# HP JETADVANTAGE SECURITY MANAGER

## Release Notes v3.0.1

## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Version Information</td>
<td>2</td>
</tr>
<tr>
<td>What’s New in Security Manager 3.0/3.0.1?</td>
<td>7</td>
</tr>
<tr>
<td>Software Notes and Known Issues:</td>
<td>8</td>
</tr>
<tr>
<td>Key Features</td>
<td>9</td>
</tr>
<tr>
<td>Solutions</td>
<td>9</td>
</tr>
<tr>
<td>Supported Operating Systems and Databases</td>
<td>10</td>
</tr>
<tr>
<td>Hardware Requirements</td>
<td>11</td>
</tr>
<tr>
<td>NOTES</td>
<td>11</td>
</tr>
<tr>
<td>VMware Support</td>
<td>11</td>
</tr>
<tr>
<td>Installation</td>
<td>12</td>
</tr>
<tr>
<td>Installation Notes:</td>
<td>12</td>
</tr>
<tr>
<td>Network Port Assignments</td>
<td>13</td>
</tr>
</tbody>
</table>
OVERVIEW

Announcing HP JetAdvantage Security Manager 3.0/3.0.1, 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.

VERSION INFORMATION

Version history of HP JetAdvantage Security Manager releases:

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.0</td>
<td>Feb 2012</td>
<td>76 HP Device Models Supported (See Supported Devices)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Instant-On Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intelligent Security Policy Editor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Background Security Compliance Monitoring</td>
</tr>
<tr>
<td>2.0.5</td>
<td>May 2012</td>
<td>Added support for HP LaserJet Enterprise 500 color MFP M575</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for HP LaserJet Enterprise 500 MFP M525</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for Microsoft SQL 2012 and Microsoft SQL 2012 Express</td>
</tr>
<tr>
<td>2.0.7</td>
<td>Nov 2012</td>
<td>Implemented Password Management Functionality</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced Instant-On Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for operating systems:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 8 &amp; Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added support for devices &amp; accessories:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HP LaserJet 700 M712</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HP LaserJet color flow MFP M575</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HP LaserJet flow MFP M525</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Changes</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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  
  - 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 for:  
  - 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 | - Added FIPS-140 support for JetDirect Print Server cards  
- Added MS Server 2012 R2 and Windows 8.1 OS support  
- New device support for:  
  - 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 |
<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
</table>
| 2.1.0   | Nov 2014   | - New Fleet Certificate Management solution  
- Added/Updated Security Settings  
- Improved Reports  
- Data Export  
- TLS1.1/1.2 Communication  
- New HP Device Support:  
  - 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 |
| 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  
- New HP Device Support:  
  - LaserJet Enterprise M604  
  - LaserJet Enterprise M605  
  - LaserJet Enterprise M606  
  - Color LaserJet Pro M252  
  - Color LaserJet Pro MFP M277  
  - Color LaserJet Enterprise M552  
  - Color LaserJet Enterprise M553 |
| 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 MFP 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 |
| 2.1.4   | Feb 2016   | - Improved credential management including global credential store  
- Firmware assessments  
- Assessment on new security features (Secure Boot, Intrusion Detection, Whitelisting) |
<table>
<thead>
<tr>
<th>Changes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to enter greater than 8 MB for Max Attach Size under E-mail settings</td>
<td></td>
</tr>
<tr>
<td>Upgrade improvements when using a remote SQL database</td>
<td></td>
</tr>
<tr>
<td>HP LaserJet M400 series devices now allow SNMPv3 remediation</td>
<td></td>
</tr>
<tr>
<td>Fixed cases where Instant On discovered devices are not remediating</td>
<td></td>
</tr>
<tr>
<td>Fixed cases where tasks are hanging and never completing</td>
<td></td>
</tr>
<tr>
<td>Max Attach Size under E-mail settings no longer reports failure on assess when values match</td>
<td></td>
</tr>
<tr>
<td>Security Manager no longer crashes when attempting to upload CA cert without a particular value present</td>
<td></td>
</tr>
<tr>
<td>HP Color LaserJet M476 no longer claims Not Supported</td>
<td></td>
</tr>
<tr>
<td>Auto-refresh is now turned off by default</td>
<td></td>
</tr>
<tr>
<td>Updated bundled SQL to Microsoft SQL Server Express 2014</td>
<td></td>
</tr>
<tr>
<td>New HP Device Support</td>
<td></td>
</tr>
<tr>
<td>HP LaserJet Pro M501</td>
<td></td>
</tr>
<tr>
<td>HP Color LaserJet Pro MFP M377</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Color 556</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Color MFP M586</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Color Flow MFP M586</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Pro 452</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Pro MFP 477</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Pro 552</td>
<td></td>
</tr>
<tr>
<td>HP PageWide Pro MFP 577</td>
<td></td>
</tr>
<tr>
<td>HP Pagewide XL 4500</td>
<td></td>
</tr>
<tr>
<td>HP Pagewide XL 5000</td>
<td></td>
</tr>
<tr>
<td>HP Pagewide XL 8000</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T1120 44In</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T1500/Postscript</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T2300/Postscript</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T2500/Postscript</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T770</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T790 44In</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T790PS 24In</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T790PS 44In</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T920/Postscript</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T1300</td>
<td></td>
</tr>
<tr>
<td>HP DesignJet T1300/Postscript</td>
<td></td>
</tr>
<tr>
<td>HP Designjet T3500</td>
<td></td>
</tr>
<tr>
<td>HP Designjet Z5400</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New Policy Items</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Certificate for IPP/IPPS Pull Printing</td>
<td></td>
</tr>
<tr>
<td>Enable WINS Port</td>
<td></td>
</tr>
<tr>
<td>WINS Registration</td>
<td></td>
</tr>
<tr>
<td>Secure Disk Password</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Changes to Policy Items</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Alternate Names (SANs) added to Identity certificates.</td>
<td></td>
</tr>
<tr>
<td>802.1x remediation</td>
<td></td>
</tr>
<tr>
<td>Bootloader Password remediation</td>
<td></td>
</tr>
<tr>
<td>Ability to remediate SSL 3.0</td>
<td></td>
</tr>
<tr>
<td>Maximum Attachment Size for SMTP E-mail settings can be remediated to any custom value between (0-999).</td>
<td></td>
</tr>
<tr>
<td>EWS Password Account Lockout settings</td>
<td></td>
</tr>
<tr>
<td>Certificate Management of Pro devices</td>
<td></td>
</tr>
</tbody>
</table>
| 3.0 April 2017 | Browser-based user interface  
| | Dashboard indicating status of fleet compliance  
| | Ability to login as guest or admin role  
| | Logging of user and service activity in syslog format for integration into  
| | SIEM tools  
| | Support for Symantec Certificate Authority  
| | 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  
| | New policy items:  
| | Service Access Code  
| | Wi-Fi Direct  
| | 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  
<p>| | HP Color LaserJet MFP E87660 |</p>
<table>
<thead>
<tr>
<th>3.0.1</th>
<th>July 2017</th>
</tr>
</thead>
</table>
| • 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. |

**WHAT’S NEW IN SECURITY MANAGER 3.0/3.0.1?**

- Browser-based user interface redesigned to improve usability as well as bring it visually up to date.
- Dashboard indicating status of fleet compliance
- Ability to login as guest or admin role
- Logging of user and service activity in syslog format for integration into SIEM tools
- Support for Symantec Certificate Authority
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

Automatic logout of user from Security Manager after a period of inactivity for improved security. The feature is set to OFF by default but can be enabled and customized by editing values in the configuration file named C:\Program Files (x86)\HP JetAdvantage Security Manager\Webapp\Web.config as such:

```
<add key="ClientIdleTimeInMins" value="20" />
<add key="EnableClientIdleTimeOut" value="false" />
```

- Set "EnableClientIdleTimeOut" to a value of “true” to enable the feature and set “ClientIdleTimeInMins" to indicate the desired period of inactivity in minutes to automatically logout the user.

New policy items:
- Service Access Code
- Wi-Fi Direct
- 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
- PJL Password now supported for LJ 5200
- Fixed two very unique possible causes for task hangs

Software Notes and Known Issues:

- Upgrades from version 2.1.2 directly to version 3.0/3.0.1 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 3.0.
- A locked policy automatically becomes unlocked after 2 hours.
- Device discovery fails if an imported discovery file contains invalid IP Addresses.
- For better representation of pages, maximum recommended zoom is 150%.
- Assess/remEDIATE tasks run forever if an invalid email address is configured in automated output. In such a case, tasks should be cancelled manually and a correct email address should be configured in settings.
- Security Manager relies on a shared library called Microsoft.MSHTML.dll to perform queries on devices using a technique referred to as “web scraping” to manage the features. Older devices rely on this technique more than newer Futuresmart devices. Typically this file is already present in the Global Assembly Cache (GAC), and if so Security Manager will use the file loaded in GAC. If the file is not present in GAC, Security Manager will load a copy of this file. Issues may arise where functionality of this file is not working or is blocked by browser settings, for example. One such setting is a browser setting called “Run antimalware software on ActiveX controls” under the Security tab that will block the usage of this dll. If so, there is a possibility that a task relying on this .dll file to perform managing of a feature may hang as there is never a return to the query. Newer builds (v2.1.5 and 3.0.1) of Security Manager have been released that use a newer library to perform web scraping to alleviate this issue on these unique servers that block the usage of the older library.
- The global credentials store is not being used to validate credentials on a remediation attempt if the global store contains only the SNMP Read/Write Community Name but a verify task passes using the default public SNMP Read Community Name. If a device has an SNMP Set Community Name set through EWS, but SNMP Gets are open to public, Security Manager will only succeed in remediating settings that require SNMP if the SNMP Read/Write Community Name is manually added to the database for the device. Adding the SNMP Read/Write Community Name only to the global credential store will still result in failure during remediations.
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.

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 JetAdvantage Security Manager - Policy Editor Settings” for more detailed information regarding settings for solutions.

SUPPORTED OPERATING SYSTEMS AND DATABASES

OPERATING SYSTEMS
Client and Server

Note: Security Manager is supported on 32-bit and 64-bit operating systems

- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows 10
- Microsoft Server 2008 R2 (64-bit only)
- Microsoft Server 2012
- Microsoft Server 2012 R2
- Microsoft Server 2016

TESTED Browsers
- Internet Explorer 11 and greater
- Google Chrome v55.0 and greater

.NET Versions
Recommended: .NET 3.5 and 4.6.2

Note: Earlier versions of .NET can be used such as 4.6.1, but some issues were seen in testing on the Windows 10 and Windows Server 2016 operating systems using these older versions.

TESTED DATABASES
- Microsoft SQL Server Express 2012
- Microsoft SQL Server 2012
- Microsoft SQL Server Express 2014 (Bundled)
- Microsoft SQL Server 2014

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.
Note: Recommended initial database size of 10GB

HARDWARE REQUIREMENTS

SERVER MINIMUM HARDWARE
- CPU: Dual-core processor or greater – 2.33 GHz or greater
- RAM: 32-bit systems – Minimum 4 GB
- RAM: 64-bit systems – Minimum 8 GB
- STORAGE: Minimum of 4 GB

CLIENT MINIMUM HARDWARE
- CPU: PC with 1.8 GHz or greater processor
- RAM: 32-bit systems – 3 GB or greater
- RAM: 64-bit systems – 4 GB or greater

The following hardware requirements are recommended, especially with the inclusion of IIS for the web-based interface. Microsoft recommends quad core processors and 10 GB RAM for IIS.

RECOMMENDED SERVER HARDWARE
- CPU: 4 or more processor cores – 2.8GHz or higher processor speed
- RAM: 64-bit systems – 12 GB or greater
- STORAGE – 4 GB or greater

NOTES
- Connecting to a remote database is made possible through the install process. See whitepaper titled “HP JetAdvantage Security Manager - Using Microsoft® SQL Server” for more information.
- After upgrading to Security Manager 3.0 from earlier versions, existing policies must be opened in the policy editor and saved to be compatible with Security Manager 3.0.
- Before any upgrade or machine restart, it is required that no tasks are in running state. Otherwise, the tasks will remain in the database in a running state.
- For better performance, it is recommended to start new tasks only after the completion of the current task. For example, launch verification task only after the discovery task is complete.

VMWARE SUPPORT

Security Manager is supported in a VMware environment.

Requirements:

The Supported Operating Systems and Databases listed above, are also supported in a VMware environment.

Note: If installing Security Manager on a VMware instance, you must use the hardware (MAC) address of that virtual adapter during the ordering of the license file. Be aware that VMware dynamically generates the virtual adapter MAC address and does not guarantee it will remain static during session restarts or power toggling. If the MAC address changes, the print license service will fail to operate properly. Refer to VMware help documentation for instructions on how to configure a static MAC address or how to change the modified MAC address back to original.
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 requirements are listed below:

- Microsoft SQL Server Systems CLR Types [x86] - (part of installation script)
- Microsoft SQL Server Systems CLR Types [x64] - (part of installation script)
- Microsoft Primary Interop Assembly - (part of installation script)
- Microsoft Report Viewer 2012 Runtime - (part of installation script)
- Microsoft .NET Framework 4.6.1 or greater - (install prior to installation script)
- Microsoft .NET Framework 3.5 or greater - (install prior to installation script)
- Microsoft SQL Server Database - (see supported databases above)
- 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 2014 database which is bundled with the product.

Installation Notes:

- Recommended .NET versions are: .NET 3.5 and 4.6.2. Earlier versions of .NET can be used such as 4.6.1, but some issues were seen in testing on the Windows 10 and Windows Server 2016 operating systems using these older versions.
- The new 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 new 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 new 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 new browser-based interface supports either Microsoft Internet Explorer or Google Chrome. 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.
- If it is desired to run version 3.0.1 but with the older non-web based interface, just run the file named HPSM_UserInterface.exe found under the HP JetAdvantage Security Manager folder.
- Users need to be re-added to the HPIPSC group after software upgrade.
- Licenses need to be re-loaded if the operating system is upgraded.
- 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 JetAdvantage 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.

## 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</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.</td>
</tr>
<tr>
<td><strong>Server to Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80 and 8080</td>
<td>TCP</td>
<td>HTTP</td>
<td>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.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Port used for secure HTTP communication to devices, HTTP Web over SSL.</td>
</tr>
<tr>
<td>N/A</td>
<td>ICMP</td>
<td>PING</td>
<td>Internet Control Message Protocol - port used to check if node is active.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
<td>Simple Network Management Protocol - port used for many configuration items on devices as well as discovery of devices.</td>
</tr>
<tr>
<td>7627</td>
<td>TCP</td>
<td>SOAP-HTTP</td>
<td>Web service port used to manage communications on Futuresmart devices.</td>
</tr>
<tr>
<td><strong>Devices to Server</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3329</td>
<td>TCP</td>
<td>HP Instant-On Security</td>
<td>Secure port (uses SSL) used from the device to the Security Manager service for Instant-On discovered devices.</td>
</tr>
<tr>
<td><strong>Server to SQL database</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1433</td>
<td>TCP</td>
<td>MS SQL</td>
<td>Standard DB Connection - port used from the Security Manager service to a remote SQL database. Can be customized in a configuration file.</td>
</tr>
<tr>
<td><strong>Server to Email</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
<td>Typical port used for communication to mail server if Automated Output feature is enabled. Port can be customized under File, Settings, Automated Output.</td>
</tr>
<tr>
<td><strong>Server to Certificate Authority</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>135</td>
<td>TCP</td>
<td>DCOM/RPC</td>
<td>Certificate management - port used between Security Manager service and CA server.</td>
</tr>
</tbody>
</table>
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 three separate services represented by four executables:

- C:\Program Files (x86)\HP JetAdvantage Security Manager\HPSM_Service.exe
- C:\Program Files (x86)\HP JetAdvantage Security Manager\HP Print License Service\HP.Print.License.Host.WindowsService.exe
- C:\Program Files (x86)\HP JetAdvantage Security Manager\HP Print License Service\HPQ.exe
- C:\Program Files (x86)\HP JetAdvantage Security Manager\HP Print License Service\lmgrd.exe

The only time Security Manager could potentially traverse outside the company firewall is if Check for Latest Firmware assessments are 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.