table>

**Note:** With 3.2.1 release all Zebra devices with Link OS >=5.0 are supported. So any devices listed below with required Link OS may work as expected.

- Zebra QLn220
- Zebra QLn320
- Zebra ZQ310
- Zebra ZQ510
- Zebra ZD410
- Zebra ZD420
- Zebra ZD500R
- Zebra ZT230 200dpi
- Zebra ZT610 203dpi

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3</td>
<td>Aug 2019</td>
<td><strong>Features:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stop automatically allowing members of local admin group to launch HPSM-100122</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Manager should automatically remediate ID certificates which are revoked/deleted-103278</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HPSM shall preserve few settings during upgrade-103973</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HPSM still referring to .NET 3.51 during installation-104487</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security Manager compliance with FIPS 140 standards-103003</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Improve Syslog effectiveness - are we capturing the right events? 100923</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support Analyst role in Security Manager-103256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HPSM needs to compare asset name from firm service against glf entry for firmware upgrade-82285</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for Windows server 2019-104924</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Advanced error handling on DB connectivity and update-101995</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Changes to Essential and Base policy items - review from PSAS team-104773</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Some of the RBAC menus in EWS is missing in Locksmith-104599</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Better refresh behavior for devices with new hostname-87705</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accessibility: TAA Compliant RAM Disk-94288</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Epic]Secure loading and access restriction in certificate management plugins-103991</td>
</tr>
<tr>
<td>Version</td>
<td>Release Date</td>
<td>Features</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [EPIC]- Security Shield Dashboard in HP SM-102887</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Localize Newly added Chinese text in 3.2-104852</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proper backup &amp; restore of data during installation-104685</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• French language for HPSM-104950</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SQL 2017 support with Level 140 support in Security Manager-105218</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added UPN field to ID cert Policy (Based on the string value the UPN will be generated)-104689</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fixed the behavior for Disk encryption policy when the device has the disk present but can’t be encrypted-105087</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support for configurable alerts based on the security posture of devices over a period-103130/106168</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Policy for Email settings does not support device-individual from: addresses-104871</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [EPIC][Reports] Executive Fleet Assessment Report-103129</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Localization] Add support for new German language-105983</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Epic] FW Assessment against known vulnerabilities (Shell's)-94289</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Improving Auto Group filter deficiencies-106062</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 106281: [Installation][Usability] Provide option to enter custom name as database name during installation/upgrade</td>
</tr>
</tbody>
</table>

**New Policy Items:**
RAM Disk Configuration

**Fixes:**

- Policy Items Assessed report has incorrect numbers-100976.
- SNMPv3 credential store UI only supporting up to 23 characters-104690
- PDF report download not working in latest chrome version-104883
- Count mismatch between policy items and assessed items-104085
- ID cert remediation on a few Pro devices fails with 409 conflict error-104593
- SNMPv1/v2 Read and Read/Write Community Names limited to 20 characters in UI-104879
- Remediating ID certificate every time on German OS server-104688
- 3.2.1 broke ability to enable GCM ciphers and TLS 1.0/1.1 in same policy-104884
- Upgradation issue with RBAC changes and RBAC Policy is not getting saved with latest release version Policy item selected -105366
- Network services policy state becomes invalid without any changes/validation-105209
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
|         |              | • Installation is getting terminated if dot net 3.5 is not installed while installing HPSM with SQL 2014-105553  
|         |              | • SnmpV3 fails to set when best possible encryption algorithm is applied on the device-105483  
|         |              | • "Write verification failed...." error message observed when performing CA certificate, A&R task on Pro devices-104661  
|         |              | • P3005 and J7979 JDI need to tag IPPS as Not Supported-105159  
|         |              | • Configuring FS4 Contacts using Security Manager results in an EWS error message-104874  
|         |              | • [HPSM 3.3][Installation]: Installation is getting terminated if .net 3.5 is not installed & user tries to install SQL2014 from HP5M-106007  
|         |              | • Web Encryption Strength not working for OfficeJet X476 and X576-106026  
|         |              | • CA certs fail to install on M401/402 in different language-106589  
|         |              | • LJ 4050 and LJ 4100 should be tagged as Not Supported for latest firmware policy item-106674  
|         |              | • deleting a task should kill all open tasks-104451  
|         |              | • can't remediate 802.1x on Pro and Oz devices-106510  
|         |              | • LJ P3015 should tag File Erase Mode as Not Supported  
|         |              | • Remote Configuration Password broken for LJ M630-106821  
|         |              | • not adding 802.1x name to SANs in ID certificate-106771  
| 3.4.0.16986 | Dec'19     | • not installing CA certs intermittently on Oz devices-106282  
|         |              | • not deleting CA certs on non-unified devices when checkbox to delete is checked-106118  
|         |              | **New Device Support:**  
|         |              | • HP LaserJet MFP M528  
|         |              | • HP LaserJet M507  
|         |              | • HP LaserJet MFP E82560  
|         |              | • HP Color Laserjet MFP E87640  
|         |              | • HP Color LaserJet FlowMFP M776  
|         |              | • HP Color LaserJet M856  
|         |              | • HP Color laserjet MFP E77422  
|         |              | • HP laserjet MFP E72425  
|         |              | • HP DesignJet XL 3600 MFP  
|         |              | • HP DesignJet T2600dr MFP  
|         |              | • HP Color LaserJet Pro MFP M479fdw  
|         |              | • HP Color LaserJet Pro M454dn  
|         |              | • HP LaserJet Pro M404dn/dw  
|         |              | • HP LaserJet Pro MFP M428fdn  
|         |              | • Support Edit of Discovery task in Security Manager  
|         |              | • Licensing Improvement  
|         |              | • HPSM Database Improvement  
|         |              | **Features**
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
|         |              | - Remediate LDAP and SMTP credentials  
|         |              | - Firmware Assessment Usability Improvements  
|         |              | - Autogrouping to automatically remediate policies assigned to group  
|         |              | - SCEP standard connector support in Certificate Management 
|         |              | - Firmware Assessment Improvement 
|         |              | - NTP server/Time Sync for the print fleet 
|         |              | - Security Manager should support Pull Print under RBAC  
|         |              | - Policy change notification feature in Security Manager  
|         |              | - Term SKUs support in HP Security Manager - license expiry warning  

**New Policy Items:**
- Network Server Sync

**Fixes:**
- Incorrect response from HPSM to Instant On packets  
- Device Announcement Agent shows error in recommendations when IP Address field is blank  
- Device status is changed to error state when A & R task is executed with HTTPS enable policy item on Samsung device  
- Unable to remediate 802.1x setting values when applied policy with no password with PEAP enabled settings  
- Selected policy items are getting unselected post upgrade  
- Bootloader Password broken in 3.3, can't remediate if device has existing password  
- Unable to launch HPSM when installed in French OS  
- Renewal Threshold in ID Cert policy doesn't allow value above 365  
- Admin (EWS) Password minimum password length does not allow 0 value  
- unlicensed device reverts to licensed after discovery  
- Auth Manager breaks Pull Print on device  
- Jedi devices claim unexpected value or type when remediating job held timeout  
- CA Certificates should replace the JD Certificate Store Certificate for Non-Unified Devices  
- Disk Encryption Status reporting failed on non-encryptable disks on Oz devices  
- PJL Password config entry to temporarily enable PJL Access needs to apply for remediations too

**New Device Support:**
- HP LaserJet M608  
- HP LaserJet MFP M635
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0.19036</td>
<td>Dec ‘20</td>
<td><strong>Features</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for Microsoft Edge (Chromium) browser</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bundled with SQL Express 2019</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Additional Ciphers have been added to the policy item Web Encryption Settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add configuration option for timeout of direct SQL commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added support for license with different end-dates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Add support for variable data for the Return E-mail address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Zebra Certificate Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enhanced Dashboard with support for Device level assessment and remediation history and alerts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• [Firmware Assessment-File/HPWeb] Use Asset Identifier to match firmware detail entries from glf file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Several performance improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HPSM installer now asks for credentials before creating/updating the Database.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TLS 1.2 support in HPSM Installer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maintenance Task Improvements.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All HPSM services can now run as a local user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Certificate Management Plug-in Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added localization into Malay and Spanish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added option to disable SMBv1, v2, v3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added EST (Enroll over secure transport) ID certificate support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HPSM integration with Qualys.</td>
</tr>
</tbody>
</table>

**New Policy Items**

- E-mail Domain Restriction

**Updated Policy Names:**

- JA Link -> HP work path
- Digital send -> Job Behavior
- Web Encryption Settings -> Web Encryption Settings or Active Ciphers
- System Logging > Syslog (System logging)
- CCC Logging > Enhanced (security event) logging
- CIFS (Shared Folder) > SMB/CIFS(Shared Folder)

**Fixes**

- Officejet x576 no longer fails in assessment for CP Lock when moderate is selected
- LJ M404 (with latest firmware) can now remediate settings requiring SNMP in same remediation as enabling v3.
- When applying an SNMP v3 only policy HPSM no longer indicates unable to remediate with SNMPv1 credential error when the device is only configured with SNMPv3 only.
- HPSM is now accepting an email address which contains a plus sign (+).
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 3.6.0.20307 | July 2021 | - Added configuration option `AssessOnlyNewDevice` in HPSM_service.exe.config  
- Added configuration option `AllowRepetitiveInstantOnPolicyAfter` in HPSM_service.exe.config  
- Added configuration option `alwaysUseLastAppliedPolicyForInstantOn` |

### New Device Support
- HP Color LaserJet Enterprise M554  
- HP Color LaserJet Enterprise M555  
- HP Color LaserJet Enterprise MFP M578  
- HP DesignJet T650 24-in

### Managed devices:
- HP Color LaserJet Managed MFP E77428  
- HP LaserJet Managed MFP E72535  
- HP LaserJet Managed MFP E72430

- HPSM is no longer hanging on Export page when you enter long, or invalid email address and CPU is not going to 100%.  
- When running the installDBrmt.bat script for a remote database it no longer adds rights for network service.  
- The JetDServerCert (servcert.pfx) has been renewed  
- Assessment of EWS password is no longer taken ~ 10 minutes when snmp access is set to read-only.  
- Credentials no longer failing with M401 over SNMPv3 with SNMPv1 read enabled.  
- The term Alerts has been changed into Alert Subscriptions.  
- M404-M405 Series and M454 Series expose 'Retain Print Job' also w/o Flash Drive and no longer cause invalid remediations results (when latest device firmware is used)  
- syslogging can now be disabled when enhanced security event logging is enabled on the device  
- ID certificate on Z9 can now be installed when CSR Source is set to HPSM.  
- No longer hanging tasks  
- Instant on is now also using global credentials.  
- No longer intermittent database Stale Errors with default setting for Delect Rule to No Action for foreignkey FK9B4CDE5E7E9133 for RecToReasonsTable.  
- HPSM can now remediate the setting Retain Print Jobs after Reboot when set to disabled on policy and enabled on the device.  
- Manual discovery will not perform a hostname resolution, when host-name resolution has been disabled  
- ID certificate installation no longer failing with Venafi SCEP service.  
- Added missing sign-In Methods for new HPAC versions in HPSM.
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
</table>
|         |              | • Added support for Flexworker devices  
|         |              | • Added IPv6 support. HPSM can now discover and manage devices over IPv6  
|         |              | • Added option to extract Database scripts in a user specified location when running the HPSM installer.  
|         |              | • Instant on messages will now also be logged in a separate log file called InstantOn.log.  
|         |              | • HPSM now only update Credential status in UI after all credential attempts have been completed (device, global and default). |

**New Policy Items**

- Added new ECDHE Ciphers support in the policy setting Web Encryption Settings or Active Ciphers
- Added Syslog Protocol option in the syslog policy setting

**Fixes**

- Nightly maintenance task is no longer failing due to too many parameters
- HPSM can now remediate SNMPv3 settings with a policy which disabled SNMPv1, enables SNMPv3 with a non-complex passphrase, while the device was enforcing strong encryption for SNMPv3 before the policy was applied
- HPSM can now install ID certificate with HPSM on T790 and T1300 which have an HP JetDirect 640N.
- The manual maintenance script and nightly maintenance are now making the recommendations table smaller.
- The timeout for communication over port 7627 is now configurable with configuration option `httpTimeout` in EapNetworkLib.dll.config.
- Unable to contact licensing service and "Failed to retrieve data while loading HPSM"  
All these licensing issues have been resolved by removing the HP Print License Service.  
The Flexera.log is now available under:  
C:\Program Files (x86)\HP JetAdvantage Security Manager\log
The license files are now available under:  
C:\ProgramData\HP\HPSM\LicenseFiles
Instead of a registry key for HPQ_LICENSE_FILE, a system variable is created for this variable during HPSM installation.
- Handle Inconclusive credential status by adding a new device status: “Credentials not Validated or Incorrect” and add Credential retries into the logs.
- When a device is deleted from HPSM, it’s corresponding serial number for instant on authentication is no longer deleted
- Remediation report was showing that EWS password was not set and Allow PJL/PS access settings had been remediated, while in reality no settings had been changed
<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>on the device and the EWS password was set on the device. Instead of showing EWS “<strong>Password Not Set</strong>” and “<strong>ERROR</strong>” for other settings like PJL/PS password, HPSM will now display in the remediation report “<strong>Error while retrieving value from the device</strong>” when the device can temporarily not answer correctly web services questions from HPSM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When using firmware security service HPSM is no longer reporting for some devices medium risk when firmware is up-to-date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• During the nightly maintenance a Qualys maintenance error will no longer occur</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device discovery now also starts when the FQDN starts with a number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Discovery now also starts when DNS entry contains an underscore for the corresponding device</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>New Device Support</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet Enterprise M455</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet Enterprise MFP M480</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Enterprise M406</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Enterprise MFP M430</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Enterprise MFP M431</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet M110we</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet M140we</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet M209dwe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet M234sdne</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet M407</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet MFP M139w</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP PageWide XL 4200 MFP series</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Managed devices:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet Managed E45028</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP Color LaserJet Managed MFP E47528</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Managed E40040</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• HP LaserJet Managed MFP E42540</td>
</tr>
</tbody>
</table>
Appendix B

Other HP Security Manager Whitepapers and Manuals

Many support manuals and whitepapers are available for HP Security Manager. To view them, go to the HP Security Manager Support page and click Manuals. The following list of documents is available at this location:

- Instant-On Security and Auto-Group Remediation (white paper)
- Automatic Email notification for remediation tasks and policy changes (white paper)
- Certificate management (white paper)
- Credential management (white paper)
- Discover Devices, Determine Device Details, and Export Devices (whitepaper)
- Frequently Asked Questions
- Instant-On Security and Auto Group Remediation (whitepaper)
- Installation and Setup Guide
- Manage devices running HP FutureSmart 4.5 firmware (whitepaper)
- Policy Editor Settings including supported devices feature table (white paper)
- Release Notes including Port information (white paper)
- Reporting, Email Alert Subscriptions & Remediation Summary, Auditing & Syslog Functionality, and Understanding Exported Device Data (white paper)
- Securing the HP Security Manager (white paper)
- Sizing and Performance (white paper)
- Supported devices (white paper)
- Troubleshooting issues (white paper)
- User Guide
- Using licenses and troubleshooting licensing issues (white paper)
- Using Microsoft® SQL Server (white paper)

Also available on the HP Security Manager Support page under the Product Information section is the following information:

- Supported device features matrix (.xls)

© Copyright 2021 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Rev.39, Sept 2021