Technical white paper

HP JetAdvantage Security Manager

Release Notes v3.2.1

Table of contents

Overview

Announcing HP JetAdvantage Security Manager 3.2.1, 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.

Version information

Version history of HP JetAdvantage Security Manager releases:

Version	Release Date	Features
2.0.0	Feb 2012	• 76 HP Device Models Supported (See Supported Devices) • Instant-On Security • Intelligent Security Policy Editor • Background Security Compliance Monitoring
(Major Release)	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
2.0.5	Nov 2012	• Implemented Password Management Functionality • Enhanced Instant-On Security • Added support for operating systems: o Windows 8 & Windows Server 2012 • Added support for devices & accessories: o HP LaserJet 700 M712 o HP LaserJet color flow MFP M575 o HP LaserJet flow MFP M525 o HP LaserJet 700 color MFP M775 o HP JetDirect 640n and 695nw
2.0.7	April 2013	• Device DNS alias resolve and discovery • Selectable SNMPv3/AES or SHA-1 credential/device communication • New support for HP Officejet Pro devices: o 251dw printer o 276dw MFP o X451dw printer o X476dw MFP o X551dw printer o X576dw MFP • New support for HP LaserJet Pro devices: o P2055 printer o 300 color MFP M375 o 400 printer M401 o 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
2.0.8	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
2.1.0 (Major Release)	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
		  o LaserJet Enterprise M604
		  o LaserJet Enterprise M605
		  o LaserJet Enterprise M606
		  o Color LaserJet Pro M252
		  o Color LaserJet Pro MFP M277
		  o Color LaserJet Enterprise M552
		  o 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
		  o HP LaserJet MFP M527
		  o HP LaserJet Flow MFP 527
		  o HP LaserJet M506
		  o HP Color LaserJet MFP M477
		  o HP Color LaserJet M452
		  o HP LaserJet MFP M426
		  o HP LaserJet M402
		  o HP Color LaserJet MFP M577
		  o 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) • 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 o HP LaserJet Pro M501 o HP Color LaserJet Pro MFP M377 o HP PageWide Color 556 o HP PageWide Color MFP M586 o HP PageWide Color Flow MFP M586 o HP PageWide Pro 452 o HP PageWide Pro MFP 477 o HP PageWide Pro 552 o HP PageWide Pro MFP 577 o HP PageWide XL 4500 o HP PageWide XL 5000 o HP PageWide XL 8000 o HP DesignJet T1120 44In o HP DesignJet T1500/Postscript o HP DesignJet T2300/Postscript o HP DesignJet T2500/Postscript o HP DesignJet T770 o HP DesignJet T790 44In o HP DesignJet T790PS 24In o HP DesignJet T790PS 44In o HP DesignJet T920/Postscript o HP DesignJet T1300 o HP DesignJet T1300/Postscript o HP DesignJet T3500 o HP DesignJet Z5400
2.1.5	June 2016	• New Policy Items o Verify Certificate for IPP/IPPS Pull Printing o Enable WINS Port o WINS Registration o Secure Disk Password • Changes to Policy Items o Subject Alternate Names (SANs) added to Identity certificates. o 802.1x remediation o Bootloader Password remediation o Ability to remediate SSL 3.0 o Maximum Attachment Size for SMTP E-mail settings can be remediated to any custom value between (0-999). o EWS Password Account Lockout settings • Certificate Management of Pro devices • Installed solutions can now set "Local" for many of the Authentication Manager settings • Reports include Device Model column instead of Device Name for consistency across products • Assessments reports now include an Export Data tab to export to .csv or .xml file on the fleet

		• Serial number no longer has to be upper case for Instant On filtering
		• The checkbox to E-mail results for remediation task now saves correctly in UI when editing task
		• dbo_DeviceTable now removes records during nightly cleanup when device is deleted
		• Database is no longer locked to a specific Security Manager server allowing for much easier failover techniques on the Security Manager server
		• New HP Device Support
		  o HP LaserJet Pro M203
		  o HP LaserJet Pro MFP M227

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:
		  o Service Access Code
		  o 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:
		  o PJL Password now supported for LJ 5200
		  o Fixed two very unique possible causes for task hangs
		• New HP Device Support
		  o HP Color LaserJet Enterprise M652
		  o HP Color LaserJet Enterprise M653
		  o HP Color LaserJet Enterprise MFP M681
		  o HP Color LaserJet Enterprise MFP M682
		  o HP Color LaserJet MFP E77822
		  o HP Color LaserJet Flow MFP E77822
		  o HP Color LaserJet MFP E77825
		  o HP Color LaserJet Flow MFP E77825
		  o HP Color LaserJet MFP E77830
		  o HP Color LaserJet Flow MFP E77830
		  o HP Color LaserJet MFP E87640
		  o HP Color LaserJet Flow MFP E87640
		  o HP Color LaserJet MFP E87650
		  o HP Color LaserJet Flow MFP E87650
		  o HP Color LaserJet MFP E87660
		  o HP Color LaserJet Flow MFP E87660
		  o HP LaserJet Enterprise M607
		  o HP LaserJet Enterprise M608

		o HP LaserJet Enterprise M609 o HP LaserJet Enterprise MFP M631 o HP LaserJet Enterprise Flow MFP M631 o HP LaserJet Enterprise MFP M632 o HP LaserJet Enterprise Flow MFP M632 o HP LaserJet Enterprise MFP M633 o HP LaserJet Enterprise Flow MFP M633 o HP LaserJet MFP E72525 o HP LaserJet Flow MFP E72525 o HP LaserJet MFP E72530 o HP LaserJet Flow MFP E72530 o HP LaserJet MFP E72535 o HP LaserJet Flow MFP E72535 o HP LaserJet MFP E82540 o HP LaserJet Flow MFP E82540 o HP LaserJet MFP E82550 o HP LaserJet Flow MFP E82550 o HP LaserJet MFP E82560 o HP LaserJet Flow MFP E82560 o HP PageWide Pro 750 o HP PageWide Pro 755 o HP PageWide Pro MFP 772 o HP PageWide Pro MFP 777 o HP PageWide P75050 o HP PageWide P75060 o HP PageWide MFP P77740 o HP PageWide MFP P77750 o HP PageWide MFP P77760 o HP DesignJet T930 o HP DesignJet T930 Postscript o HP DesignJet T1530 o HP DesignJet T1530 Postscript o HP DesignJet T2530 o HP DesignJet T2530 Postscript
3.0.1	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 theold MSHTML library.
3.1	December 2017	• 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 24.5firmware • New policy items:

		o Web Scan and Secure Web Scan o Individual cipher suites under Web Encryption Settings o Role Based Access Control o Add Roles to User or Group o EWS Roles under Authentication Manager o HP Connection Inspector o Cross Site Request Forgery (CSRF) Prevention o IPSEC/Firewall o 802.1x (wireless) • Fixes: o Global credentials working properly o Incorrect passwords stored in database remain in database if unsuccessful o Time zone difference between client and server allows for running tasks immediately if desired o Time zone displayed in proper 24-hour format if desired o CA certificates are now deleted if checkbox is checked to remove certificates not in policy o CA certificates are now successfully installed on devices set to non-English language • New HP Device Support o HP Color LaserJet M254 o HP Color LaserJet MFP M281 o HP Color LaserJet E65050 o HP Color LaserJet E65060 o HP Color LaserJet E67550 o HP Color LaserJet E67560 o HP LaserJet E60055 o HP LaserJet E60065 o HP LaserJet E60075 o HP LaserJet MFP E62555 o HP LaserJet MFP E62565 o HP LaserJet MFP E62575 o HP LaserJet MFP E72545 o HP LaserJet Flow MFP E72545 o HP PageWide Enterprise Color 765dn o HP PageWide Enterprise Color MFP 780 o HP PageWide Enterprise Color Flow MFP 785 o HP PageWide Color E55650 o HP PageWide Color MFP E58650 o HP PageWide Managed Color E75160 o HP PageWide Managed Color MFP E77650 o HP PageWide Managed Color MFP E77660 o HP PageWide P55250 o HP PageWide MFP P77740 o HP PageWide MFP P77750 o HP PageWide MFP P77760 o HP PageWide MFP P57750 o HP DesignJet T830 24-in MFP o HP DesignJet T1700dr PostScript o HP Digital Sender Flow 8500

		○ HP ScanJet Flow N9120 fn2 ○ Zebra ZTC ZT410-203dpi ZPL
3.1.1	March 2018	• Fixed issue with Admin (EWS) Password always remediating evenif 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 Policy Items: ○ HTTPS ○ CIFS (Shared Folder) ○ FTP Client ○ FTP Server ○ JetAdvantage Link ○ Extended Signature Verification ○ Control Panel Logout Policy • Fixes: ○ Order of operation causing Network Connection Error or Credentials Failed status ○ Autogroups limited to 10 ○ Autogroup filter for Hostname cannot be blank ○ Disk Encryption Status claims failed for SSD/eMMC ○ File Erase Mode fails when no disk is present ○ Incorrect hover help for Certificate Authority Name ○ Can't install an intermediate CA cert on older devices ○ Duplicate ID certificates installed ○ Can't add IP Addresses to ACL ○ Installer uses ODBC to connect to SQL on third option for Connect to Existing DB ○ Device replacing another at same IP Address does not update all attributes • Secure Boot Presence fails for devices that don't support feature • SNMPv3 queries when v3 is disabled • New Device Support ○ HP PageWide Managed Color P75250 ○ HP PageWide Managed Color MFP P77440 ○ HP LaserJet MFP E50045n ○ HP LaserJet MFP E52545dn ○ HP LaserJet Flow MFP E52545c ○ HP Color LaserJet MFP E55040dn ○ HP Color LaserJet MFP E57540dn ○ HP Color LaserJet Flow MFP E57540c ○ HP DesignJet T3500 ○ HP DesignJet Z5600 ○ Samsung Multifunction MultiXpress K7400, K7500, K7600,

		• K7650, K703, K705, K706
		  o Samsung Multifunction MultiXpress X7400, X7500, X7600, X703,
		• X704, X705, X706
		  o Samsung Multifunction ProXpress M4580,M4583
		  o Samsung Multifunction MultiXpress M4370, M5370,M5270
		  o Samsung Multifunction MultiXpress X4220, X4250, X4300, X400, X401, K4250, K4300, K4350, K401,K400

3.2.1	December 2018	• Features:
		  o Firmware version is now an autogrouping filter.
		  o 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 remediated.
		  o More than one range can be entered for a single IP Range discovery.
		  o Discoveries can now be scheduled to occur at some desired frequency.
		  o Added option to properly assess PJL Password if PJL Accessis disabled by temporarily enabling PJL Access.
		  o Added support for Active Directory authentication to be usedto remotely manage devices instead of Admin (EWS) Password.
		  o A new option is available to limit Assessment & Remediation history stored in the database to some desired amount ofdays.
		  o New Repetitive Remediation report includes devices being remediated for the same items multiple times.
		• New Policy Items:
		  o SIP Server Settings
		  o Postscript Security
		  o Wireless Radio State
		  o Information Hiding
		  o Added Fax Receive Owner option (Drop down values as Guest, Administrator, Network User) under Fax Receive Policy Item.
		• Fixes:
		  o SNMP Read/write Community Name is now attempted in global credentials if public is enabled for SNMP Reads on the device.
		  o 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.
		  o CA certificate now remediates on a CLJ CM4730mfp when server localization is non-English.
		  o Duplicate identity certificates are no longer installed if an assessment finds a mismatch in the ID

		certificate. Certificate is replaced instead of appended. o CA certificate displays Issued To name instead of Issued By name. o Fixed CA certificates issue on older devices requiring checkbox to allow intermediate certs. Root and intermediate certificates now install successfully. o Fixed ID certificates issue where SANs are assessed incorrectly and a new certificate is always installed. o 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. o Fixed the SAN behavior for non-unified devices where FQDN was not included as a SAN. o Added certificate management support for DesignJet T1700. o Vulnerabilities in Bootstrap library and AngularJS library resolved by patching code fixes from new versions. o 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. o Write verification failed is no longer displayed while remediating FTP firmware Update policy on LJ M631. o 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. o PJL Passwords and File System Passwords are now pulled from the Global Credential Store during assessments/remediations if required. o HP JetDirect XML Services now assesses properly on some older JetDirect nics. o Fixed model name sorting issue on older devices that display with lower case. o Added support for CSRF with FS3 firmware o Fixed the behavior where a non- reachable device was displaying o as "Credentials Failed" for device status. o Fixed the behavior where PJL password was not remediating on multiple older devices. o CA and ID certificates now correctly claim Not Supported on CLJ 3600 and LJ 300 M375 devices. o Web Encryption Strength fixed in a special build of 3.2.1 posted in February to allow GCM ciphers enabled in policy at same time as TLS 1.0/1.1. • New Device Support

		○ HP PageWide Color MFP 779 ○ HP PageWide Color MFP 775 ○ HP PageWide Color MFP 751 ○ Zebra ZQ320 ○ Zebra ZQ620 • **Note**: All Zebra devices with Link OS >=5.0 are supported just not fully tested. All devices listed below with required Link OS should work as expected. ○ Zebra QLn220 ○ Zebra QLn320 ○ Zebra ZQ310 ○ Zebra ZQ510 ○ Zebra ZD410 ○ Zebra ZD420 ○ Zebra ZD500R ○ Zebra ZT230 200dpi ○ Zebra ZT410 203dpi ○ Zebra ZT610 203dpi

What's new in Security Manager 3.2.1?

- 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 remediated.
  - 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 remediated for the same items multiple times.
- New Policy Items:
  - SIP Server Settings
  - Postscript Security
  - Wireless Radio State
  - Information Hiding
  - Added Fax Receive Owner option (Drop down values as Guest, Administrator, Network User) under Fax Receive Policy Item.
- Fixes:

- SNMP Read/write Community Name is now attempted in global credentials if public is enabled for SNMP Reads on the device.
- 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.
- CA certificate now remediates on a CLJ CM4730mfp when server localization is non-English.
- Duplicate identity certificates are no longer installed if an assessment finds a mismatch in the ID certificate. Certificate is replaced instead of appended.
- CA certificate displays Issued To name instead of Issued By name. This makes it easier to discern between multiple intermediate certificates.
- Fixed CA certificates issue on older devices requiring checkbox to allow intermediate certs. Root and intermediate certificates now install successfully. HPSM now determines if a CA certificate is a root certificate or intermediate certificate and checks/unchecks the box under EWS as required.
- Fixed ID certificates issue where SANs are assessed incorrectly and a new certificate is always installed.
- 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.
- Fixed the SAN behavior for non-unified devices (certificates managed under Networking tab) where FQDN was not included as a SAN.
- Added certificate management support for DesignJet T1700. Newer firmware is required.
- 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 remediating FTP firmware Update policy on LJ M631.
- 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.
- PJL Passwords and File System Passwords are now pulled from the Global Credential Store during assessments/remediations if required.
- HP JetDirect XML Services now assesses properly on some older JetDirect nics.
- Fixed model name sorting issue on older devices that display with lower case.
- Added support for CSRF with FS3 firmware
- Fixed the behavior where a non- reachable device was displaying as "Credentials Failed"
- for device status.
- Fixed the behavior where PJL password was not remediating on multiple older devices because the technique being used was not supported for those devices.
- CA and ID certificates now correctly claim Not Supported on CLJ 3600 and LJ 300 M375 devices.
- Web Encryption Strength fixed in a special build of 3.2.1 posted in February to allow GCM ciphers enabled in policy at same time as TLS 1.0/1.1. Note that some devices may report an error attempting to enable GCM ciphers and TLS 1.0/1.1, but most devices allow it.

Software notes and known issues

- 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.
- Remediation for FTP Server policy item is currently not supported on Samsung Printers.
- 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.
- 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.
- 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 for communication to take place 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 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 browser-based interface requires Internet Information Services (IIS) in order to operate. The installer verifies 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 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.
- 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
    - Launch chrome using command "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:
    - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\pendingFileRenameOperation
        - This entry needs to be deleted if it exists.
- 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.
- 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 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 be 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

Operating systems

Client and Server

- Windows 8
- Windows 8.1
- Windows 10
- Microsoft Server 2008 R2
- Microsoft Server 2012
- Microsoft Server 2012 R2
- Microsoft Server 2016

NOTE: Windows 7 SP1 is no longer tested. Therefore, it is no longer officially supported but can be used at customer's own risk. Also, only 64-bit operating systems are tested.

NOTE: MS Windows Server 2019 testing is underway using early Server 2019 builds. Changes were made to the Security Manager 3.2.1 installer to allow for successful installation on an MS Server 2019 operating system. However, exhaustive testing has not been completed, especially on the final Server 2019 release, to ensure proper operation of all Security Manager functionality in MS Server 2019. Therefore, no guarantees can be made that all functionality is performing correctly. Security Manager 3.3 will be the first officially supported version for MS Server 2019.

Tested browsers

- Internet Explorer 11 and greater
- Google Chrome v60.0 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.

IIS Versions

- Recommended: 7.5 or newer

Tested databases

- Microsoft SQL Server Express 2014 (Bundled)
- Microsoft SQL Server 2016

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

Server minimum hardware

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

Client minimum hardware

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.

- CPU: PC with 1.8 GHz or greater processor
- RAM: 64-bit systems – 4 GB or greater

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 3.1 and beyond from earlier versions, existing policies must be opened in the policy editor and saved to be compatible with Security Manager 3.1.
- 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.

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 installationand 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.

Network port assignments

This section lists the ports used by Security Manager.

Port	Protocol	Service	Notes
Client to Server			
7637 (version 3.0+)	TCP	HTTPS	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.
8002 (version 2.1.5-)	TCP	WCF-NET.TCP	WCF with message encryption - port used from a remote client interface to the Security Center service. HPSM versions 2.1.5 and prior.
Server to Devices			
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.
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. Can be customized in a configuration file.
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			
135	TCP	DCOM/RPC	Certificate management - port used between Security Manager service and CA server.
Random allocated high	TCP	DCOM/RPC	Certificate management - port used between Security Manager service and CA server.

TCP ports above 1024			
Licensing			
8888	TCP	HP Print License Service	Licensing - port used between the Security Manager service and the HP Print License service.
27000	TCP	Flexera service	Licensing - port used between the Flexera service and the HP Print License service.

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 SecurityManager\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.

c03601653ENW, Rev.18, February 2019