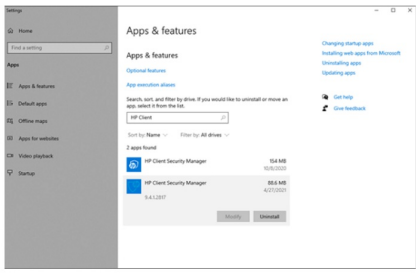


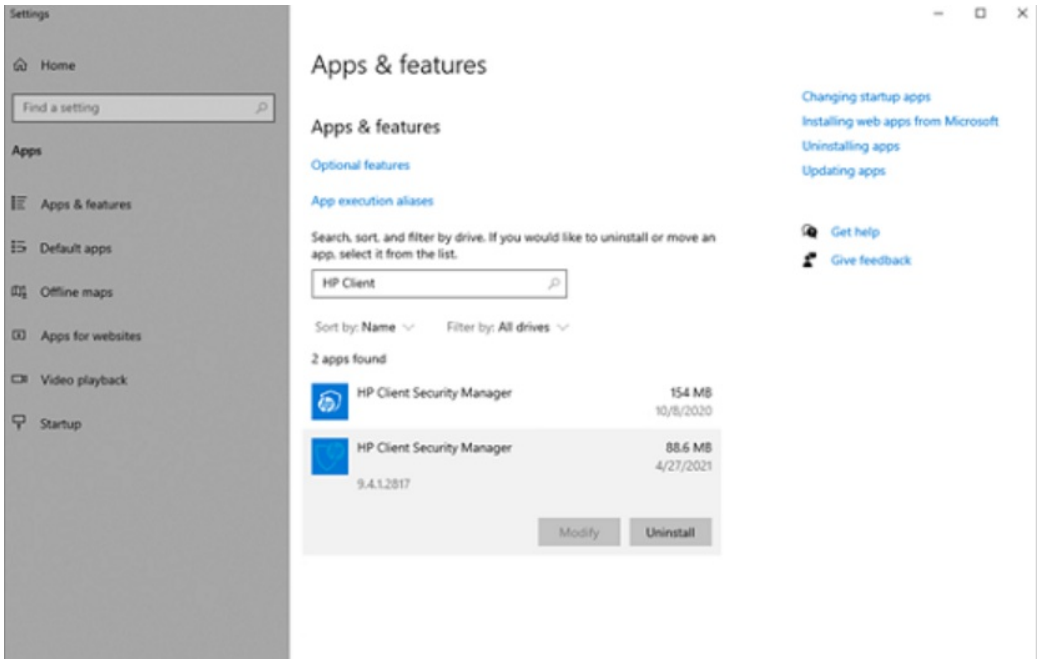

# hp Client Security Manager User Guide



Contents



## hp Client Security Manager



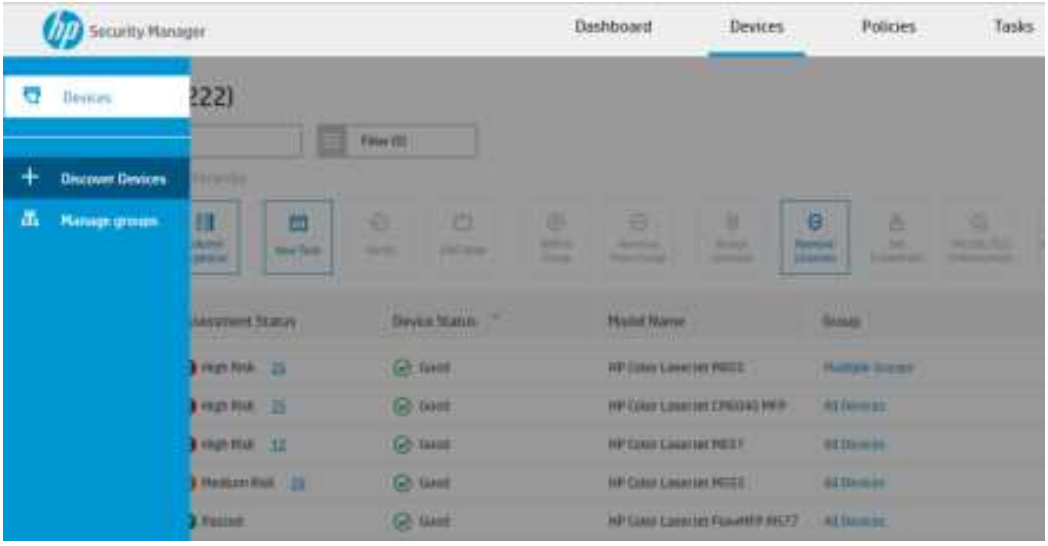

## Overview

Devices are added to HP Security Manager manually using the Discover Devices option or dynamically using the Instant-On Security feature. This whitepaper describes the Discover Devices option in detail, including device identity tracking in the Security Manager database. For information about adding devices using the Instant-On Security feature, see the Instant-On Whitepaper.

## General Description

### Adding devices to Security Manager

Unless the Instant-On Security feature is in use, adding devices to Security Manager is a manual process.
To set up either automatic or manual device discovery, expand the Discover Devices menu from the left pane of the Devices tab.
**Figure:** HP Security Manager Devices tab, Discover Devices menu in the left pane



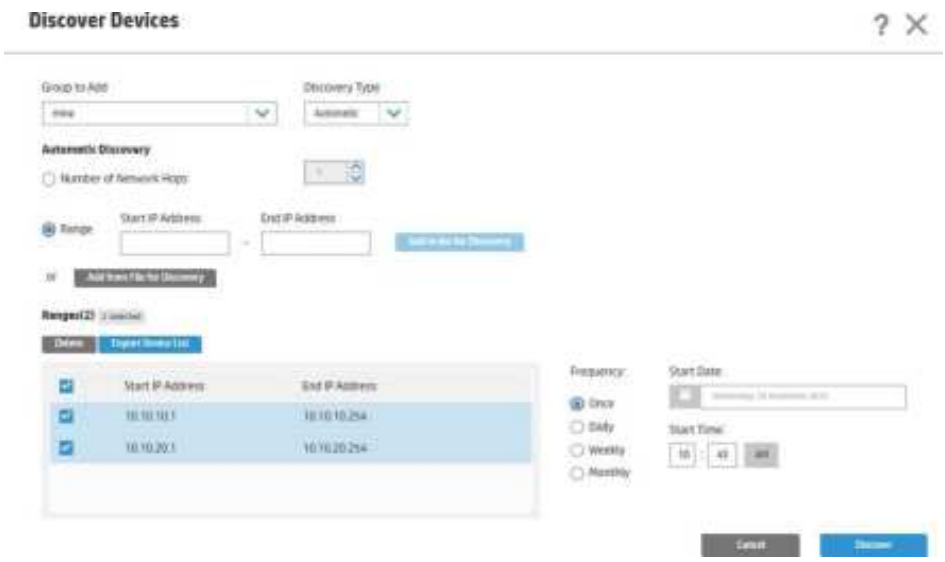

Devices can be manually added by importing a text or XML file that contains a list of devices or by manually entering the device information.
A device list exported from HP Web Jetadmin or from other properly formatted sources can also be used.
Device lists can include IP addresses, hostnames, DNS aliases, or a combination of all three in either an XML or text format.
Use the Verify option on the Devices tab to verify support for a device or group of devices.

Unsupported devices are indicated in the devices panel.
To use the Automatic Discovery feature, select the Devices tab, and then expand the Discover Devices option in the left pane.
Select Automatic on the Discover Devices screen.

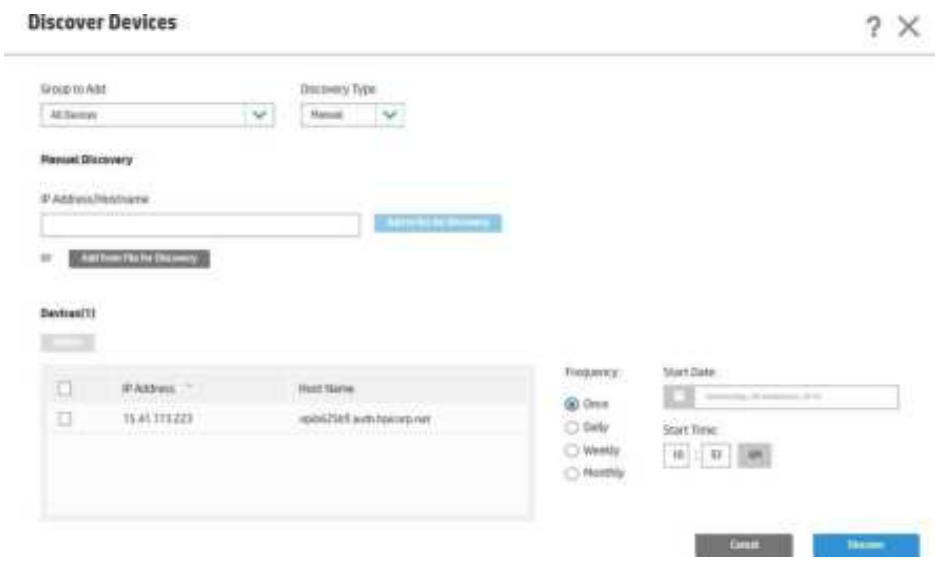
**Select a Discovery Type**

- **Number of Network Hops –** This method uses a multicast UDP discovery mechanism to ask HP imaging and printing devices to identify themselves. The user can select the number of network hops or routers to traverse in the multicast query. The default is 4 hops.
- **Range** – This discovery method scans the given IP address range for all devices that are supported by Security Manager.

**Figure:** HP Security Manager, Discover Devices window, Range discovery option selected



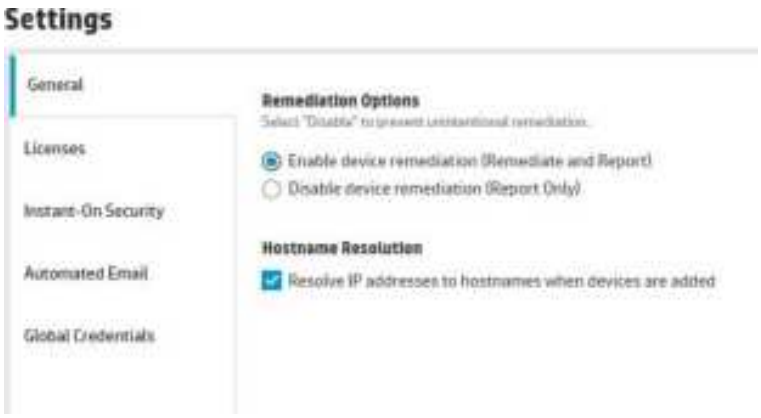

Adjust the Number of Network Hops if an SLP type of discovery is desired. Range is the most popular option.
This method requires typing a Start IP Address, typing an End IP Address, and then clicking the Add to list for Discovery button.
Multiple ranges can be added to the list at one time and added to the box below.
The list of ranges can be exported to a file by selecting Export Device List and later imported again if desired by selecting Add from File for **Discovery.** Discoveries can also be scheduled to occur at a desired frequency.
The group name that is highlighted during the add devices process is the group that populates the Group to Add field.
To select a different group, select it from the Group to Add drop-down list.
To use the Manual Discovery option, select Manual from the Discovery Type drop-down list.
Either type an IP address range to discover devices manually or select Add from File for Discovery to import a file of devices exported from Web Jetadmin.
**Figure:** HP Security Manager, Discover Devices window, Devices discovered under the Devices section using the Manual method




### Adding devices manually to Security Manager

Adding devices manually to Security Manager is a two-step process. The first step stages the devices before database entry.
After an IP address or hostname is typed into the IP Address/Hostname field, or if a file in imported by selecting Add from File for Discovery, if the Resolve IP addresses to hostnames when devices are added check box is selected (default selection) under the Settings menu, HP Security Manager attempts to resolve the provided IP addresses to a hostname and/or performs a reverse lookup on the IP Address. This is strictly Security Manager making calls to the operating system such as GetHostByAddr, and it is the responsibility of the server to find DNS servers and retrieve the information.
When IP addresses are provided, clearing the check box Resolve IP addresses to hostnames when devices are added will disable DNS resolve and results in displaying only the IP address during the add devices process. This can be desirable in the absence of a DNS server or if an IP address timeout is expected (typically within 5 seconds).

If adding devices by hostname or DNS alias, the DNS resolve to IP address occurs automatically.
**Figure:** HP Security Manager, Settings window, General tab is selected




As the final step, devices from the Devices to Add table are added to the database and assigned a license by selecting Discover.
Currently Security Manager interrogates the devices and gathers minimal data to display in columns such as Model Name.
**Figure:** HP Security Manager, after clicking Discover a list of Devices is displayed

The Device Status column indicates No Information since the devices have not been verified yet.
When the devices are selected and after selecting the Verify tab, Security Manager performs a more complete interrogation such as checking credentials to populate the remaining columns.
The System Name column is also populated by taking the sesame object from the device itself.
No DNS lookups are performed here, it is strictly an object returned from the device.
This can be useful for location purposes.

## Overwrite Existing Devices or Create Duplicate IP/Hostname Entries

In a large fleet of devices, devices are getting changed for other/newer devices.
When the new device has the same IP address and/or hostname as the original device HPSM can either overwrite the existing device or create a new device.
This Discovery Behavior depends upon the following settings in the HPSM_service.exe.config file (available from HPSM 3.5 and newer):

- <add key=”OverwriteDeviceDetailsWhenIPsMatches” value=”true” />
- <add key=”OverwriteDeviceWhenHostNameMatches” value=”true” />

When set to true, then the existing device will be overwritten with details from the new device. The HPSM_service.exe.config file is in the following location:
C:\Program Files (x86)\HP Security Manager
After making changes to this file, a restart of the HP Security Manager service is required.

## Detailed Description

**Resolve IP Address to Hostname**
The tracking of Security Manager device identity depends on how the device was added and entered in the database.
The following section provides a detailed explanation of the process.
When the Resolve IP addresses to hostnames when devices are added option is selected and an IP address is provided without a correlating hostname, the IP address DNS resolve process is as follows:

1. A reverse DNS lookup is performed on the IP address.
2. If resolved to a hostname, a forward DNS lookup is performed on that hostname. The hostname must resolve back to the IP address to be valid.
3. If the above steps fail, then an LLMNR broadcast message will be sent to perform a lookup on the system name. If the device responses, then that will be used as the hostname.
   **NOTE:** This requires that LLMNR is enabled on the device and on the operating system.
4. If the above steps fail, then a NBNS (NetBios Name Service message) will be send directly to the device to query the netbios name of the IP address. If the device sends a NBNS response, then that will be used as the hostname.

**NOTE:** this requires that NBNS (called Wins Port in the HP FutureSmart EWS) is enabled on the device and NBNS is enabled for the NIC of the OS.

5. If any address resolve step fails, the device is still staged displaying the IP address only.
6. If reverse and forward address resolve succeeds, the IP address is staged with the hostname.
7. After the device is entered into the database, Security Manager uses the hostname as the primary device identifier.

**NOTE:** A reverse lookup is only done during discovery. If the Hostname column is empty, it will remain empty, even if DNS entries are created afterwards. To display the hostname in HPSM after it has been discovered without a hostname, you must delete the device from HPSM and rediscover.

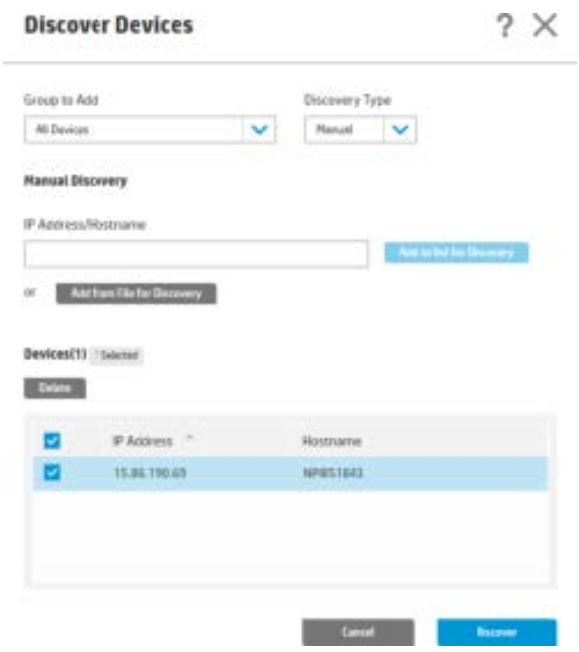
Typing anything other than a valid IP address is interpreted as a hostname or DNS alias. The hostname resolve process will ignore the Resolve IP addresses to hostnames when devices are added setting and always attempt a DNS resolution.

#### Resolve Hostname/DNS Alias to IP Address

**The hostname DNS resolve process is as follows:**

1. A hostname or DNS alias is provided.
2. A DNS forward lookup occurs, and the corresponding IP address is paired for database entry.

Unlike the IP address resolve process, only a forward DNS lookup is required by the hostname resolve process. Failure to resolve the hostname or DNS alias to an IP address produces an error.
Staging devices in the Discover Devices window can assist with device identity validation before entering that device address into the database.
After a device is added to the Devices list, it can be removed by highlighting it and clicking the Delete button (multiple rows can by highlighted and removed).
**Figure**: HP Security Manager, Discover Devices window

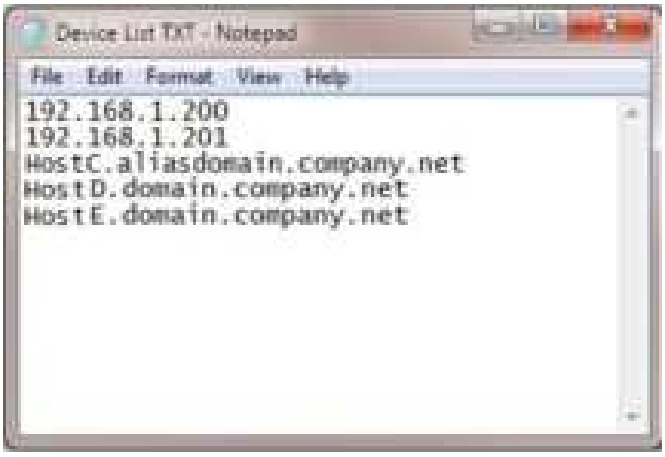



**Add Devices Using a Text or XML File**
The alternative to staging devices in a singular fashion is to import a pre-populated device list in text or XML file format.
This is performed by clicking the Add from File for Discovery button and browsing to your device file of choice.

**Add Devices with a Text File**
The devices listed in the text file (one per line) can include IP addresses, hostnames, DNS alias records, or a mixture of all three.
The text file is invalid if the following parameters exist:

- An address line exceeds 256 characters,
- An address line contains control characters or symbols, and/or
- It cannot be parsed correctly

**Figure:** Example Text File using Notepad




**Add Devices with an XML File**
You can create device lists in XML format from a Security Manager export, an HP Web Jetadmin export, or by using an XML editor. Security Manager only uses the data found for the IP Address and IP Hostname tags. Examples of exported HP Web Jetadmin and Security Manager device lists are listed below.
**Figure:** Example Text File exported from Web Jetadmin

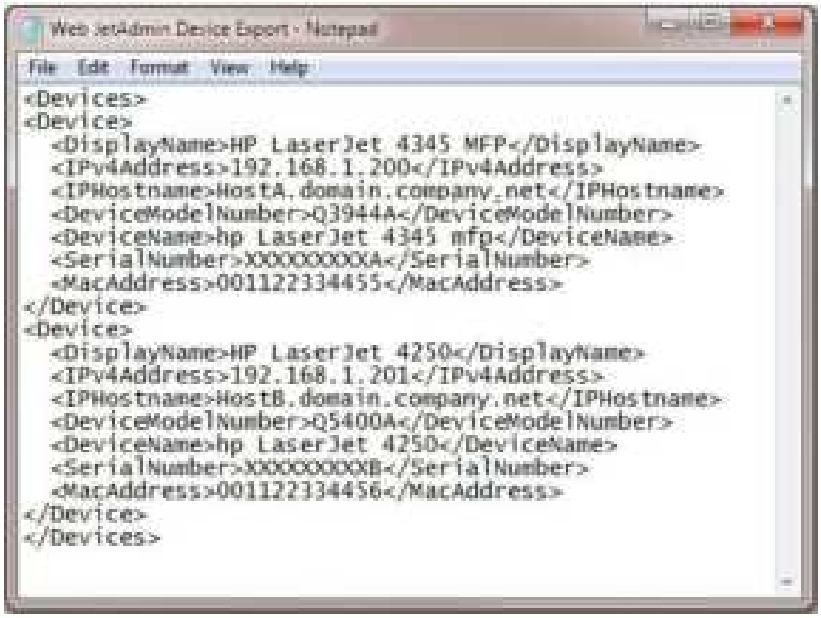
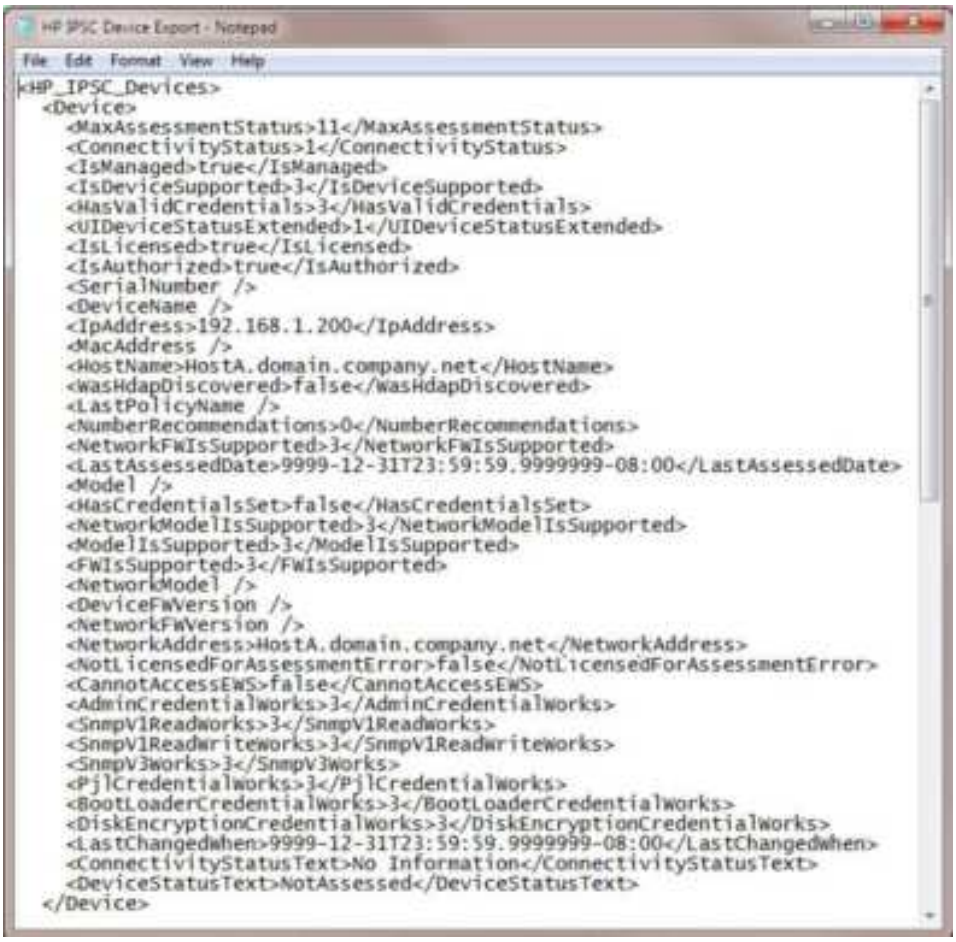



**Figure:** Example Text File exported from Security Manager (IPSC)




If both the hostname and IP address are included in the XML file, the hostname is used during DNS resolution and the Resolve IP addresses to hostnames when devices are added setting is ignored. Hostname resolution always occurs when the hostname is provided, regardless of whether the Resolve IP addresses to hostnames when devices are added option is selected.

HP Security Manager uses the IP address that the provided hostname resolves to, which might be different than the IP address provided in the same XML file with the hostname. This ensures that the hostname to IP address pairing is current.

## Add devices to the Security Manager database

To add the devices listed in the Discover Devices table, click the Discover button.
If a license file is installed in Security Manager, devices are added to the database and automatically assigned a license.
Without a license file installed, devices are still added to the database.
Licenses can be manually assigned later. A Success message displays the number of new devices added, duplicates skipped, devices licensed and unlicensed.

### Determining Device Details

How a device is entered into the database determines how device identity is tracked and used for communication. Use the following definition and the flow chart below to understand how Security Manager tracks and determines device identity.

### Manually adding devices to the database

Devices are manually added to Security Manager in a singular fashion or through a device list during the import process.
Device identity is provided to Security Manager via an IP address, hostname, or DNS alias (CNAME). Devices cannot be added by MAC or network interface hardware address.
If a device is added using the hostname or DNS alias, the device's IP address is automatically resolved and

paired to the hostname or DNS alias in the database. The Resolve IP Addresses to Hostnames when devices are added setting is ignored when a hostname or DNS alias is provided as the device identity. If the device is added using the IP address, a database entry choice is provided.

- If the Resolve IP Addresses to Hostnames when devices are added option is selected (default), the hostname is resolved and linked to the IP address in the database.
- If the Resolve IP Addresses to Hostnames when devices are added option is NOT selected, the device's hostname is not resolved and only the IP address is entered in the database.

**Communicating with the Device**

When a task is launched, HP Security Manager checks for the presence of the hostname or DNS alias in the database. If the hostname or DNS alias is not present, the IP address in the database is used instead.

If the hostname or DNS alias is present in the database, it is resolved to the DNS registered IP address. If the IP address is valid and the device is online, communication with that device should be successful.

If the device does not respond to the database IP address or DNS provided IP address, communication with that IP address will fail. If communication fails, the appropriate error status is updated in HP Security Manager.

When communication is successful and new device identifying information is gathered, the database is updated with the latest information.

Figure: Diagram of HP Security Manager communication with the device

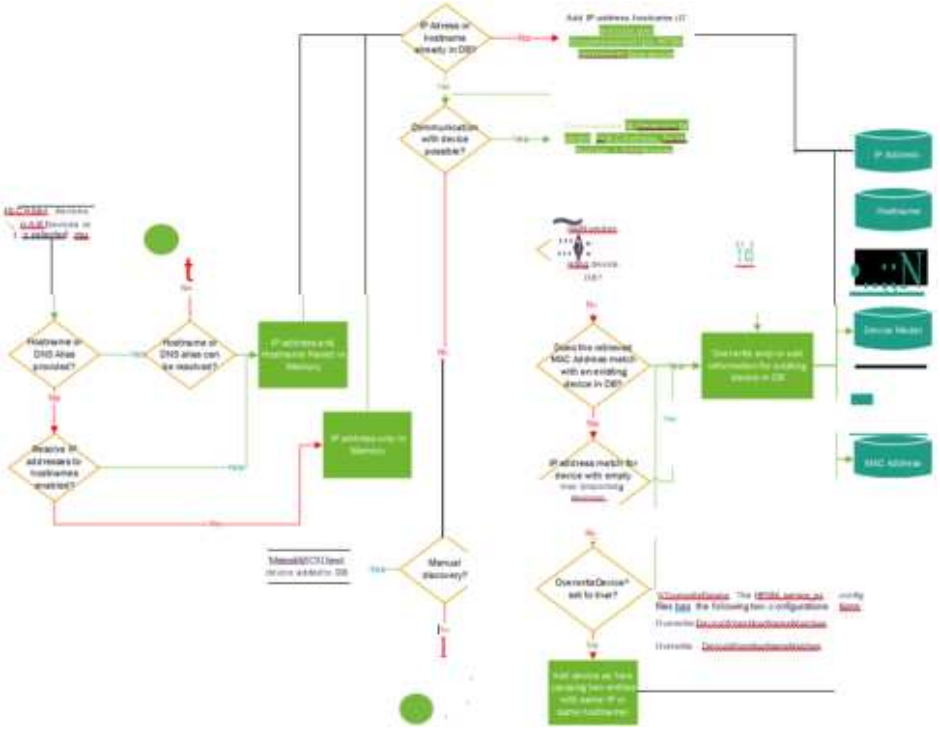
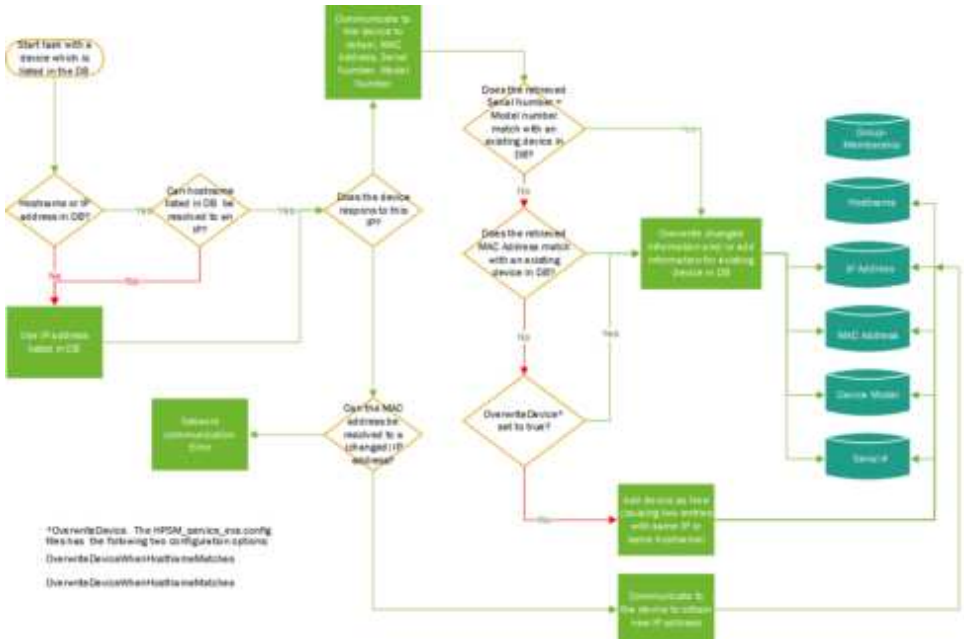


**Figure:** Diagram of HP Security Manager communication with the device, cont.



### Exporting devices from Security Manager 3.8 and older

When exporting devices from HPSM 3.8 and older, HPSM will display the numerical values instead of a description of the value. When exporting device details from HPSM 3.9 onwards, a textual description of the value will be available in the exported data..
**MaxAssessmentStatus** – Displays the Assessment Status using the following numbers:

- -1 = None
- 0 = No Match, or to indicate that there is no filter selected in the UI
- 10 = Passed Assessment
- 11 = Not Assessed
- 12 = Failed Assessment with Low Risk
- 13 = Failed Assessed with Medium Risk
- 14 = Failed Assessed with High Risk
- 16 = Error

**ConnectivityStatus** – Displays the connectivity status of the device using the following numbers:

- 1 = Unknown, Device Status will display the following status:


- 2 = Valid Connection including statuses such as Good, Connection Refused, Credentials Failed, Not Supported, Hostname Resolution Error, Credentials not Validated or Incorrect
- 3 = No Connection, Device Status will display the following status:


- 4 = No Connection because of Error status

**IsManaged** – Indicates if the device has a license. Displays as false/true.

**IsDeviceSupported** – Is dependent on results from networkFWisSupported, networkModelIsSupported, modelIsSupported, fwIsSupported values. Displays the supported device status by HPSM using the following numbers:

- 1 = Device is supported. Device status can be displayed as one of the following statuses:
  - Good or
  - Credentials Failed
  - Network Connection Error
  - Connection Refused
  - Hostname Resolution Error
- 2 = Device is not supported. Device status can be displayed as one of the following statuses:
  - Error
  - Not Supported
- 3 = Unknown if device is supported. Device status will be displayed as: No information (not verified)

**HasValidCredentials** –Indicates whether HPSM has the correct credentials for the device.
Displays the credentials status using the following numbers:

- 1 = Credentials are valid. Device status can be displayed as:
  - Good
  - Connection Refused (Not Supported)
- 2 = Credentials are invalid. Device status will be displayed as:
  - Credentials Error
- 3 = Cannot determine if credentials are valid. Device status can be displayed as:
  - Error
  - Network Connection Error, or
  - No Information

**UIDeviceStatusExtended**

1. = No information (not verified)
2. = Good
3. = Error
4. = Network Connection Error
5. = Credentials Failed, SNMP invalid, cannot retrieve device model or NIC
6. = Not Supported
7. = Connection Refused
8. = Credentials Failed, SNMP valid
9. = Device Not Authorized
10. = License Required for Assessment
11. = Hostname Resolution Error

IsLicensed – Displays if the device licensed in HPSM. Displays as false/true.
IsAuthorized – Only used internally in HPSM code. Displays as false/true.
IsNewDevice – As long as no manual changes are made to the device, the device will be listed as New. Displays as false/true.
ExactModelName – This is the column Exact Model Name in the Security Manager UI. For example: HP LaserJet 500 color M551
SerialNumber – This is the device serial number.

**DeviceName** – This is the Nickname of the device.
This is the column Name in the Security Manager UI.
In HP FutureSmart 4, the nickname of the device can be seen on the Configuration page of the device:


This can be changed as part of the device configuration in the Embedded Web Server on the General tab:


**NOTE:** On HP Future Smart 3, this is called Device Name in the Embedded Web Server (EWS).


**NOTE:** On the Networking tab, a different name will display below the printer's name. See DeviceHostName.
IpAddress – This is the IP Address.
MacAddress – This is the MacAddress which is used for communication with the device. For example: 3CD92BA0F064
HostName – This is the resolved hostname.
WasHdapDiscovered – Indicates whether the device is discovered via Instant On (HP device announcement protocol). Displays as false/true.
LastPolicyName – This is the last policy used for assessment.
NumberRecommendations – Indicates the number of recommendations for a device. If there are

recommendations, then the number will be displayed with an underlined in the Assessment Status

column. Zero means that there are no recommendations (the device was never assessed, or the device passed the assessment).

**NetworkFWIsSupported -Subcategory for is DeviceSupported**

- 0 = Network FW is not supported by HPSM
- 1 = Network FW is supported by HPSM
- 2 = Failed
- 3 = Unknown
- 4 = FirmwareUpgradeNeeded (firmware is supported by HPSM but upgrade is recommended)

**NOTE:** HPSM determines if the Network firmware is supported by querying several properties of the device.

LastAssessedDate – This is the date of last assessment. A date of 9999-12-31T23:59:59 means that the device has not been assessed.
Model – This is the Device Model.
HasCredentialsSet – No longer used, always holds the default value of false. Displays as false/true.

**NetworkModelIsSupported – Subcategory for isDeviceSupported**

- 0 = Network model is not supported by HPSM
- 1 = Network model is supported by HPSM
- 2 = Failed
- 3 = Not Verified (unknown)

**ModelIsSupported – Subcategory for isDeviceSupported**

- 0 = Printer model is not supported by HPSM
- 1 = Printer model is supported by HPSM
- 2 = Failed
- 3 = Not Verified (unknown)

If a printer model is considered as supported by HPSM depends upon a combination of several properties which are queried by HPSM.

**FWIsSupported – Subcategory for isDeviceSupported**

- 0 = Network FW is not supported by HPSM
- 1 = Network FW is supported by HPSM
- 2 = Failed
- 3 = Not Verified (unknown)
- 4 = Network FW is supported by HPSM, but firmware upgrade is recommended
- NetworkModel J8028
- DeviceFWVersion 2309025_582108

- NetworkFWVersion JDI23900042

NetworkAddress – Hostname of the device, if hostname is not present then the IP address will be used.

**AdminCredentialWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried (Not Verified, perhaps because no SNMP read access)
- 4 = NotTriedReadOnly
- 5 = Inconclusive
- 6 = TimeOut (available from HPSM 3.6 and newer)

**SnmpV1ReadWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried (Not Verified, perhaps because no OID support)
- 4 = NotTriedReadOnly
- 5 = Inconclusive
- 6 = TimeOut (available from HPSM 3.6 and newer)

**SnmpV1ReadWriteWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried
- 4 = NotTriedReadOnly
- 5 = Inconclusive
- 6 = TimeOut (available from HPSM 3.6 and newer)

**SnmpV3Works**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried
- 4 = NotTriedReadOnly
- 5 = Inconclusive
- 6 = TimeOut (available from HPSM 3.6 and newer)

**PjlCredentialWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried
- 4 = NotTriedReadOnly
- 5 = Inconclusive

**BootLoaderCredentialWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried
- 4 = NotTriedReadOnly
- 5 = Inconclusive

**DiskEncryptionCredentialWorks**

- 0 = None
- 1 = Success
- 2 = Failed
- 3 = NotTried
- 4 = NotTriedReadOnly
- 5 = Inconclusive

SslValidCert – Indicates whether the installed ID certificate is valid using the following numbers:

- 0 =true
- 1 = false (a self-signed certificate is always displaying SslValidCert as false)

LastChangedWhen – Displays when the latest date when a change was made on the device with an HPSM policy. **NOTE:** A date of 9999-12-31T23:59:59 means that HPSM has not made any changes to the device configuration. When a device is reset to Not Assessed, the lastChangedWhen entry remains unchanged. Example: 2021-02-24T09:40:38

CreatedDate – Date when the device was created in HPSM 2021-02-10T20:50:52


EnforceSslCertifcateValidation – Only connect to the device if a valid ID certificate is installed on the device.

- false – Do Not Enforce SSL/TLS Validation
- true – Enforce SSL/TLS

**Validation Button in HPSM:**


EnforceSSLManual – Not available in UI, is managed only internally in HPSM code. Displays as false/true.
DeviceHostName – This is the column System Name in the Security Manager UI and the configured Host Name on the device.
**NOTE:** In the EWS, the Host Name will be displayed as well below the printer's name.


**NOTE:** If on a different tab than the Networking tab, a different name will display below the printer's name. See DeviceName.

DeviceLocation – This is the column Device Location in HPSM and is the configured device location on the device. In the EWS.
ConnectivityStatusText – This is the textual status which will be displayed in the Device Status column:

**Figure:** Screenshot of all possible Device Statuses in HPSM


The exported values are always truncated (meaning no spaces between the different words).

**DeviceStatusText** – This is related to the text which is displayed in the Assessment Status column None.

- Pass = Passed
- NotAssessed = Not Assessed
- Low = Low Risk
- Medium = Medium Risk
- High = High Risk
- Error =

**FirmwareSecurityStatus** – Only after running an assessment with Check for Latest Firmware set to Firmware Security Service, you can see one of the following values. If no assessment with Firmware Security Service had been running, then the value will always be None.

- OK = the device firmware is OK
- Vulnerable = there are one or more vulnerabilities in the firmware
- OutOfSupport = the firmware for the model is no longer actively being updated by HP
- OutOfDate = the firmware is more than two revisions out-of-date
- NonHP = the model in question is a non-hp product
- NoFirmware = the model in question does not have upgradeable firmware
- NotEvaluated = the firmware was not evaluated because there was not enough data to evaluate (as printer might be too old and might not be listed in firmware security service)
- NotDefined = Indicates either a new status or an invalid response.

Bulletins – Displays more details about the relevant bulletins for the corresponding Firmware Security Status

### Other Assessment/remediation data in the SQL database

The previous section already explains the tables which are used for exporting device data.
In this section some additional tables are described.
The following information is provided “As Is”, which means HP Support cannot be expected to provide assistance as they are not trained SQL experts.
**NOTE:** Even if you have permissions to write information to the database such as DBO rights, never alter any of the information in the SQL tables for fear of breaking the software.
Reading information is fine but altering any data in the tables could affect the functionality of the software itself.
The Security Manager database is always named HPIPSC.
The database includes many tables, but the one table containing the most valuable device data is named dbo_DeviceTable.
The table listed earlier in this appendix describes the columns and values in this table responsible for storing information pertaining to which devices have been assessed or unassessed and the risk levels for each that has been assessed.
Besides the information, which is exported when you select export devices, the following columns are also available in the dbo_DeviceTable:

State – Indicates if device is present in All Devices List or not

- 2 = Valid and present in All Devices List
- 3 = Deleted and no longer present.

There is a nightly process that cleans up and removes devices in State=3, but you will want to exclude these from queries if they exist since they represent deleted devices.

LastPolicyName – Last policy used for assessment

**uiDeviceStatus**

- 1 = No information
- 2 = Good
- 4 = Connection Refused, Credentials Failed, Error, Not Supported, Network Connection Error, Hostname Resolution Error

**uiAssessmentStatus**

- 1 = Passed, no remediation necessary as device is in compliance with policy
- 2 = Not Assessed because of statuses such as Error, Network Connection Error, Connection Refused, Not Supported, No Information, Credentials Failed, Hostname Resolution Error
- 3 = Low Risk
- 4 = Medium Risk
- 5 = High Risk

**HostnameResolutionFailed**

- 1 = Yes
- 2 = No
- 3 = Not Verified, perhaps because no OID support

**Appendix A**
Other HP Security Manager Whitepapers and Manuals
There are a lot of guides and whitepapers available for HP Security Manager.
The view them, go to the HP Security Manager Support page and click the Manuals tab.
The following list of documents is available at the above 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)
- Device Discovery, Determining Device Details, and Exporting Devices (whitepaper)
- HP Security Manager – Installation and Setup Guide
- Manage devices with HP FutureSmart 4.5 Firmware
- Policy Editor Settings including supported devices feature table (white paper)
- Release Notes with Ports (white paper)
- Reporting, Email Alert Subscriptions & Remediation Summary, Auditing, & Syslog Functionality (white paper)
- Securing the HP Security Manager (white paper)
- Sizing and Performance (white paper)
- Supported Devices (white paper)
- Troubleshooting Issues (white paper)
- HP Security Manager – User Guide
- Using licenses and troubleshooting licensing issues (white paper)
- Using Microsoft® SQL Server (white paper)

The section Product Information on the HP Security Manager Support page contains the following information:

- Supported device features matrix (.xls)

**hp.com/go/support**
Current HP driver, support, and security alerts delivered directly to your desktop.

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. 12, January 2023

## Documents / Resources

| | |
|---|---|
|  | [hp Client Security Manager] [pdf] User Guide<br>Client Security Manager, Security Manager, Client Manager, Manager |

## References

- hp.com/go/support
- hp.com/go/support
- HP Security Manager Software Manuals | HP® Customer Support