Technical white paper

HP JetAdvantage Security Manager

Instant-On Security and Auto-Group Remediation

Table of Contents

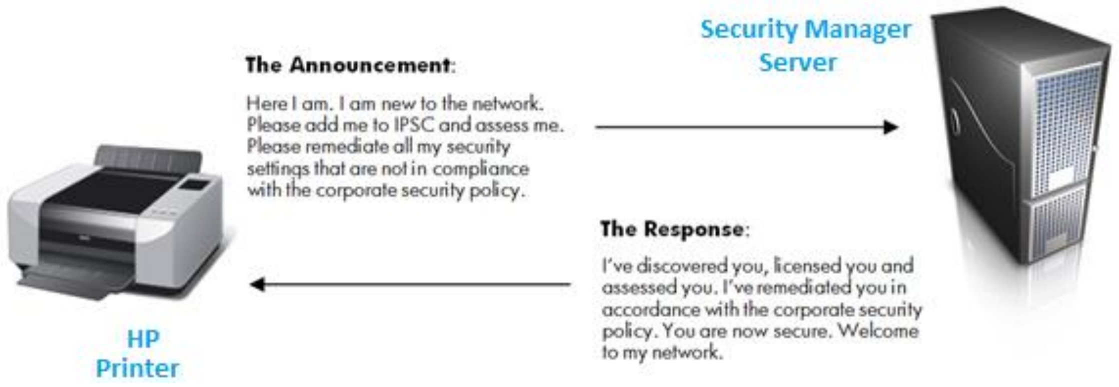
Overview

What is Instant-On Security?

HP JetAdvantage Security Manager (HPSM) is the industry's first policy-based security compliance solution for HP printing and imaging devices. Unique to Security Manager, the Instant-On Security feature provides automatic device discovery and security compliance configuration when an HP supported device is first connected to the network. Afterwards, Instant-On Security maintains security compliance when the usual "after installation" scenarios place the device into a non-compliant state.

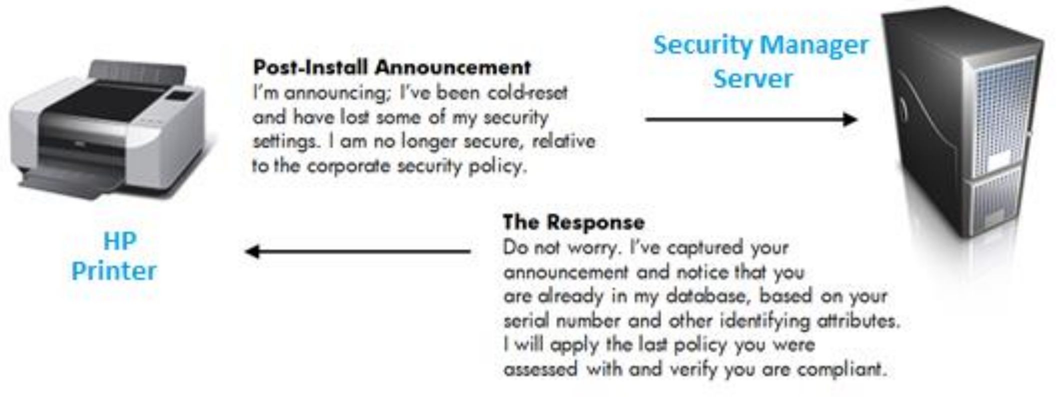
What is Instant-On Secure at Install?

Instant-On Security is a dual component solution consisting of dedicated communication between a supported device and appropriately configured Security Manager software. When enabled at the device, a special device announcement agent locates the Security Manager server and requests secure communication. After the agent source is authenticated, the Security Manager server responds by adding the device to the database and applying a pre-configured corporate security policy. This activity will be referred to as Secure at Install throughout the document.


Security Manager Server
The Announcement:
Here I am. I am new to the network. Please add me to IPSC and assess me. Please remediate all my security settings that are not in compliance with the corporate security policy.
The Response:
I've discovered you, licensed you and assessed you. I've remediated you in accordance with the corporate security policy. You are now secure. Welcome to my network.
HP Printer

What is Instant-On Stay Secure?

After being registered with Security Manager, a device generates an announcement when power cycled, cold reset, assigned a different IP address and for other device specific conditions while on the network. Upon receiving an announcement, Security Manager assesses the device and immediately remediates any setting found to be out of compliance with the last security policy applied to that device. This activity will be referred to as Stay Secure throughout the document. Instant-On security does not rely on periodic database refreshing or special device group configuration. The process is simple; any time a device announces, Security Manager will assess the device and remediate any setting found to be out of compliance with the established corporate security policy.


Post-Install Announcement
I'm announcing; I've been cold-reset and have lost some of my security settings. I am no longer secure, relative to the corporate security policy.
Security Manager Server
HP Printer
The Response
Do not worry. I've captured your announcement and notice that you are already in my database, based on your serial number and other identifying attributes. I will apply the last policy you were assessed with and verify you are compliant.

How do I implement Instant-On Security?

The remainder of this document includes a general and detailed understanding of the Instant-On Security feature, organized into two primary sections. Part 1 covers the device side component, referred to as the Device Announcement Agent. Part 2 covers the Security Manager Instant-On Security configuration server component. Familiarization with both components will explain Instant-On Security as a complete solution and provide assistance for proper implementation.

Instant-On Security, Part 1 - Device Announcement Agent (DAA)

Introduction to Device Announcement Agent (DAA)

This section provides a general understanding of the Device Announcement Agent, why it was developed, and the value it provides.

The Device Announcement Agent (DAA) serves as the device-side component of the Instant-On Security solution and can be found as embedded functionality in most Security Manager supported printers. The DAA can also be found in recently released HP JetDirect network interface cards to provide Instant-On compatibility with legacy HP printers missing the embedded DAA functionality. Please refer to the HP JetAdvantage Security Manager Supported Devices document found at www.hp.com/go/securitymanager for the most current list of Instant-On Security supported devices.

Note: Security Manager Instant-On Security supported devices are a subset of Security Manager overall supported devices.

Developed strictly for use with the Security Manager Instant-On feature, the DAA combined with Security Manager addresses three primary customer desires:

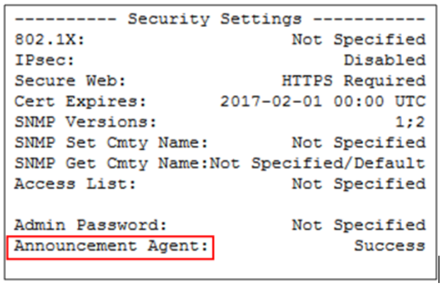
1. An automatic printing device discovery solution that doesn't require additional network configuration, additional protocol enabling, exhaustive searches or chatty broadcasts
2. A solution that provides a true out-of-the-box device security compliance experience or what is referred to as **Secure at Install**
3. A solution that can maintain security settings when the installed device is cold reset or changes IP addresses or hostname, referred to as the **Stay Secure** experience

Due to limitations in fully automatic discovery methods, networked printer discovery is generally a manual process requiring device or network specific input. For example, automatic device discovery methods such as SLP (Service Location Protocol) and Bonjour (mDNS) can provide some automation to the discovery process. Both methods commonly possess limitations that prevent them from being a complete solution in most corporate environments. SLP adoption typically faces packet filtering restrictions, and Bonjour is limited to a single broadcast domain, without special DNS configuration. In addition, automatic discovery methods such as exhaustive subnet scanning are not feasible for IPv6 networks due to size of the address space. These and other automatic methods typically involve some manual intervention, lack efficiency, and do not scale well for large enterprises.

To overcome such limitations, the innovative Device Announcement Agent (DAA) was developed and provides a supported HP printing device the capability of “announcing” its presence directly to the Security Manager server. This announcement process is handled through common DNS address resolve and dedicated TCP port communication (port 3329). The DAA model alleviates the need for manual intervention, is not chatty, and serves as a more efficient device discovery mechanism. After the initial device discovery process is complete, Security Manager applies the established security policy to the device over a secure TCP connection.

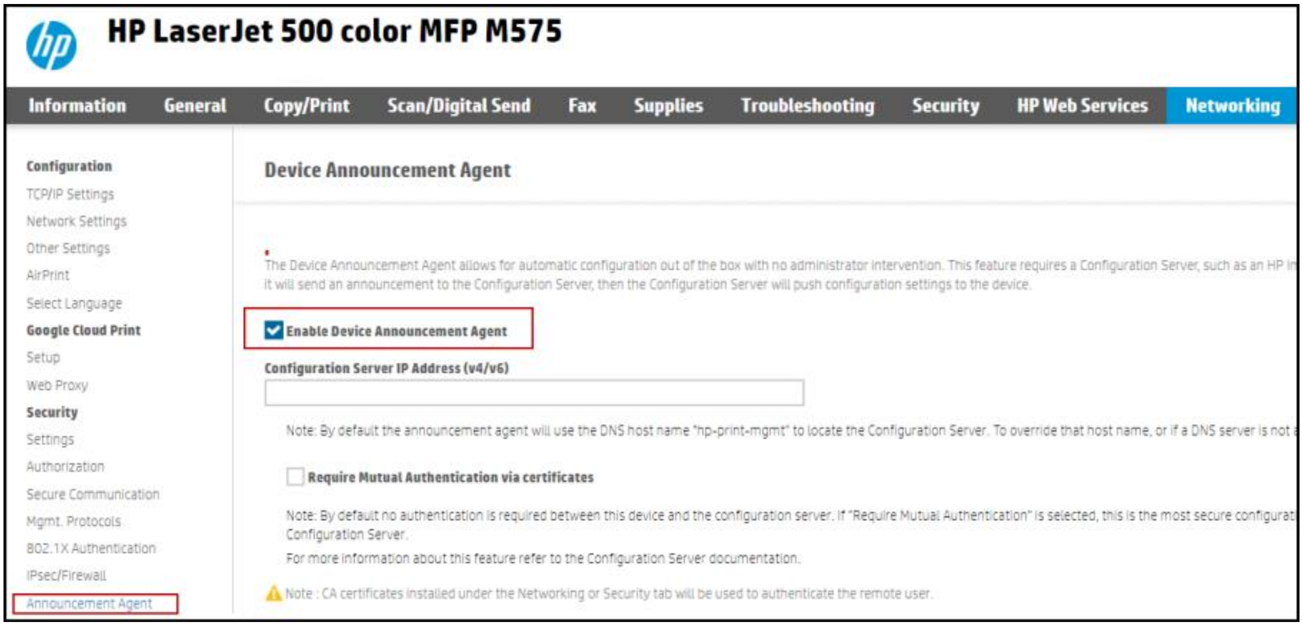
A device **Secure at Install** experience is the result of this two-step process. After the **Secure at Install** process is complete, Instant-On continues with the **Stay Secure** process via the DAA announcements that occur for device cold resets, IP address changes and other device specific conditions. The **Stay Secure** process ensures the device is remediated in accordance with the last security policy applied. With Security Manager, only the settings found to be out of compliance with the established security policy are targeted for remediation.

To quickly identify DAA functionality presence on a specific device, you may print a configuration page. A configuration page example of DAA presence is provided below. You may also browse to the device’s embedded web server “Networking” page to verify DAA presence.



```
---------- Security Settings -----------
802.1X:                    Not Specified
IPsec:                          Disabled
Secure Web:               HTTPS Required
Cert Expires:       2017-02-01 00:00 UTC
SNMP Versions:                       1;2
SNMP Set Cmty Name:        Not Specified
SNMP Get Cmty Name:Not Specified/Default
Access List:               Not Specified

Admin Password:            Not Specified
Announcement Agent:              Success
```



Device Announcement Agent

The Device Announcement Agent allows for automatic configuration out of the box with no administrator intervention. This feature requires a Configuration Server, such as an HP In
it will send an announcement to the Configuration Server, then the Configuration Server will push configuration settings to the device.

☑ Enable Device Announcement Agent

Configuration Server IP Address (v4/v6)

Note: By default the announcement agent will use the DNS host name "hp-print-mgmt" to locate the Configuration Server. To override that host name, or if a DNS server is not a

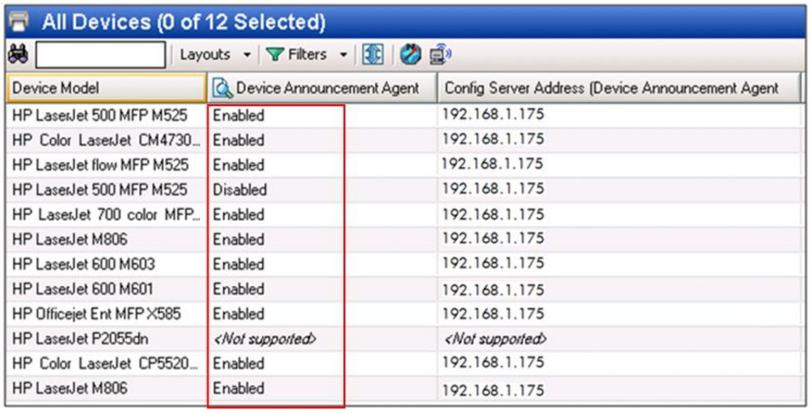
☐ Require Mutual Authentication via certificates

Note: By default no authentication is required between this device and the configuration server. If "Require Mutual Authentication" is selected, this is the most secure configurat
Configuration Server.

For more information about this feature refer to the Configuration Server documentation.

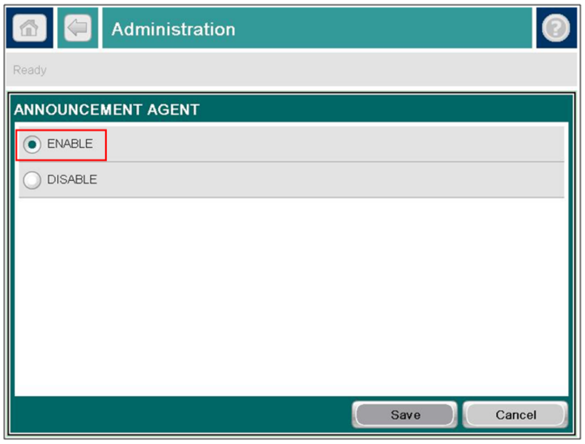
Note : CA certificates installed under the Networking or Security tab will be used to authenticate the remote user.

HP Web Jetadmin provides fleet configuration of the Device Announcement Agent. You can set up a device layout in HP Web Jetadmin to include the Device Announcement Agent column. DAA presence is represented by an **Enabled**, **Disabled** or **Not Supported** status in this column.



Device Model	Device Announcement Agent	Config Server Address (Device Announcement Agent
HP LaserJet 500 MFP M525	Enabled	192.168.1.175
HP Color LaserJet CM4730...	Enabled	192.168.1.175
HP LaserJet flow MFP M525	Enabled	192.168.1.175
HP LaserJet 500 MFP M525	Disabled	192.168.1.175
HP LaserJet 700 color MFP...	Enabled	192.168.1.175
HP LaserJet M806	Enabled	192.168.1.175
HP LaserJet 600 M603	Enabled	192.168.1.175
HP LaserJet 600 M601	Enabled	192.168.1.175
HP Officejet Ent MFP X585	Enabled	192.168.1.175
HP LaserJet P2055dn	<Not supported>	<Not supported>
HP Color LaserJet CP5520...	Enabled	192.168.1.175
HP LaserJet M806	Enabled	192.168.1.175

The device DAA functionality is enabled by default but can be manually disabled via the control panel, Embedded Web Server or HP Web Jetadmin.



ANNOUNCEMENT AGENT

● ENABLE

○ DISABLE

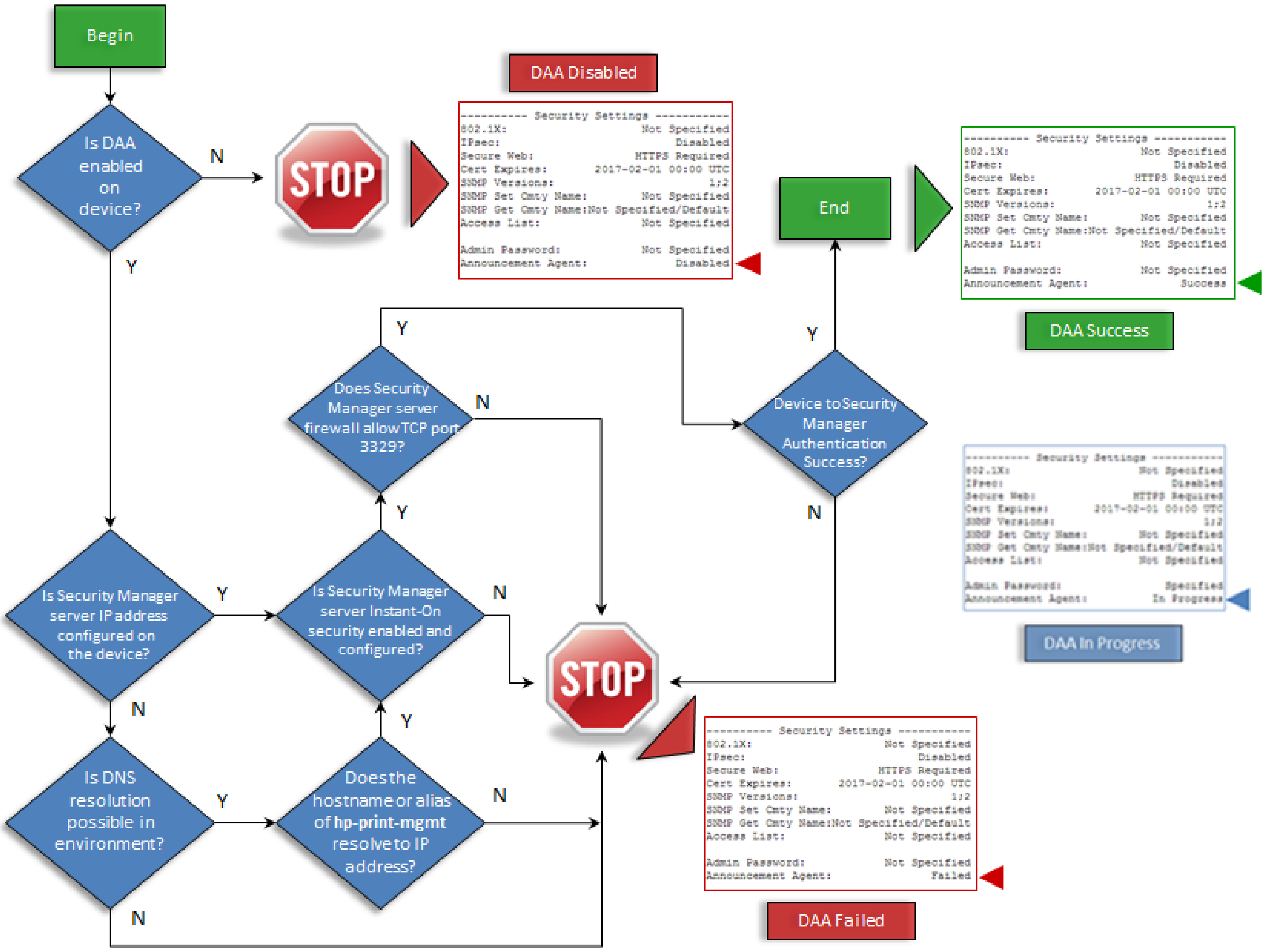
An enabled Device Announcement Agent will announce when the device is powered up on the network for the first time. Announcements also occur during a device power cycle, cold reset, IP address change and link down/link up scenario.

Instant-on workflow

The Device Announcement Agent is enabled by default. The device is capable of displaying four different DAA states; **Disabled**, **In Progress**, **Success** or **Failed**. **Success** indicates the device was able to discover a Security Manager server and establish communication. **Failed** indicates the device wasn't able to discover a Security Manager server or wasn't able to establish a connection with a discovered Security Manager server.   Use the following DAA workflow description and the diagram below to understand the device announcement experience:

1. A supported device is powered up on network with a pre-configured IP address or automatically acquires an IP address after network installation. The DAA is enabled by default on the device, but can easily be disabled if Instant-On Security is not desired. In the disabled scenario, the device will show a **disabled** status for the announcement agent.
2. If the DAA is enabled, and the Security Manager server IP address is configured on the device, the device will target the provided Security Manager server IP address to begin Instant-On communication. If the Security Manager server IP address is not configured on the device, the device will attempt DNS IP resolution of the following hostname or DNS alias (CNAME): **hp-print-mgmt**. Note: This hostname or alias must be administratively assigned to the Security Manager server for successful default Instant-On functionality.
3. The Security Manager server Instant-On feature must be enabled and configured to allow DAA communication to proceed without failure. The Instant-On feature can be configured to discover only or discover, assess and remediate.
4. With the Security Manager server IP address known (either through direct configuration or DNS resolve), TCP port 3329 communication is attempted with the Security Manager server. Device announces itself using SSL and its self-signed identity certificate.
5. Upon receiving the announcement, the Security Manager configuration server authenticates the device, retrieves the device's identity details, and adds the device to the database. Security Manager then continues with an assessment of the device based upon the designated Security Manager security policy and remediates the device's non-compliant security settings.

DAA Workflow Diagram


Begin
Is DAA enabled on device?
N
Y
DAA Disabled
End
DAA Success
Y
Does Security Manager server firewall allow TCP port 3329?
N
Y
Device to Security Manager Authentication Success?
N
Is Security Manager server IP address configured on the device?
Y
Is Security Manager server Instant-On security enabled and configured?
N
N
DAA In Progress
Y
Is DNS resolution possible in environment?
Y
Does the hostname or alias of hp-print-mgmt resolve to IP address?
N
N
DAA Failed

```
----------- Security Settings -----------
802.1X:                        Not Specified
IPsec:                              Disabled
Secure Web:                   HTTPS Required
Cert Expires:           2017-02-01 00:00 UTC
SNMP Versions:                           1;2
SNMP Set Cmty Name:            Not Specified
SNMP Get Cmty Name:Not Specified/Default
Access List:                   Not Specified

Admin Password:                Not Specified
Announcement Agent:                 Disabled
```

```
----------- Security Settings -----------
802.1X:                        Not Specified
IPsec:                              Disabled
Secure Web:                   HTTPS Required
Cert Expires:           2017-02-01 00:00 UTC
SNMP Versions:                           1;2
SNMP Set Cmty Name:            Not Specified
SNMP Get Cmty Name:Not Specified/Default
Access List:                   Not Specified

Admin Password:                Not Specified
Announcement Agent:                  Success
```

```
----------- Security Settings -----------
802.1X:                        Not Specified
IPsec:                              Disabled
Secure Web:                   HTTPS Required
Cert Expires:           2017-02-01 00:00 UTC
SNMP Versions:                           1;2
SNMP Set Cmty Name:            Not Specified
SNMP Get Cmty Name:Not Specified/Default
Access List:                   Not Specified

Admin Password:                    Specified
Announcement Agent:              In Progress
```

```
----------- Security Settings -----------
802.1X:                        Not Specified
IPsec:                              Disabled
Secure Web:                   HTTPS Required
Cert Expires:           2017-02-01 00:00 UTC
SNMP Versions:                           1;2
SNMP Set Cmty Name:            Not Specified
SNMP Get Cmty Name:Not Specified/Default
Access List:                   Not Specified

Admin Password:                Not Specified
Announcement Agent:                   Failed
```

Explanation of the DAA workflow

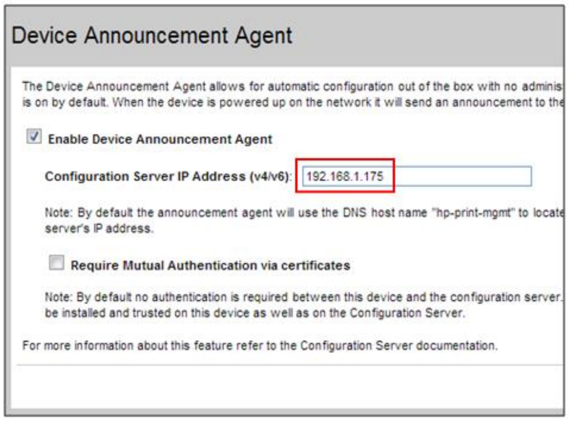
This section presents the Device Announcement Agent workflow in greater detail, including network configuration for default functionality, network activity, primary use cases, communication specifics, and authentication.

Device and DNS configuration

DAA communication occurs via a protocol that will be referred to in this document as HDAP (HP Device Announcement Protocol). When a DAA enabled printer comes online in a networked environment, it follows a process of contacting the default Security Manager server to request discovery and compliance with a configured corporate security policy. All use cases follow the same basic workflow, but differ in the way that the device is authenticated to the Security Manager server and if some manual intervention in the workflow is required.

In order to leverage the default functionality provided by a DAA enabled printer, the network administrator must make a minimal DNS configuration change to the networked environment. Once the configuration change is complete, any Instant-On supported device coming online will be automatically discovered and configured to a secure setting. The required steps are as follows:

1. The DNS administrator configures a DNS entry for the default Security Manager server hostname **hp-print-mgmt** on the network where a new HP print device is to be placed. The **hp-print-mgmt** reference can be the actual Security Manager server hostname or a DNS alias (CNAME) of that specific server. If the administrator is unable or unwilling to configure this DNS entry, the DAA must be manually configured to include the IP address of the Security Manager server. HP Web Jetadmin can assist with the DAA configuration from a fleet management perspective. Pre-configuring the Security Manager server IP address in the DAA eliminates the need for DNS, but adds a manual step to the default Instant-On process.



Device Announcement Agent

The Device Announcement Agent allows for automatic configuration out of the box with no adminis
is on by default. When the device is powered up on the network it will send an announcement to the

☑ Enable Device Announcement Agent

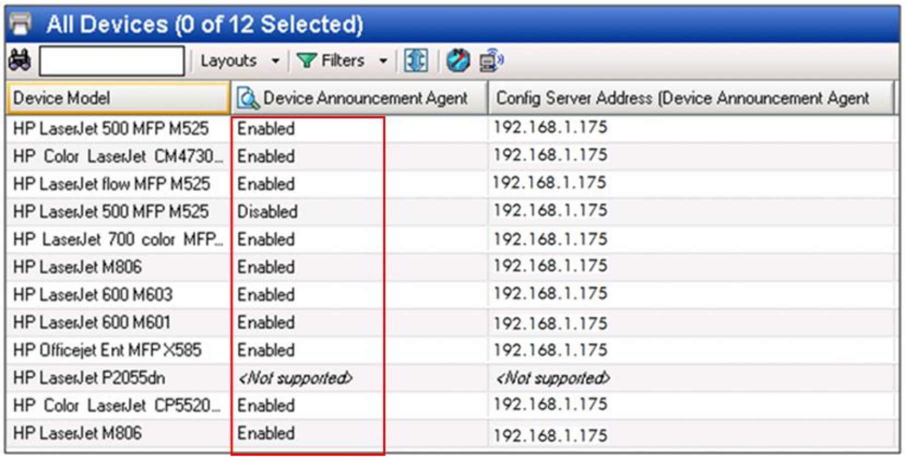
Configuration Server IP Address (v4/v6): 192.168.1.175

Note: By default the announcement agent will use the DNS host name "hp-print-mgmt" to locate
server's IP address.

□ Require Mutual Authentication via certificates

Note: By default no authentication is required between this device and the configuration server.
be installed and trusted on this device as well as on the Configuration Server.

For more information about this feature refer to the Configuration Server documentation.

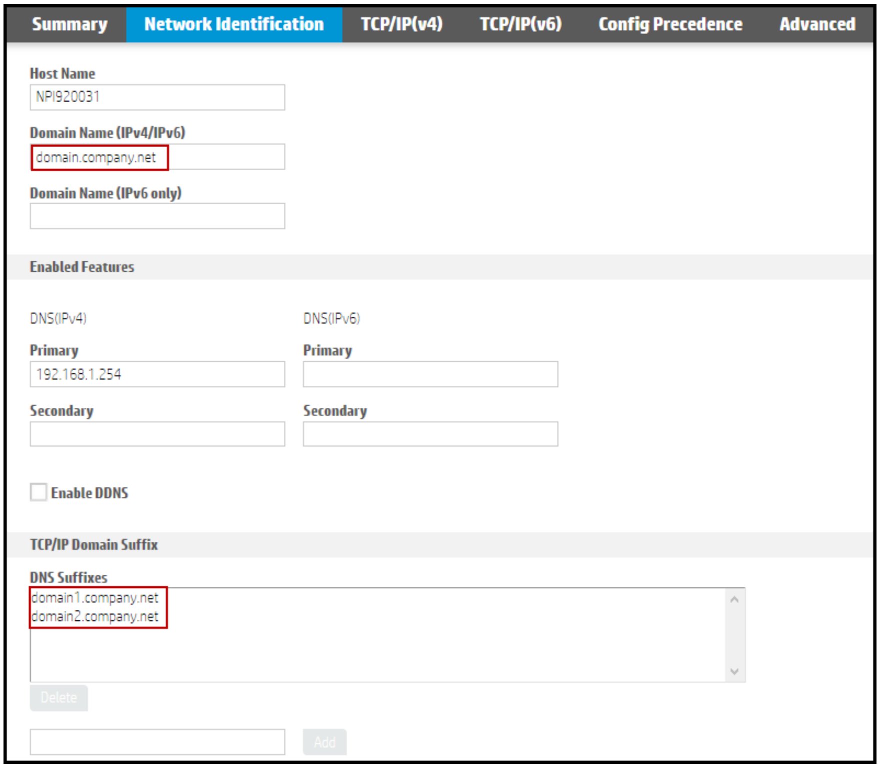


All Devices (0 of 12 Selected)

Device Model	Device Announcement Agent	Config Server Address (Device Announcement Agent
HP LaserJet 500 MFP M525	Enabled	192.168.1.175
HP Color LaserJet CM4730...	Enabled	192.168.1.175
HP LaserJet flow MFP M525	Enabled	192.168.1.175
HP LaserJet 500 MFP M525	Disabled	192.168.1.175
HP LaserJet 700 color MFP...	Enabled	192.168.1.175
HP LaserJet M806	Enabled	192.168.1.175
HP LaserJet 600 M603	Enabled	192.168.1.175
HP LaserJet 600 M601	Enabled	192.168.1.175
HP Officejet Ent MFP X585	Enabled	192.168.1.175
HP LaserJet P2055dn	<Not supported>	<Not supported>
HP Color LaserJet CP5520...	Enabled	192.168.1.175
HP LaserJet M806	Enabled	192.168.1.175

Note: The DAA DNS resolve occurs on the local domain only unless the device is configured to query additional domains or the DNS environment is configured to refer to other domains. The device can be automatically configured with a specific DHCP server option (option 119) that assigns additional domain suffixes or manually configured with the additional domain information via the device's embedded web server. The Microsoft DHCP domain search options differ by server operating system. To understand more about specific server operating system DHCP capabilities and automatic domain search options, please refer to the Microsoft Support Knowledge Base. A network trace example is shown below of DAA behavior when the **hp-print-mgmt**

hostname or DNS alias cannot be found on the local domain and the device searches on other domains for which the network interface may be configured.



Host Name
NPI920031

Domain Name (IPv4/IPv6)
domain.company.net

Domain Name (IPv6 only)

Enabled Features

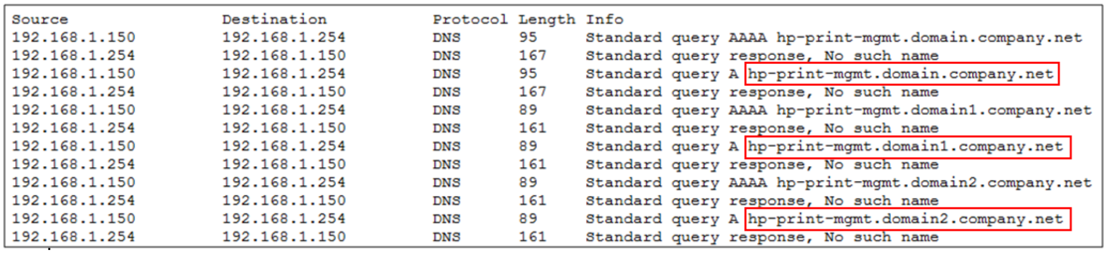
DNS(IPv4)
Primary
192.168.1.254
Secondary

DNS(IPv6)
Primary
Secondary

□ Enable DDNS

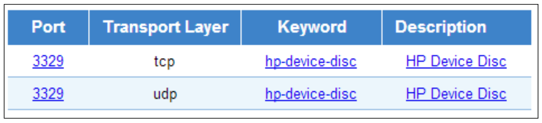
TCP/IP Domain Suffix

DNS Suffixes
domain1.company.net
domain2.company.net


```
Source              Destination         Protocol Length Info
192.168.1.150       192.168.1.254       DNS      95     Standard query AAAA hp-print-mgmt.domain.company.net
192.168.1.254       192.168.1.150       DNS      167    Standard query response, No such name
192.168.1.150       192.168.1.254       DNS      95     Standard query A hp-print-mgmt.domain.company.net
192.168.1.254       192.168.1.150       DNS      167    Standard query response, No such name
192.168.1.150       192.168.1.254       DNS      89     Standard query AAAA hp-print-mgmt.domain1.company.net
192.168.1.254       192.168.1.150       DNS      161    Standard query response, No such name
192.168.1.150       192.168.1.254       DNS      89     Standard query A hp-print-mgmt.domain1.company.net
192.168.1.254       192.168.1.150       DNS      161    Standard query response, No such name
192.168.1.150       192.168.1.254       DNS      89     Standard query AAAA hp-print-mgmt.domain2.company.net
192.168.1.254       192.168.1.150       DNS      161    Standard query response, No such name
192.168.1.150       192.168.1.254       DNS      89     Standard query A hp-print-mgmt.domain2.company.net
192.168.1.254       192.168.1.150       DNS      161    Standard query response, No such name
```

Note: When IPv6 is enabled on the device, you will notice at least one IPv6 (AAAA) and IPv4(A) DNS request per domain.

2. TCP Port 3329 is registered with the IANA (Internet Assigned Numbers Authority) and specifically assigned to HP Security Manager. This port is dedicated to Instant-On communication between the HP supported device and Security Manager. Port 3329 is also referred to as the **hp-device-disc** port. If the Security Manager server Windows firewall is in use, ensure the firewall allows TCP Port 3329 communication in both directions.



Port	Transport Layer	Keyword	Description
3329	tcp	hp-device-disc	HP Device Disc
3329	udp	hp-device-disc	HP Device Disc

3. At the Security Manager server, create a security policy that best describes the conformance requirements for devices on this network. This policy should be the most encompassing policy relative to the mix of device models found in your corporate printing environment.

4. At the Security Manager server, configure authentication requirements for communicating with devices. Devices will attempt the highest level of authentication available. Choices are “No

Authentication" (true out-of-the box conditions) or "Mutual Authentication" which leverages installed certificates.

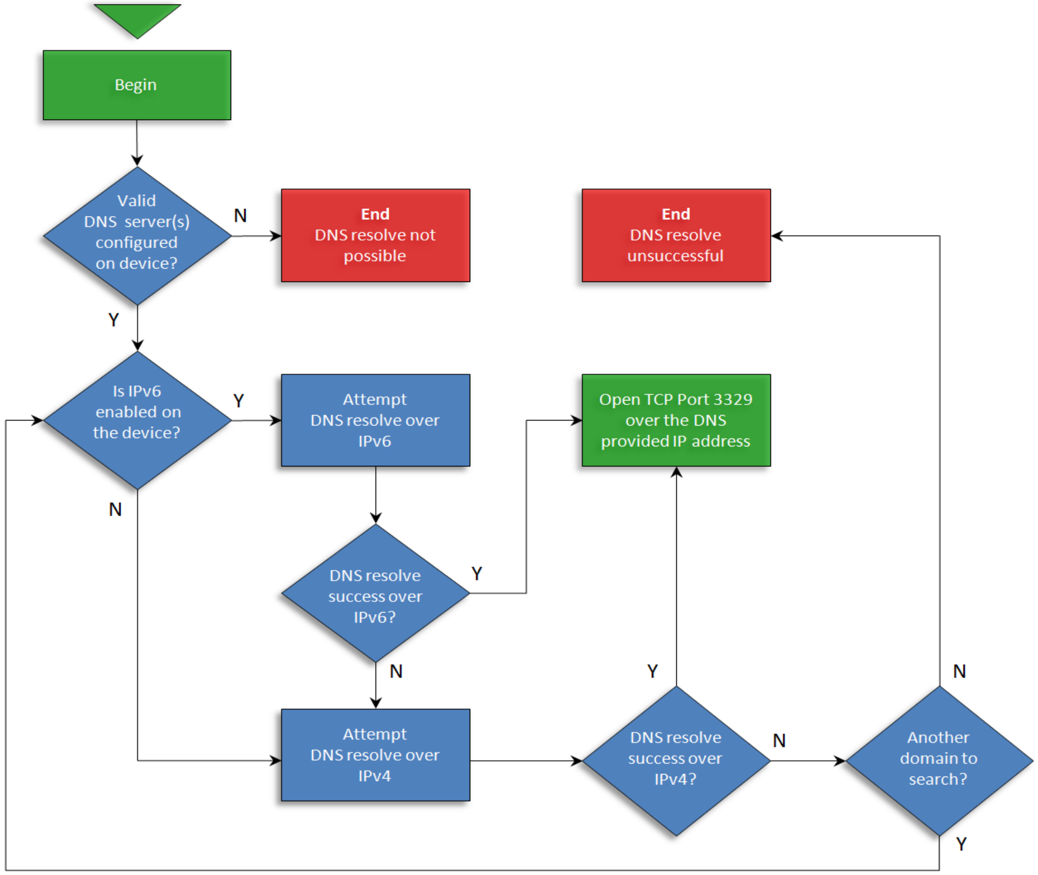
5. Place a device which supports the DAA and is enabled, on the network.

Network Activity

Instant-On security operates with very little impact to the network. As mentioned earlier in this document, the Device Announcement process consists of resolving the Security Manager server hostname or alias of **hp-print-mgmt** to an IP address. Once the address is resolved, a dedicated TCP port (3329) is opened for direct communication between the device and Security Manager. For a detailed flow of what to expect to see on the network, please see the DNS flow diagram below.

Note: If the Security Manager IP address is pre-configured in the DAA, the DNS resolve step in the Instant-On Security process is eliminated.

Resolving the **hp-print-mgmt** hostname or alias:


Begin
Valid DNS server(s) configured on device?
N
End DNS resolve not possible
End DNS resolve unsuccessful
Y
Is IPv6 enabled on the device?
Y
Attempt DNS resolve over IPv6
Open TCP Port 3329 over the DNS provided IP address
N
DNS resolve success over IPv6?
Y
N
Attempt DNS resolve over IPv4
Y
DNS resolve success over IPv4?
N
N
Another domain to search?
Y

Successful DNS resolution of the hp-print-mgmt hostname or alias (IPv6 Enabled)

The trace below is an example of a successful DNS resolution of the default hostname of **hp-print-mgmt.domain.company.net**. After an unsuccessful attempt at DNS resolve over IPv6, the device retried over IPv4. Once the hostname resolved to an IP address, the device then opened up a TCP connection on port 3329. This connection then serves as secure communication between Security Manager and the device.

Note: IPv6 is enabled by default on the device

Packet 1

```
Source          Destination     Protocol  Length   Info
192.168.1.150   192.168.1.254     DNS       94    Standard query AAAA hp-print-mgmt.domain.company.net

Domain Name System (query)
   Questions: 1
   Answer RRs: 0
   Authority RRs: 0
   Additional RRs: 0
Queries
   hp-print-mgmt.domain.company.net: type AAAA, class IN
   Name: hp-print-mgmt.domain.company.net
   Type: AAAA (IPv6 address)
```

Packet 1 is the 1st DNS query from an Instant-On supported device to the DNS server attempting to resolve the hostname of hp-print-mgmt.domain.company.net over IPv6.

Packet 2

```
Source          Destination     Protocol  Length   Info
192.168.1.254   192.168.1.150     DNS      122    Standard query response AAAA

Domain Name System (response)
   Questions: 1
   Answer RRs: 1
   Authority RRs: 0
   Additional RRs: 0
Answers
   hp-print-mgmt.domain.company.net: type AAAA, class IN, addr
   Name: hp-print-mgmt.domain.company.net
   Type: AAAA (IPv6 address)
   Addr:
```

Packet 2 is the DNS response from the DNS server back to the Instant-On supported device. The specific hostname is not resolved to an IP address over IPv6; no answer is provided.

Packet 3

```
Source          Destination     Protocol  Length        Info
192.168.1.150   192.168.1.254     DNS       94    Standard query A hp-print-mgmt.domain.company.net

Domain Name System (query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
Queries
    hp-print-mgmt.domain.company.net: type A, class IN
    Name: hp-print-mgmt.domain.company.net
    Type: A (Host address)
```

Packet 3 displays a 2nd DNS query from the Instant-On supported device to the DNS server attempting to resolve the hostname of hp-print-mgmt.domain.company.net over IPv4.

Packet 4

```
Source          Destination     Protocol  Length        Info
192.168.1.254   192.168.1.150     DNS      110    Standard query response A 192.168.1.175

Domain Name System (response)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
Answers
    hp-print-mgmt.domain.company.net: type A, class IN, addr 192.168.1.175
    Name: hp-print-mgmt.domain.company.net
    Type: A (Host address)
    Addr: 192.168.1.175 (192.168.1.175)
```

Packet 4 is the DNS response from the DNS server back to the Instant-On supported device. The specific hostname is resolved to an IPv4 IP address of 192.168.1.175.

Packet 5

```
Source          Destination     Protocol  Length              Info
192.168.1.150   192.168.1.175     TCP       62    iniserve-port > hp-device-disc [SYN] Seq=0 Win=1460 Len=0 MSS=1460 WS=1

Transmission Control Protocol, Src Port: iniserve-port (3560), Dst Port: hp-device-disc (3329), Seq: 0, Len: 0
    Source port: iniserve-port (3560)
    Destination port: hp-device-disc (3329)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
    Flags: 0x02 (SYN)
    Window size value: 1460
```

Packet 5 is the request from the device to open a TCP connection on port 3329 after receiving the IPSC server IP address (192.168.1.175) from the DNS server.

Packet 6

```
Source          Destination     Protocol  Length              Info
192.168.1.175   192.168.1.150     TCP       62    hp-device-disc > iniserve-port [SYN, ACK] Seq=0 Ack=1

Transmission Control Protocol, Src Port: hp-device-disc (3329), Dst Port: iniserve-port (3560), Seq: 0, Ack: 1, Len: 0
    Source port: hp-device-disc (3329)
    Destination port: iniserve-port (3560)
    Sequence number: 0
    Acknowledgement number: 1    (relative ack number)
    Flags: 0x12 (SYN, ACK)
    Window size value: 8192
```

Packet 6 is the response from the IPSC server "acknowledging" the port open request from the device. Communication is now established over TCP port 3329.

Initial Device Announcement Use Cases

Setting up the network as explained above will allow for an initial default out-of-the-box device security configuration experience. Below, is a list of the most common Secure at Install use cases.

Use Case 1 – Auto Discovery and Policy Conformance

A DAA enabled Security Manager supported device is placed on the network for the first time without any staged configuration. The Security Manager server Instant-On feature is configured to "Accept Device

Announcements" and "Allow Automatic Remediation". The device acquires a DHCP address and attempts to resolve the DNS hostname or alias of **hp-print-mgmt**. Once **hp-print-mgmt** is resolved to the HP Security Manager server IP address, the device is authenticated and Security Manager communication is established. Security Manager places the newly discovered device in the database, assigns a license, and remediates the device in accordance with the established security policy. In this popular use case, a new device when added to the network will be automatically discovered, licensed, assessed, remediated and verified by Security Manager.

Use Case 2 – Semi-Auto Discovery and Policy Conformance

A DAA enabled Security Manager supported device is placed on the network and manually configured with the IP address of the designated Security Manager server. The Security Manager server Instant-On feature is configured to "Accept Device Announcements" and "Allow Automatic Remediation". The device acquires a DHCP address and establishes direct communication with the Security Manager server. Once authenticated, Security Manager places the newly discovered device in the database, assigns a license, and remediates the device in accordance with the established security policy. This use case allows Instant-On functionality without DNS resolve. The trade-off; IT DNS configuration is not required, but device pre-configuration is.

Use Case 3 – Pre-staged Device Discovery and Policy Conformance

A DAA enabled Security Manager supported device is staged and placed on the network in a pre-configured state. This pre-configured state may include an installed mutual authentication certificate and applied security settings. The device is manually configured with the IP address of the designated Security Manager server. The Security Manager server Instant-On feature is configured to "Accept Device Announcements" and "Allow Automatic Remediation". After communication is established and authentication complete, the newly discovered device is placed in the database. A license is assigned, and remediation occurs for any security setting not in compliance with the applied security policy. This use case ensures all the pre-configured new devices are discovered, mutually authenticated through certificates and match security settings with the established security policy.

Use Case 4 – Filtered Discovery and Policy Conformance

A DAA enabled Security Manager supported device is placed on the network without any staged configuration. The Security Manager server Instant-On feature is configured to "Accept Device Announcements", "Allow Automatic Remediation" and utilize device serial numbers as a method of filtering Instant-On activity. The device acquires a DHCP address and attempts to resolve the DNS hostname or alias of **hp-print-mgmt**. Once **hp-print-mgmt** is resolved to the Security Manager server IP address and Security Manager communication is established, Security Manager continues the Instant-On process only if the device matches a serial number entry in the Security Manager Instant-On serial number list. If so, Security Manager places the newly discovered device in the database, assigns a license, and remediates the device in accordance with the established security policy. Upon successful interaction, the serial number is then removed from the UI list, but the database entry remains in order to continue the serial number filtering process for Instant-On. This use case provides a filtering option for selective Instant-On processing.

When are Device Announcement Messages Created?

.Many HP devices support a featured called a Device Announcement Agent whereby announcement packets are sent to Security Manager whenever any of the following condition exist on the device:

- Initial boot
- Power cycle
- Network disconnect/reconnect

- IP Address change
- Hostname change
- Cold Reset
- Every 47~48 hours regardless of any other action triggering an announcement. This is not configurable and only available from FutureSmart 4 onwards.

Post-Install Device Announcement Use Cases

After the Secure at Install process is complete, Instant-On security continues with the Stay Secure process via the DAA announcements that occur for device cold resets, IP address changes and other device specific conditions that might place the device in a non-compliant state. After receiving an announcement, Instant-On ensures the device is assessed and remediated in accordance with the last security policy applied. Below, is a list of the most common Stay Secure use cases.

Use Case 1 – Device Cold Reset

A Security Manager managed device has experienced a condition where a return to a default configuration (cold reset) is required. As a result of the cold reset, many of the security settings applied through the original Security Manager policy remediation are cleared. The cold reset action produces a DAA announcement, thus prompting communication with Security Manager. The Security Manager server processes the announcement, matches device identity with the existing database entry, and applies the last policy the device was assessed with. The device database entry is reconciled with any device identity attributes that might have changed during the cold reset. Through this process, the device is immediately placed back into its secure state.

Use Case 2 – Device Formatter or JetDirect Interface Replacement

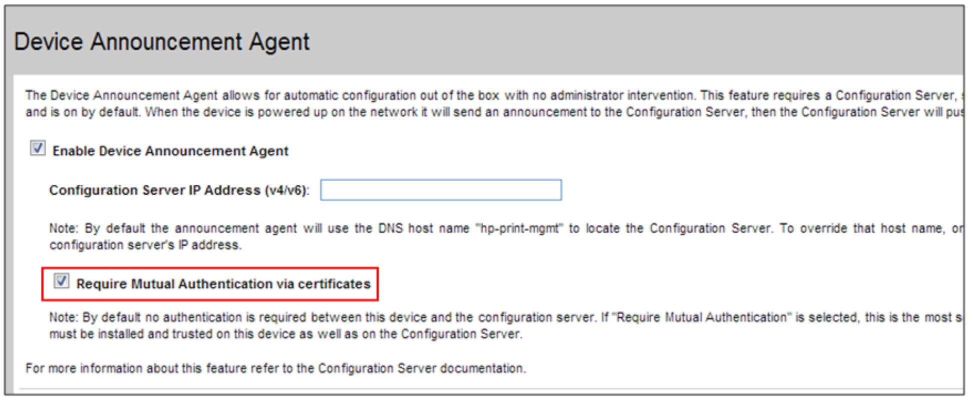
A Security Manager managed device has experienced a hardware failure, requiring a Formatter or Jetdirect interface replacement. After completing the repair, the service technician reloads the original serial number into the device. Applying power to the device after placing unit back on the network generates a DAA announcement. The Security Manager server processes this announcement, reconciles the device identity based on the serial number match and applies the last policy the device was assessed with. Through this process, the device is immediately placed back into its secure state.

Use Case 3 – Device Acquires New IP address

Device has moved physical locations and acquires a new IP address. The IP address change produces a DAA announcement, thus prompting communication with Security Manager. The Security Manager server processes the announcement, matches device identity with the existing database entry, and applies the last policy the device was assessed with. The device database entry is reconciled with any device identity attributes that might have changed as a result of the IP address change.

Security and Mutual Authentication

Once the Security Manager server IP address has been acquired, the DAA attempts to open up communication using the most secure authentication method configured on the device. No authentication is the default state. **Require Mutual Authentication via Certificates** will provide the most secure configuration method, since certificates must be installed and trusted on this device as well as on the Security Manager server.



Device Announcement Agent

The Device Announcement Agent allows for automatic configuration out of the box with no administrator intervention. This feature requires a Configuration Server,
and is on by default. When the device is powered up on the network it will send an announcement to the Configuration Server, then the Configuration Server will pus

☑ Enable Device Announcement Agent

Configuration Server IP Address (v4/v6):

Note: By default the announcement agent will use the DNS host name "hp-print-mgmt" to locate the Configuration Server. To override that host name, or
configuration server's IP address.

☑ Require Mutual Authentication via certificates

Note: By default no authentication is required between this device and the configuration server. If "Require Mutual Authentication" is selected, this is the most s
must be installed and trusted on this device as well as on the Configuration Server.

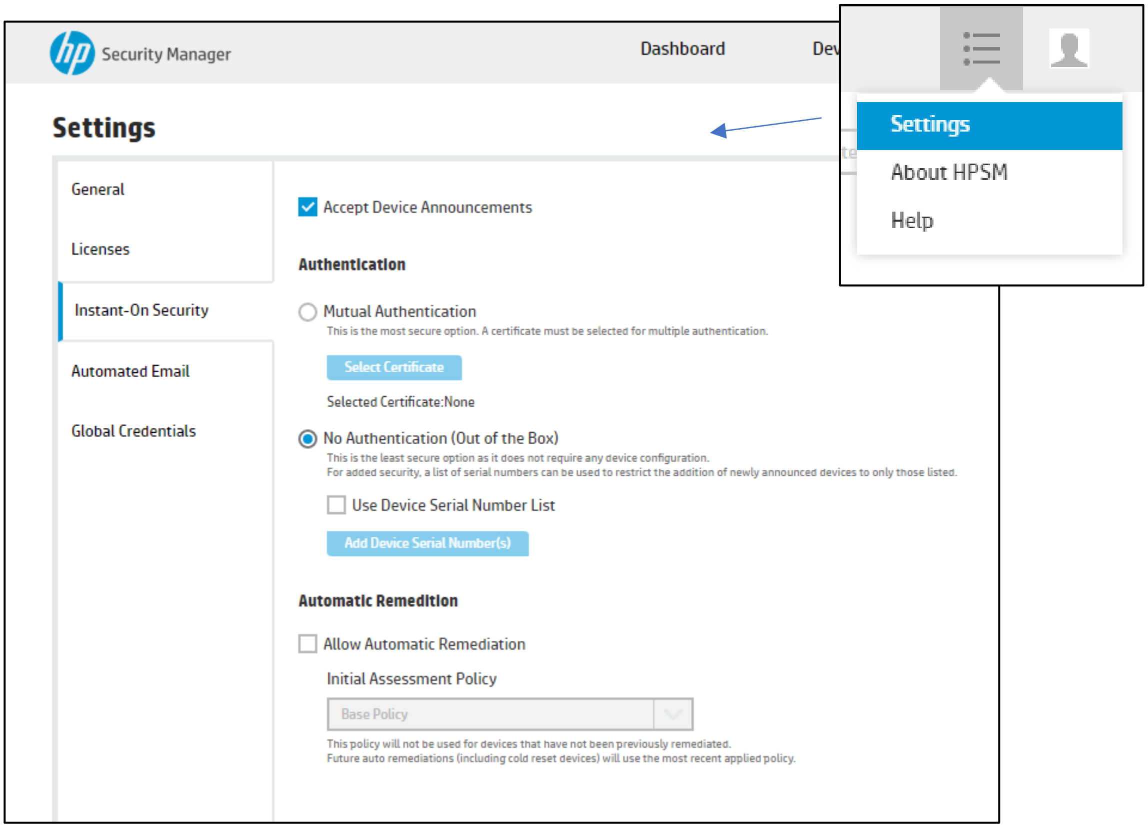
For more information about this feature refer to the Configuration Server documentation.

When **Require Mutual Authentication via Certificates** is enabled, announcements are sent using trusted SSL/TLS authentication. If certificate authentication is enabled, but fails authentication for any reason, Instant-On communication ceases and an announcement agent failure is posted. If certificates are configured on the device, but **Require Mutual Authentication via Certificates** is disabled, trusted SSL/TLS authentication is still attempted. However, the DAA allows the SSL/TLS connection to proceed after authentication fails. Security Manager may close the SSL/TLS connection as a result of failing to validate the device certificate. This decision is determined by the device announcement security policy on the Security Manager server. For more information on use of certificates with the Instant-On Security feature, please refer to Mutual Authentication in Part 2 of this document.

Instant-On Security, Part 2 - Security Manager Instant-On Security Settings

Introduction

As mentioned in Part 1, Security Manager Instant-On Security is a dual component solution. The first component is the Device Announcement Agent (DAA), explained in Part 1. The secondary component is the Security Manager server itself, configured for Instant-On functionality. This host component will be referred to as the Instant-On Configuration Server throughout the remainder of this document. When Security Manager is enabled as the Instant-On Configuration Server, it becomes the discovery and configuration server for the supported devices that are able to announce themselves through the Device Announcement Agent. Unlike the Device Announcement Agent, the Instant-On Configuration Server is <u>not</u> enabled by default. Automatic remediations by default are not checked.



Settings

☑ Accept Device Announcements

Authentication

○ Mutual Authentication
This is the most secure option. A certificate must be selected for multiple authentication.

Select Certificate

Selected Certificate:None

● No Authentication (Out of the Box)
This is the least secure option as it does not require any device configuration.
For added security, a list of serial numbers can be used to restrict the addition of newly announced devices to only those listed.

□ Use Device Serial Number List

Add Device Serial Number(s)

Automatic Remedition

□ Allow Automatic Remediation

Initial Assessment Policy

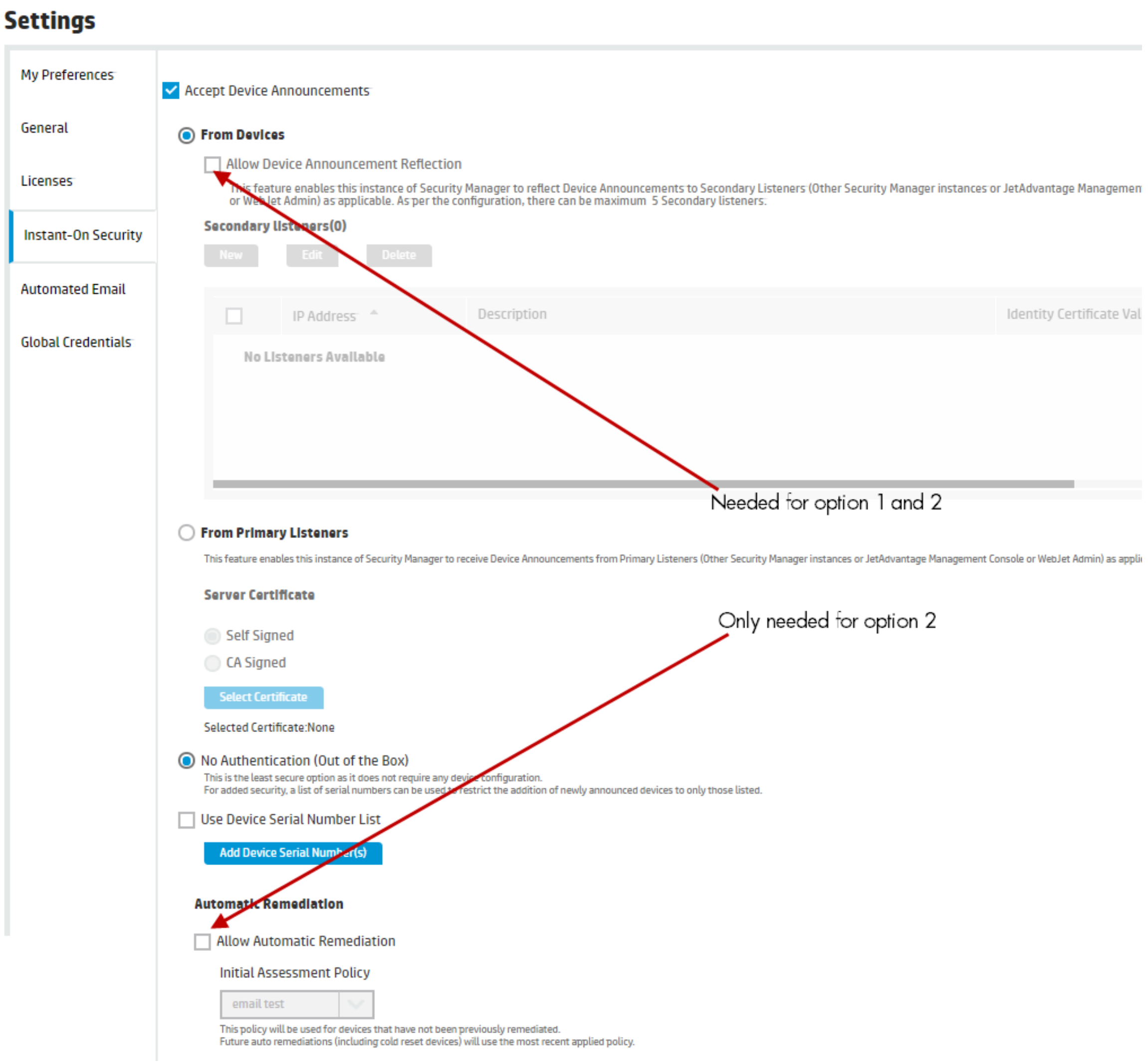
Base Policy

This policy will not be used for devices that have not been previously remediated.
Future auto remediations (including cold reset devices) will use the most recent applied policy.

The configuration options under Instant-On Security can be configured in two different options: enable discovery of devices via instant-on or enable instant-on Security.

Enabling Instant-on Discovery

Option 1 is discovery only of DAA supported devices by selecting **Accept Device Announcements** without selecting **Allow Automatic Remediation**. Upon receiving the device announcement, Security Manager will establish communication with the device, place the device in the database and assign it a license. It will not attempt to apply the configured security policy. This option does not provide Instant-On Security, only discovery through the device announcement agent.



☑ Accept Device Announcements

● **From Devices**

□ Allow Device Announcement Reflection

This feature enables this instance of Security Manager to reflect Device Announcements to Secondary Listeners (Other Security Manager instances or JetAdvantage Managemen or WebJet Admin) as applicable. As per the configuration, there can be maximum 5 Secondary listeners.

Secondary listeners(0)

□	IP Address	Description	Identity Certificate Val
	No Listeners Available		

Needed for option 1 and 2

○ **From Primary Listeners**

This feature enables this instance of Security Manager to receive Device Announcements from Primary Listeners (Other Security Manager instances or JetAdvantage Management Console or WebJet Admin) as appli

Server Certificate

○ Self Signed

○ CA Signed

Selected Certificate:None

Only needed for option 2

● No Authentication (Out of the Box)

This is the least secure option as it does not require any device configuration.
For added security, a list of serial numbers can be used to restrict the addition of newly announced devices to only those listed.

□ Use Device Serial Number List

Automatic Remediation

□ Allow Automatic Remediation

Initial Assessment Policy

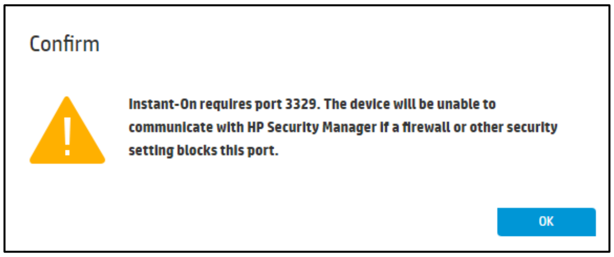
email test

This policy will be used for devices that have not been previously remediated.
Future auto remediations (including cold reset devices) will use the most recent applied policy.

Enabling Instant-On Security

Option 2 is the selection of Accept Device Announcements and Allow Automatic Remediation with an Initial Assessment Policy. This combined selection will discover the DAA enabled device and apply the security policy that appears in the Initial Assessment Policy field. This combination provides Instant-On Security.

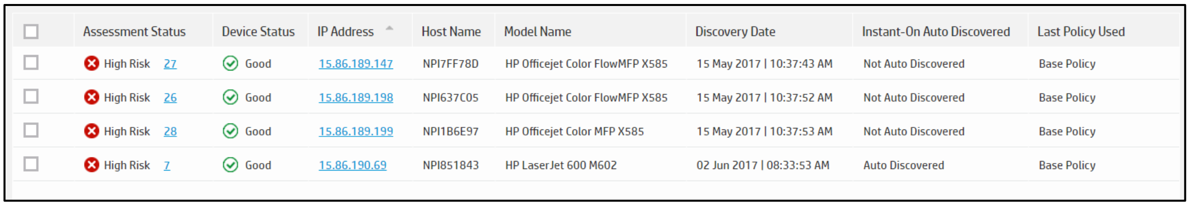
To enable listening to device announcements the **Accept Device Announcements** box must be selected. After selecting **Accept Device Announcements**, a pop-up notification provides a reminder to ensure TCP port 3329 is not blocked at the firewall.



Confirm

Instant-On requires port 3329. The device will be unable to communicate with HP Security Manager if a firewall or other security setting blocks this port.

An Instant-On discovered device appears in the device list as Auto Discovered under the Instant On Auto Discovered column, and the Last Policy Used column indicates which policy was used for automatic remediation if enabled.

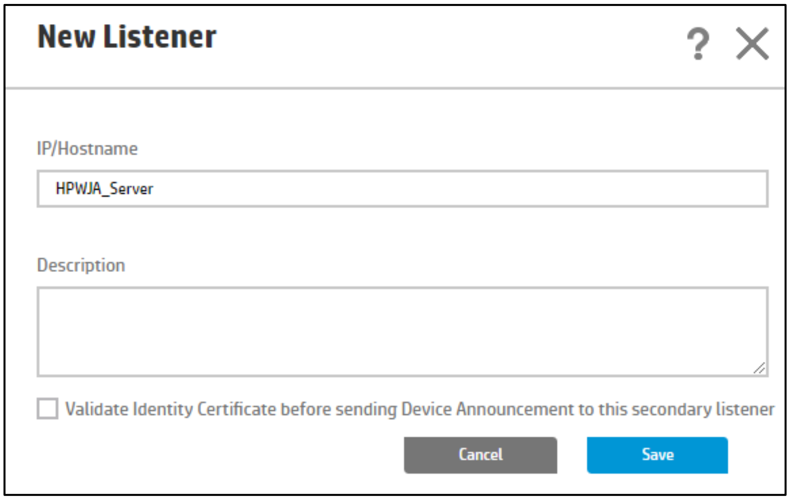


☐	Assessment Status	Device Status	IP Address	Host Name	Model Name	Discovery Date	Instant-On Auto Discovered	Last Policy Used
☐	✖ High Risk 27	✓ Good	15.86.189.147	NPI7FF78D	HP Officejet Color FlowMFP X585	15 May 2017 | 10:37:43 AM	Not Auto Discovered	Base Policy
☐	✖ High Risk 26	✓ Good	15.86.189.198	NPI637C05	HP Officejet Color FlowMFP X585	15 May 2017 | 10:37:52 AM	Not Auto Discovered	Base Policy
☐	✖ High Risk 28	✓ Good	15.86.189.199	NPI1B6E97	HP Officejet Color MFP X585	15 May 2017 | 10:37:53 AM	Not Auto Discovered	Base Policy
☐	✖ High Risk 7	✓ Good	15.86.190.69	NPI851843	HP LaserJet 600 M602	02 Jun 2017 | 08:33:53 AM	Auto Discovered	Base Policy

The default Instant-On Security configuration will accept and process discovery and policy requests from every device capable of announcing itself through the device announcement agent. This default configuration does not include the selection of trusted certificate based mutual authentication or serial number filtering of devices and is configured as such to accommodate a true out-of-the-box device security experience.

Configuring Instant On Forwarding to WJA

Devices discovered via Instant On can be shared with other Security Manager installations or Web Jetadmin installations by adding them as Secondary Listeners. Click **New** under the **Secondary Listeners** section and add hostnames or IP Addresses of all Security Manager and Web Jetadmin installations where it is desired to share the Instant On discoverd devices.   Check the box named **Validate Identity Certificate before sending Device Announcements to this Secondary Listener** if it is desired to enforce trust through identity certificates to be certain the secondary listener is who it says it is.



New Listener

IP/Hostname

HPWJA_Server

Description

☐ Validate Identity Certificate before sending Device Announcement to this secondary listener

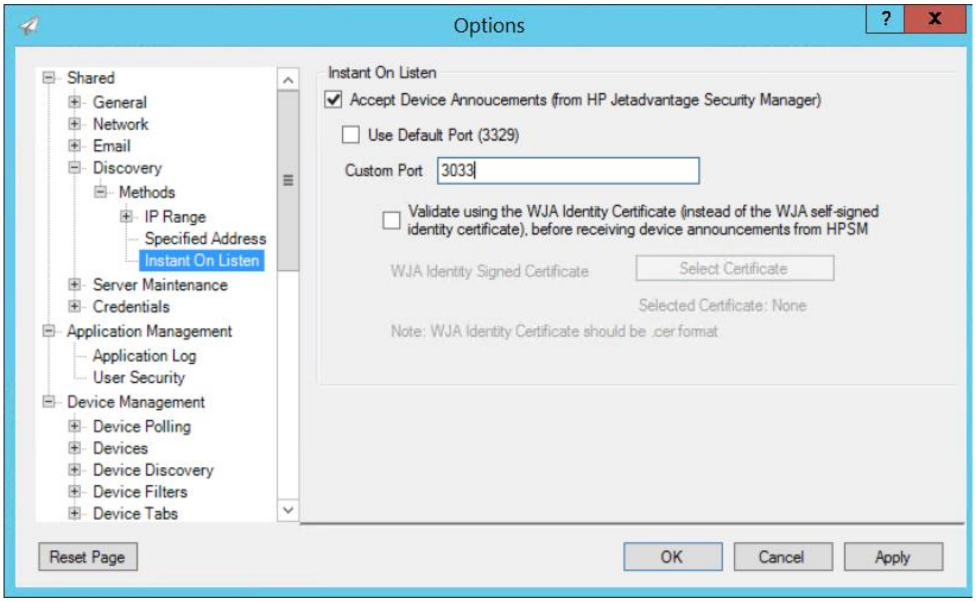
In order for Web Jetadmin to receive the Instant On discovered devices sent to it from a primary Security Manager listener server, check the box to Accept Device Announcements from HP JetAdvantage Security Manager under **Tools, Options, Instant On Listen** in HP Web Jetadmin. Web Jetadmin listens by default on port 3329 for device announcements sent to it from a primary Security Manager listener server and adds those devices to its device list. If you select a custom port in WJA (see screenshot below), you will also have to configure a custom port in HPSM. This can be done in the HPSM_Service.exe.config. Search for the secondary Listener and make changes similar to the following example:

```
<SecondaryListeners>
    <InstantOnPortMapping>
      <Mapping ipOrHostname=”WJASERVER" port="3033"/>
    </InstantOnPortMapping>
```

```
  </SecondaryListeners>
```

After making the changes, you will have to restart the HPSM Jetadvantage service.

The transaction between the primary listener (HPSM) and secondary listener (WJA) will be encrypted using the self-signed certificate in Web Jetadmin.   If it is desired to enforce trust so Security Manager can ensure the Web Jetadmin server is truly who it says it is via a certificate authority, check the box to **Validate using the WJA Identity Certificate**.



Instant On Listen

☑ Accept Device Annoucements (from HP Jetadvantage Security Manager)

□ Use Default Port (3329)

Custom Port 3033

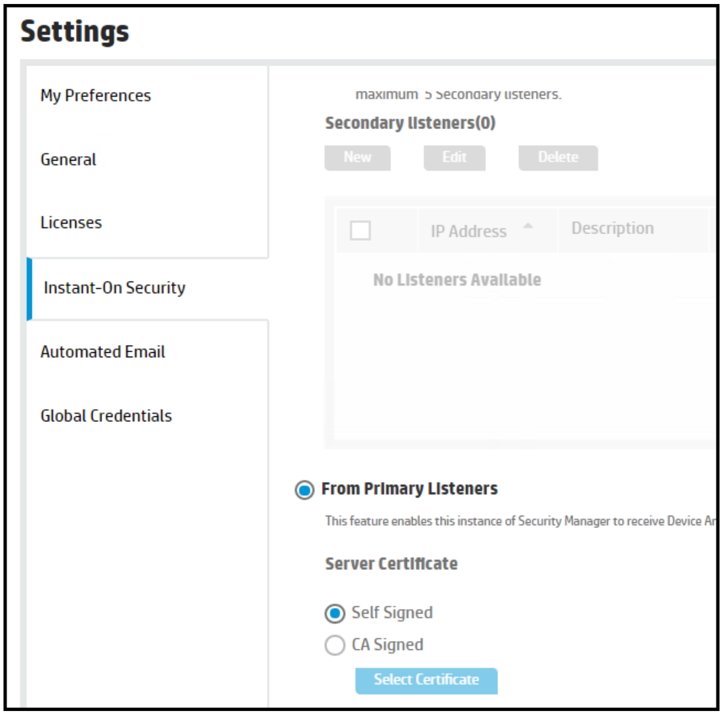
□ Validate using the WJA Identity Certificate (instead of the WJA self-signed identity certificate), before receiving device announcements from HPSM

WJA Identity Signed Certificate   Select Certificate

Selected Certificate: None

Note: WJA Identity Certificate should be .cer format

If it is desired to allow a second Security Manager receive Instant On discovered devices by a primary Security Manager listener server, check the box named **From Primary Listeners**. Choose whether just encryption will be used for the transaction via a self-signed certificate or whether trust should be enforced via a CA signed identity certificate.



maximum 5 secondary listeners.

Secondary listeners(0)

□	IP Address	Description
No Listeners Available		

● From Primary Listeners

This feature enables this instance of Security Manager to receive Device A

Server Certificate

● Self Signed

○ CA Signed

Configuring Instant On Mutual Authentication

Instant-On Security configuration options are available to filter device “Instant-On” participation. Selecting **Mutual Authentication** leverages installed trusted certificates to establish a higher level of Instant-On connection and communication security. When selected and configured, only the devices that complete device identity certificate validation can participate in the Instant-On process.

As mentioned in Part 1, HP supported devices now have the capability of announcing their presence on the network. This device capability is enabled by default. The Device Announcement Agent sends an **Announcement Message** request directly to the Instant-On Configuration Server to announce its presence. This is not a broadcasted message. The device automatically receives the Security Manager server IP address through resolving the DNS hostname of **hp-print-mgmt** or through manual configuration of the Device Announcement Agent IP address field. The **Announcement Acknowledge** reply from the Instant-On Configuration Server acknowledges receipt of the message and returns the status of the attempted authentication method.

Instant-On Security can be configured for mutual authentication; an announcement option that relies upon device and Security Manager identity assurance through a combined action of client-to-server and server-to-client SSL/TLS (Secure Socket Layer/Transport Layer Security) authentication. Mutual authentication can also be informally referred to as 2-way SSL/TLS authentication.

Deploying trusted certificates for mutual authentication provides the most secure method of Instant-On Security. Since certificates remain over a cold reset, this method of Instant-On Security protects the device even if it is cold reset. Successful mutual authentication requires the configuration and installation of a valid identity (ID) certificate on the device and in Security Manager. On the device, the unique identity certificate must be signed by a CA (Certificate Authority) and installed as a replacement of the default self-signed device certificate. On the Security Manager server, a unique identity certificate signed by a (CA) and placed in the local computer personal store is also required. The corresponding (CA) certificate must also be installed on the device (See Figure 26) and in the Security Manager server local computer trusted root certification authorities store. Using a single (CA) to sign both identity certificates isn't required, but can simplify the process by reducing the number of necessary components. Certificates can be configured manually, or a certificate manager can be used.

Handshake

When mutual authentication is configured for Instant-On communication, appropriate handshaking occurs to establish an encrypted channel prior to any message exchanges. The handshake includes dialogue to establish the identities of the device and Security Manager via the mutual presentation of signed digital certificates. The dialogue is similar to the example below:

- Client sends a message proposing the SSL/TLS options
- Server responds with SSL/TLS option selection
- Server presents its identity certificate
- Server requests client's certificate
- Server negotiation is complete
- Client presents its identity certificate
- Client sends key (encrypted with server's public key)
- Client notifies server that it owns the sent certificate
- Client sends message activating the negotiated options
- Client sends "finished" message, asking server to check negotiated options
- Server sends message activating the negotiated options
- Server sends "finished" message, asking client to check negotiated options

Authentication

Authenticating the server consists of "checks" that include:

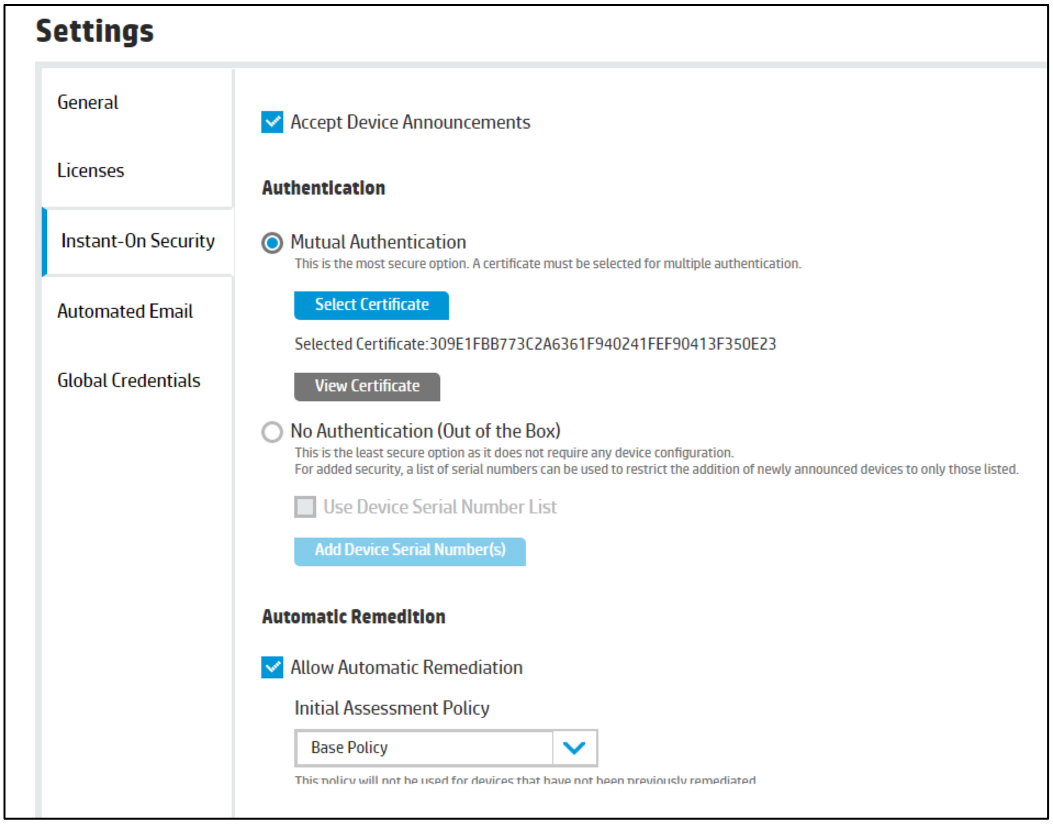
- Has the server certificate expired or been revoked?
- Can the CA (Certificate Authority) that issued the certificate, be trusted?
- Does the CA's public key validate the digital signature?
- Does the domain name in the certificate match the domain name of the server?

Authenticating the client consists of "checks" that include:

- Does the client public key validate the client digital signature?
- Has the client certificate expired or been revoked?
- Can the CA (Certificate Authority) that issued the certificate, be trusted?
- Does the CA's public key validate the digital signature?

Certificate Selection

The figure below provides the Security Manager example of how to invoke Mutual Authentication and select the appropriate certificate. The figure below also provides the device embedded web server example of where and how to install a JetDirect and CA certificate.



☑ Accept Device Announcements

Authentication

● Mutual Authentication
This is the most secure option. A certificate must be selected for multiple authentication.

Selected Certificate:309E1FBB773C2A6361F940241FEF90413F350E23

○ No Authentication (Out of the Box)
This is the least secure option as it does not require any device configuration.
For added security, a list of serial numbers can be used to restrict the addition of newly announced devices to only those listed.

□ Use Device Serial Number List

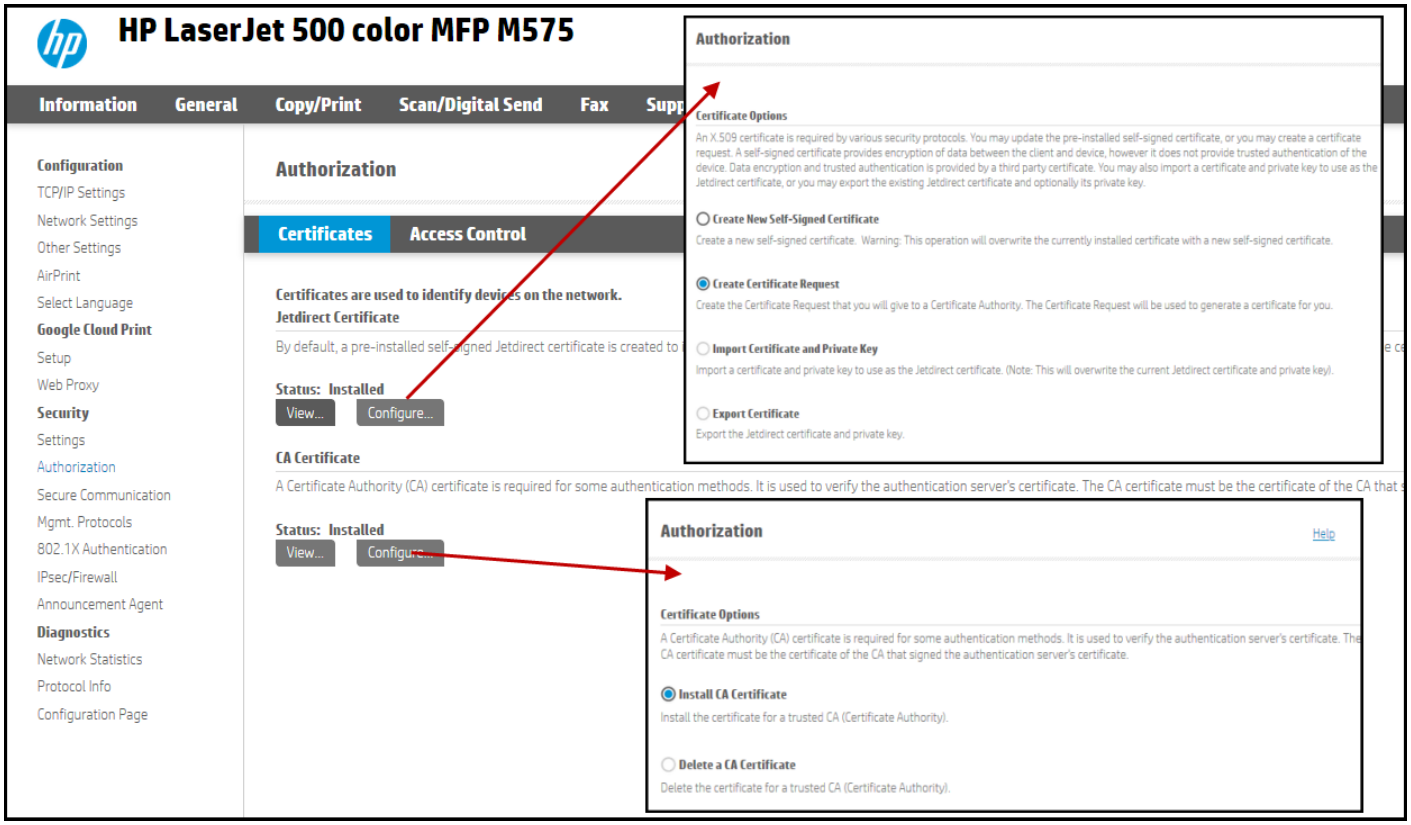
Automatic Remediation

☑ Allow Automatic Remediation

Initial Assessment Policy

Base Policy

This policy will not be used for devices that have not been previously remediated



Authorization

Certificates are used to identify devices on the network.

Jetdirect Certificate

By default, a pre-installed self-signed Jetdirect certificate is created to

Status: Installed

CA Certificate

A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that s

Status: Installed

Authorization

Certificate Options

An X.509 certificate is required by various security protocols. You may update the pre-installed self-signed certificate, or you may create a certificate request. A self-signed certificate provides encryption of data between the client and device, however it does not provide trusted authentication of the device. Data encryption and trusted authentication is provided by a third party certificate. You may also import a certificate and private key to use as the Jetdirect certificate, or you may export the existing Jetdirect certificate and optionally its private key.

○ Create New Self-Signed Certificate

Create a new self-signed certificate. Warning: This operation will overwrite the currently installed certificate with a new self-signed certificate.

● Create Certificate Request

Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.

○ Import Certificate and Private Key

Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key).

○ Export Certificate

Export the Jetdirect certificate and private key.

Authorization

Certificate Options

A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

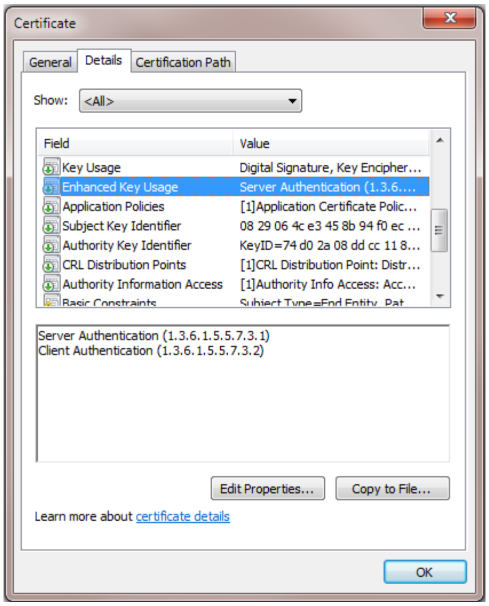
● Install CA Certificate

Install the certificate for a trusted CA (Certificate Authority).

○ Delete a CA Certificate

Delete the certificate for a trusted CA (Certificate Authority).

Note: During the Instant-On mutual authentication process, the device and Security Manager toggle between roles of client and server. When creating (ID) certificates for the printer and Security Manager, ensure the certificates are configured for Server and Client Authentication under Enhanced Key Usage.



Show: <All>

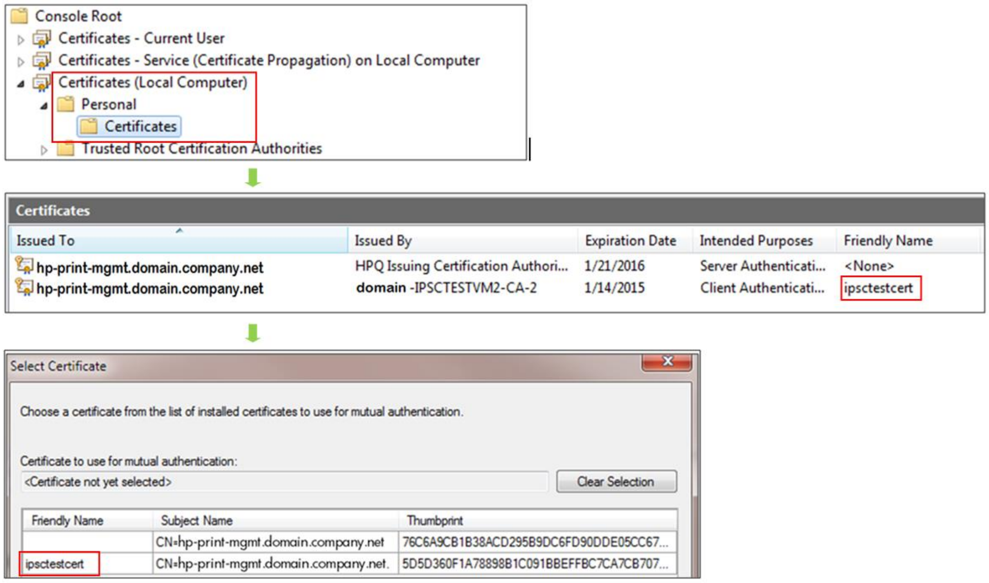
Field	Value
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Server Authentication (1.3.6....
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	08 29 06 4c e3 45 8b 94 f0 ec ...
Authority Key Identifier	KeyID=74 d0 2a 08 dd cc 11 8...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Basic Constraints	Subject Type=End Entity, Pat

Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)

Learn more about certificate details

To participate in a **Mutual Authentication** announcement, each device must be set to **Require Mutual Authentication via Certificates**. From Security Manager, select **Mutual Authentication** and choose the

Certificate to use from the list of security certificates found on the server. The Security Manager list of available certificates is derived from entries found in the Local Computer Personal Store.



Console Root
- Certificates - Current User
- Certificates - Service (Certificate Propagation) on Local Computer
- Certificates (Local Computer)
  - Personal
    - Certificates
  - Trusted Root Certification Authorities

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
hp-print-mgmt.domain.company.net	HPQ Issuing Certification Authori...	1/21/2016	Server Authenticati...	<None>
hp-print-mgmt.domain.company.net	domain -IPSCTESTVM2-CA-2	1/14/2015	Client Authenticati...	ipsctestcert

Select Certificate

Choose a certificate from the list of installed certificates to use for mutual authentication.

Certificate to use for mutual authentication:

<Certificate not yet selected>

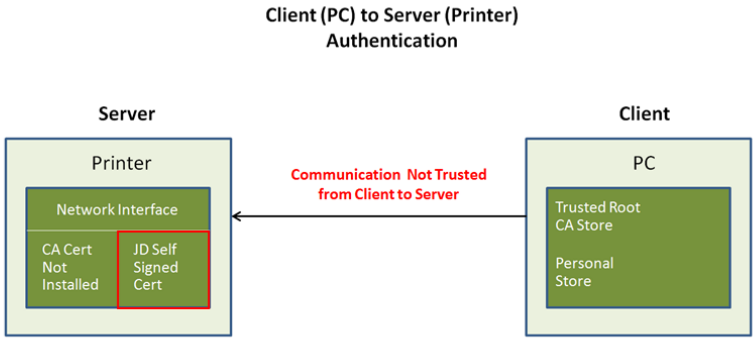
Clear Selection

Friendly Name	Subject Name	Thumbprint
	CN=hp-print-mgmt.domain.company.net	76C6A9CB1B38ACD295B9DC6FD90DDE05CC67...
ipsctestcert	CN=hp-print-mgmt.domain.company.net.	5D5D360F1A78898B1C091BBEFFBC7CA7CB707...

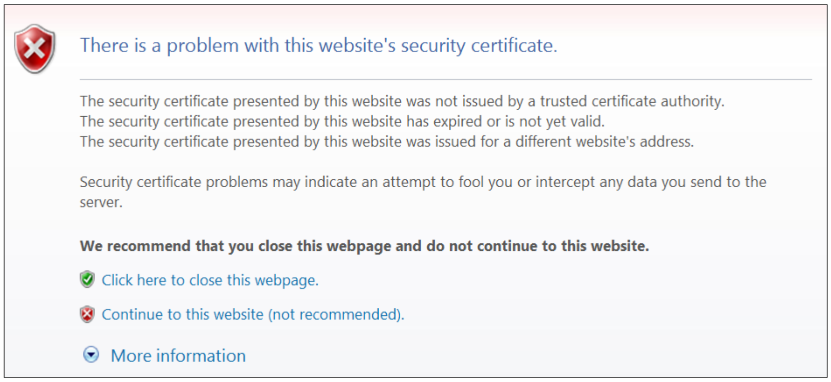
Note: When generating the identity certificate for Security Manager, it is a best practice to assign a friendly name to the certificate for easy identification in the Security Manager certificate list. In the example above, “ipsctestcert” was used.

Mutual Authentication Configuration

To assist with certificate deployment, a basic understanding of mutual authentication and a simplified deployment process is presented in figures. Figure 30 begins by showing the usual out-of-the box configuration and the expected behavior.



By default, only a JetDirect self signed certificate is installed. This certificate is not unique and does not represent the true identity of the printer. Because of this, a user (client) browsing to the printer’s embedded web page (server) will be presented with a warning that the website cannot be trusted. Microsoft Internet Explorer will give a warning that, “There is a problem with this website’s security certificate”. See next figure . Other browsers will present a similar warning.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

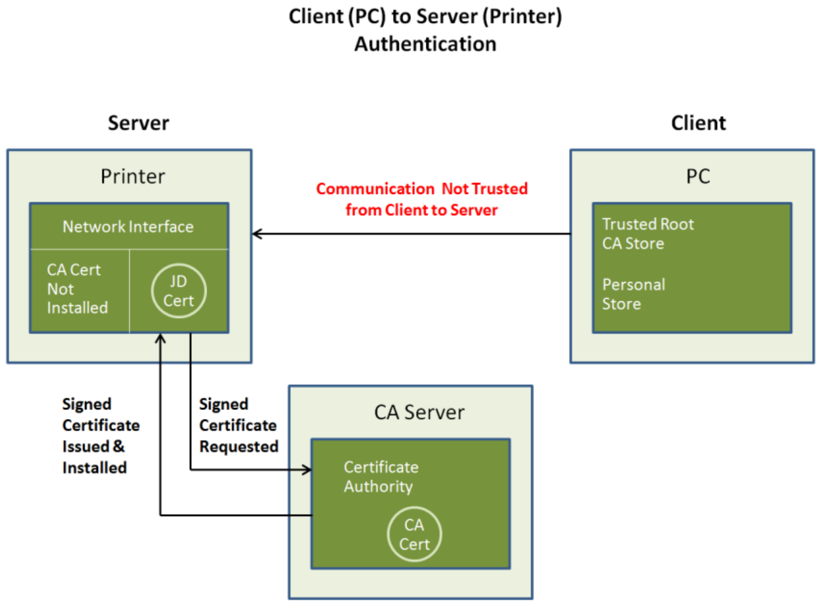
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

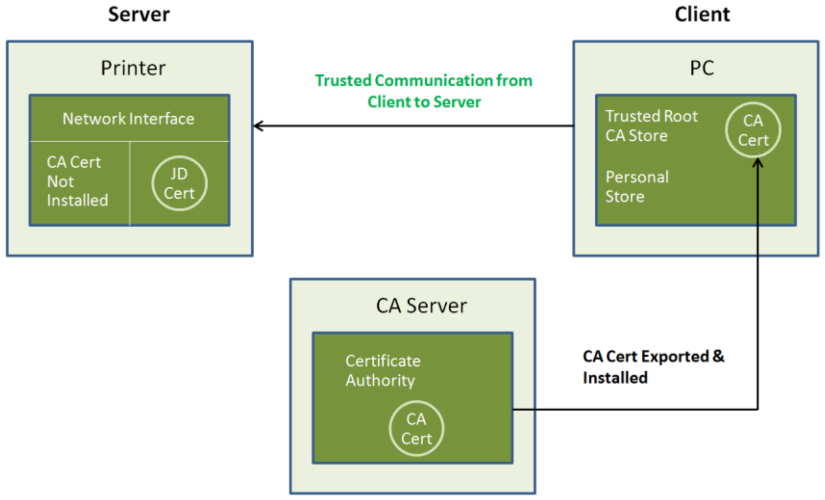
More information

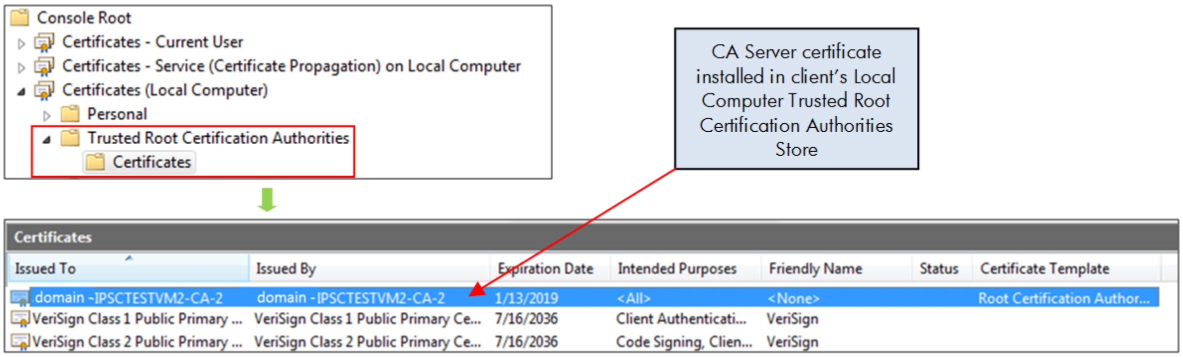
A JetDirect certificate request has been generated and provided to the Certificate Authority (CA) for signing. The (CA) generates a signed identity certificate based upon this request. The newly signed JetDirect certificate is installed, replacing the default self-signed certificate. However, the connection remains untrusted because the client hasn't knowledge of the (CA) that generated the JetDirect certificate.



The client is made aware of the (CA) that generated the JetDirect's signed certificate. The CA's identity certificate was exported and installed in the client's Trusted Root Certificate Authorities store. Trusted communication now exists, but only in one direction; from client to server. Mutual authentication between the pc and printer does not exist at this point.

Client (PC) to Server (Printer) Authentication



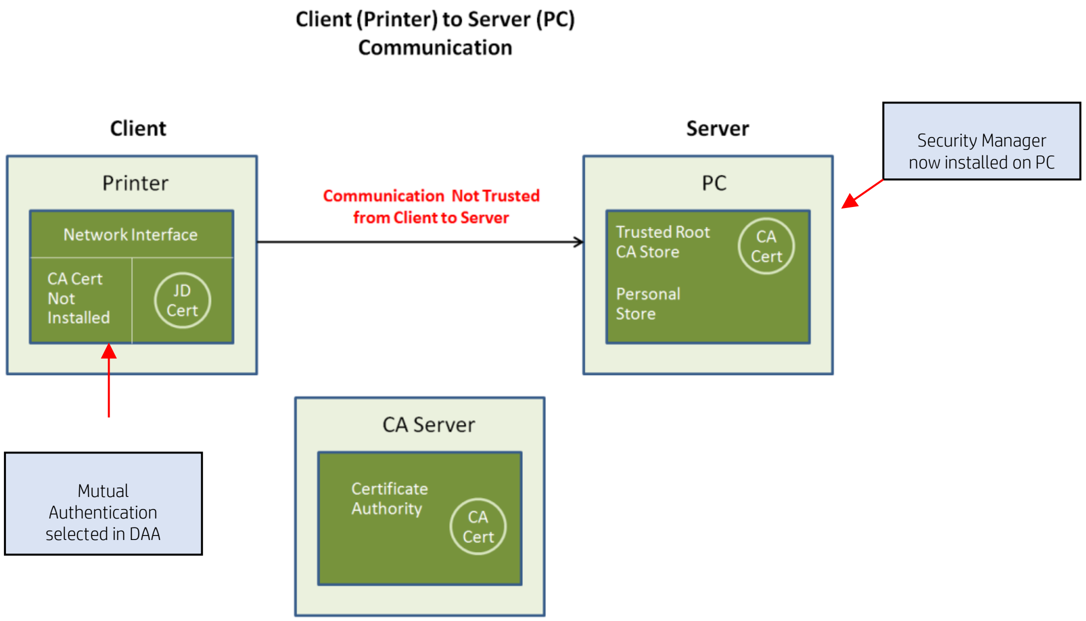

Console Root
Certificates - Current User
Certificates - Service (Certificate Propagation) on Local Computer
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates

CA Server certificate installed in client's Local Computer Trusted Root Certification Authorities Store

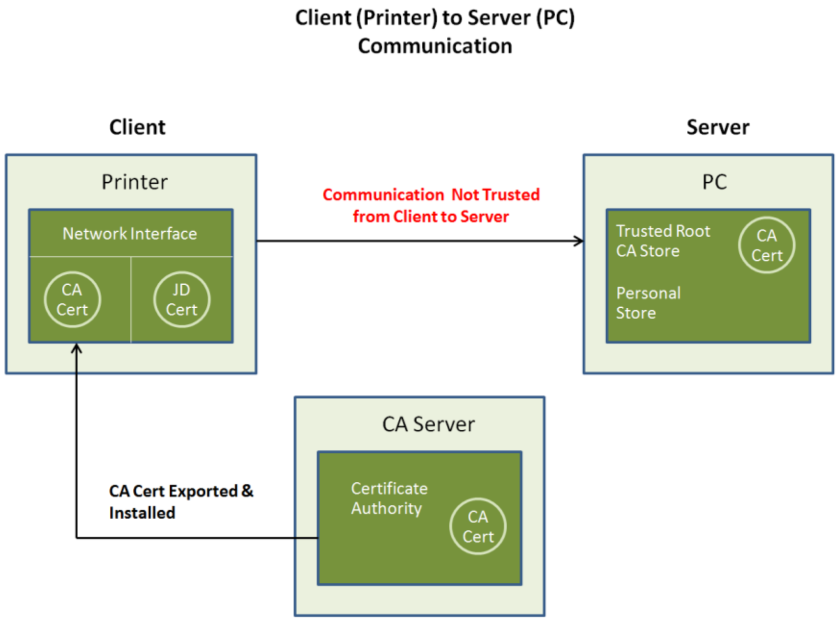
Certificates

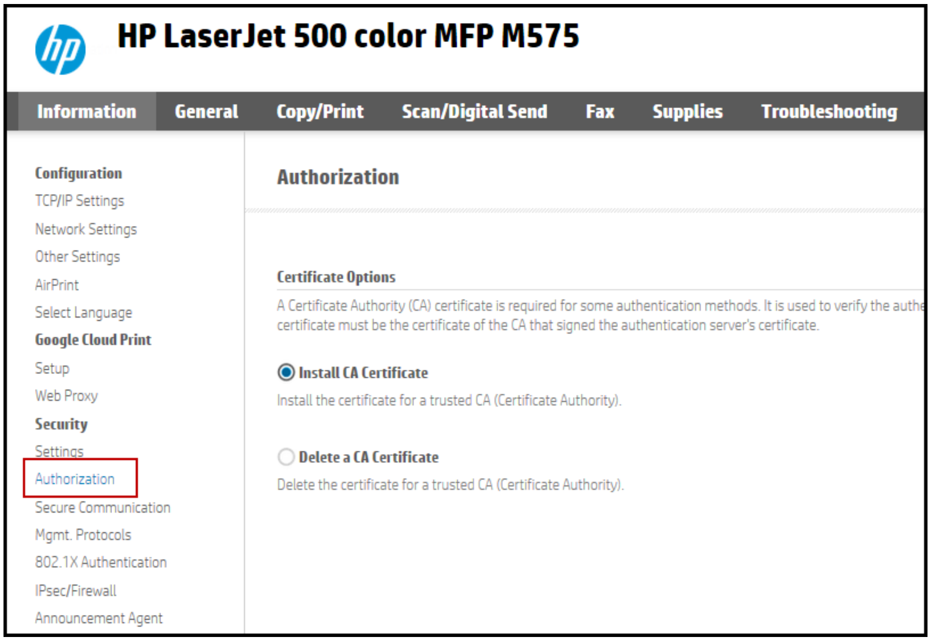
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Template
domain -IPSCTESTVM2-CA-2	domain -IPSCTESTVM2-CA-2	1/13/2019	<All>	<None>		Root Certification Author...
VeriSign Class 1 Public Primary ...	VeriSign Class 1 Public Primary Ce...	7/16/2036	Client Authenticati...	VeriSign		
VeriSign Class 2 Public Primary ...	VeriSign Class 2 Public Primary Ce...	7/16/2036	Code Signing, Clien...	VeriSign		

For Instant-On mutual authentication, the figure below shows the required role reversal between the printer and the pc. With Security Manager installed and the Instant-On Security feature enabled, the printer becomes the client looking to establish secure communication with Security Manager, the server.



With the printer now in the role of client, it requires knowledge of the CA that will be generating the identity certificate for the pc, now the server. The (CA) certificate is exported and installed on the printer. To install the CA certificate on the device.





HP LaserJet 500 color MFP M575

Information | General | Copy/Print | Scan/Digital Send | Fax | Supplies | Troubleshooting

Configuration
TCP/IP Settings
Network Settings
Other Settings
AirPrint
Select Language
Google Cloud Print
Setup
Web Proxy
Security
Settings
Authorization
Secure Communication
Mgmt. Protocols
802.1X Authentication
IPsec/Firewall
Announcement Agent

Authorization

Certificate Options

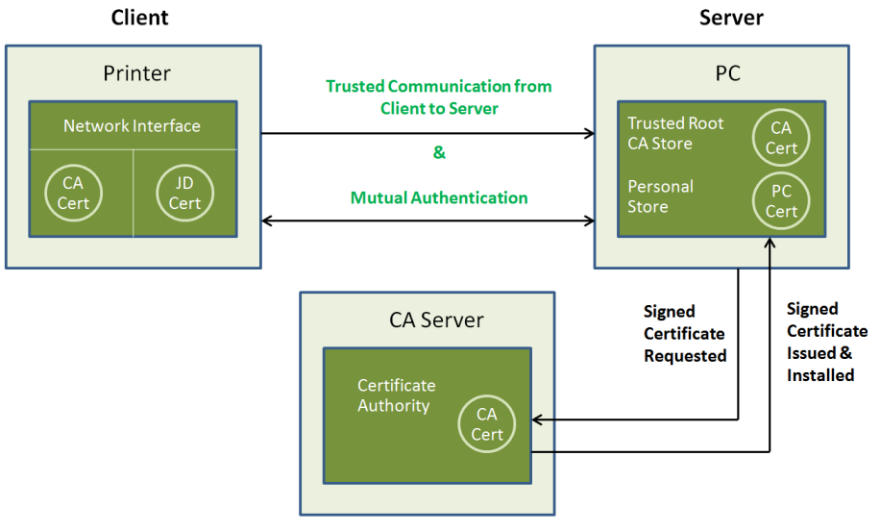
A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authe
certificate must be the certificate of the CA that signed the authentication server's certificate.

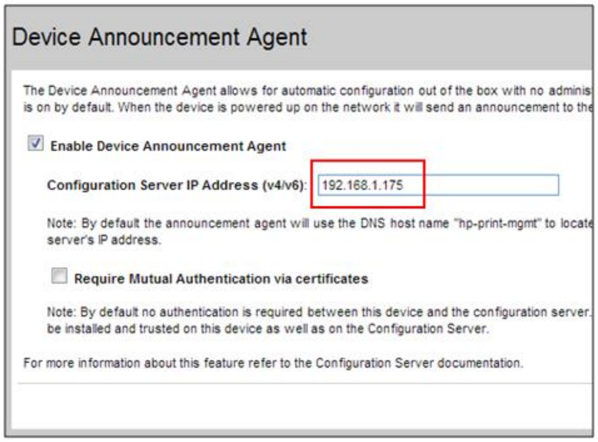
● **Install CA Certificate**
Install the certificate for a trusted CA (Certificate Authority).

○ **Delete a CA Certificate**
Delete the certificate for a trusted CA (Certificate Authority).

At this point, the only missing component needed to achieve mutual authentication is the identity certificate of the server. As was the case when the printer was the server, a certificate request is generated from the Security Manager server and submitted to the CA server for signing. Once signed and installed in the Local Computer Personal Store, trusted client-to-server communication and thus mutual authentication now exists.

Client (Printer) to Server (PC) Communication





Device Announcement Agent

The Device Announcement Agent allows for automatic configuration out of the box with no adminis
is on by default. When the device is powered up on the network it will send an announcement to the

☑ Enable Device Announcement Agent

Configuration Server IP Address (v4/v6): 192.168.1.175

Note: By default the announcement agent will use the DNS host name "hp-print-mgmt" to locate
server's IP address.

☐ Require Mutual Authentication via certificates

Note: By default no authentication is required between this device and the configuration server.
be installed and trusted on this device as well as on the Configuration Server.

For more information about this feature refer to the Configuration Server documentation.

If trusted certificates are not installed or leveraged on either the device or server, the device uses its self-signed certificate for identification purposes and the server handles authentication in an anonymous fashion. If trusted certificates are installed and leveraged on the device and server, mutual authentication can be selected to provide a higher level of communication security. Mutual authentication can serve as a form of Instant-On Security device filtering, as well. More authentication discussion is provided later in this section. The announcement and acknowledge message communication occur directly over registered TCP Port 3329 (named port **hp-device-disc**).

Announcement Message Summary

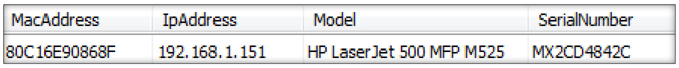
The device **Announcement Message** is always sent using the most secure authentication method the device is configured for. When the Device Announcement Agent is set for **Require Mutual Authentication via Certificates**, only trusted SSL/TLS authentication is allowed. When set, the Announcement Message requires valid identity and CA certificates be installed on the device. If this requirement is not met, the announcement is not sent. In addition, if the Instant-On Configuration Server certificate is determined to be invalid, the device will cease to contact the server, until the next announcement scenario presents itself. In either case, mutual authentication is denied and DAA status will show Fail.

Configuring Instant On with Device Serial List filtering

Selecting **No Authentication** and **Use Device Serial-Number List** configures the Instant-On Configuration Server to work only with the devices whose serial numbers are provided in the list. For example, managing a group of devices included in a Managed Print Services contract or for some other specific device scenario. Along with the product name, MAC address and IP address, the device serial number is included in the announcment message.

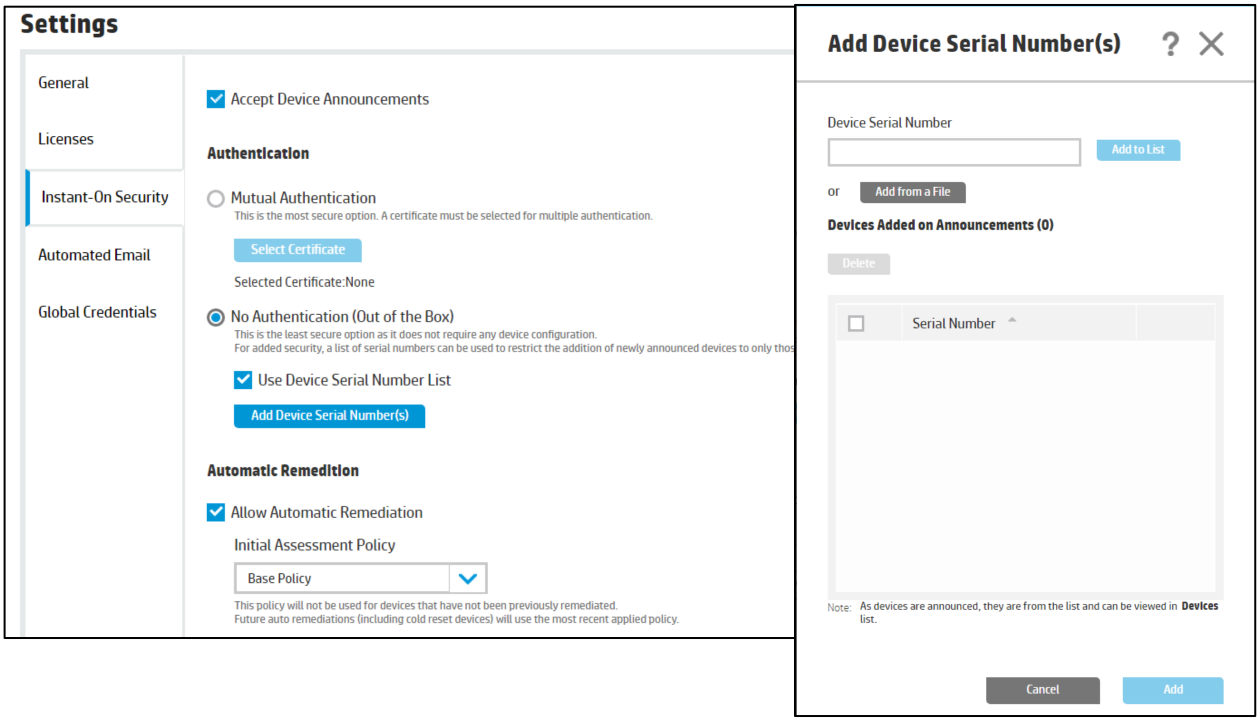
The device's **Announcement Message** request includes device identity information, such as; the MAC address, the IP address, model and the serial number. Upon initial authenticated communication between the device and server, Security Manager inserts this gathered identity information into the database. This identity information, specifically the serial number, can now be used if the serial number filtering option is chosen. Every announcement scenario is handled in identical fashion to the initial device discovery scenario. However, once the device has been discovered, no further database entry will occur to eliminate the possibility of duplicate device entries.

Device Table



MacAddress	IpAddress	Model	SerialNumber
80C16E90868F	192.168.1.151	HP LaserJet 500 MFP M525	MX2CD4842C

Instant-On Security includes the ability to utilize serial numbers as a means of filtering the devices that participate in the Instant-On process. Serial numbers can be singularly added or imported via a text file. With serial number filtering enabled, only the devices whose serial numbers match a database entry in the Serial Number List table are granted Instant-On processing. The image below shows how the Serial Numbers can be added to HPSM.



Settings

☑ Accept Device Announcements

Authentication

○ Mutual Authentication
This is the most secure option. A certificate must be selected for multiple authentication.

Selected Certificate:None

● No Authentication (Out of the Box)
This is the least secure option as it does not require any device configuration.
For added security, a list of serial numbers can be used to restrict the addition of newly announced devices to only thos

☑ Use Device Serial Number List

Automatic Remedition

☑ Allow Automatic Remediation

Initial Assessment Policy

Base Policy

This policy will not be used for devices that have not been previously remediated.
Future auto remediations (including cold reset devices) will use the most recent applied policy.

Add Device Serial Number(s)

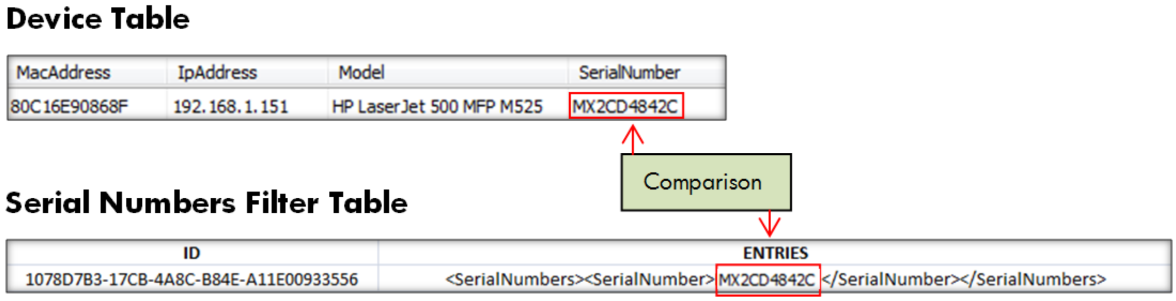
Device Serial Number

Devices Added on Announcements (0)

□	Serial Number

Note: As devices are announced, they are from the list and can be viewed in **Devices** list.

The image below shows the two tables that require a serial number match.



Device Table

MacAddress	IpAddress	Model	SerialNumber
80C16E90868F	192.168.1.151	HP LaserJet 500 MFP M525	MX2CD4842C

Serial Numbers Filter Table

ID	ENTRIES
1078D7B3-17CB-4A8C-B84E-A11E00933556	<SerialNumbers><SerialNumber>MX2CD4842C </SerialNumber></SerialNumbers>

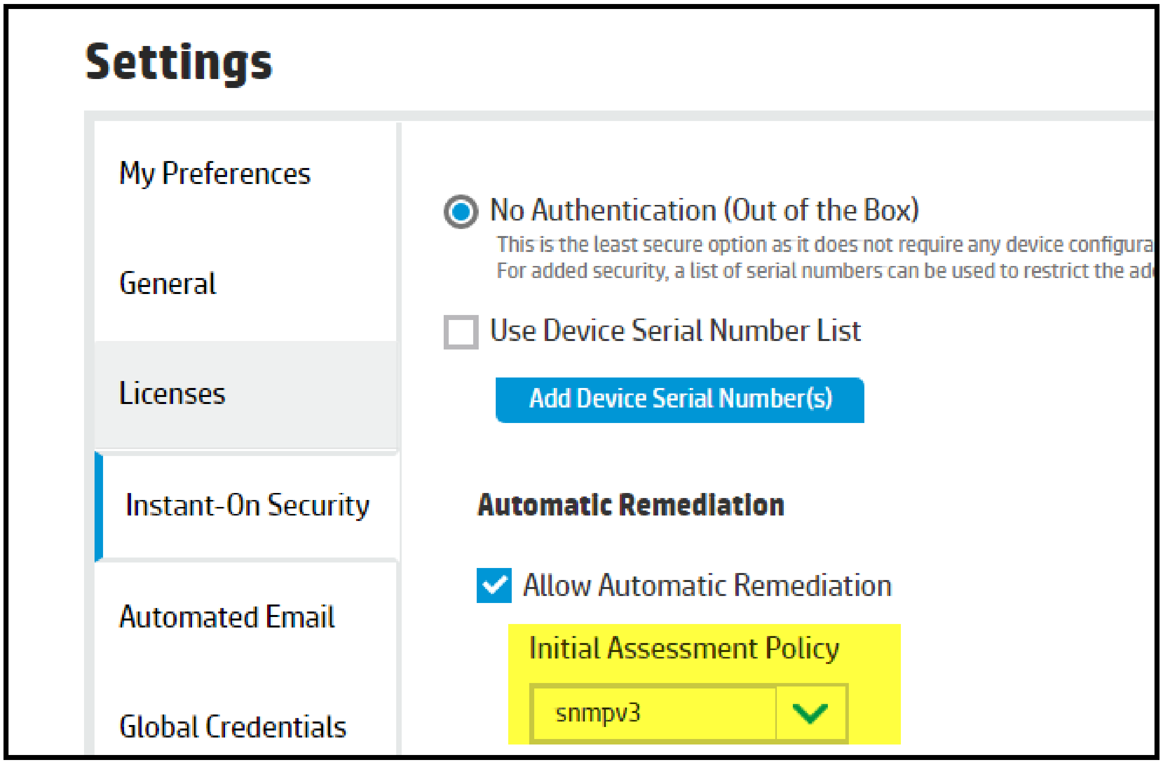
As devices announce, are discovered and placed into the Device Table, the serial number entry is removed from the UI serial number list. From the devices tab, status will show device as being Auto Discovered. As long as **Use Device Serial Number List** remains selected in the Instant-On settings window, only the serial numbers in the Serial Numbers Filter Table will participate in the Instant-On Security process.

Instant-On Assessment Policy with HPSM 3.3 and older

The policy used in the Instant-On Security feature is labeled as the Initial Assessment Policy and as a best practice should always reflect the minimum device security required for all devices participating in Instant-On. Devices participating in Instant-On for the first time will always receive this initial policy. The device will continue to receive the initial policy during Instant-On unless that device was later assessed with a policy other than the Initial Assessment Policy. In this case, that particular policy will be applied the next time the device enters into an Instant-On scenario. Security Manager keeps track of the policy the device was last assessed with and will always apply that policy during Instant-On.

Instant-On Assessment Policy from HPSM 3.4 onwards

Due to the introduction of autogroup remediation policies HPSM 3.4 will *always* use the selected **Initial Assessment Policy** for instant-on remediation when **Allow Automatic Remediation** is enabled under Instant-On Security.



● No Authentication (Out of the Box)

This is the least secure option as it does not require any device configura

For added security, a list of serial numbers can be used to restrict the ad

□ Use Device Serial Number List

Automatic Remediation

☑ Allow Automatic Remediation

Initial Assessment Policy: snmpv3

This change was made as more choices are now possible with autogrouping and autogroup policies. This will be explained in next chapter.

Part 3- Autogrouping and autogroup remediation

HPSM 3.4 introduced the option to configure Autogroups with auto group remediation policies. Autogrouping now includes ability to have one policy automatically remediated when a device is added to the group. Remediations can occur in these scenarios if the autogroup has a policy assigned to it and under the following situations:

A. Device discovered via Instant-on (only remediate the devices which are added to an autogroup via instant on)
B. Device discovered via manual or automatic discovery method (only remediate the devices which are now added to an autogroup)
C. Every x days:hours:minutes:seconds after starting HPSM service (remediate all devices in the autogroup)
D. An auto group or auto group policy has been changed/edited (remediate all devices in the autogroup)

The actual behavior for the above situations is controlled by different configuration settings in the HPSM_Service.exec.config file and in the Web.config file. The HPSM_Service.exe.config (in C:\Program Files (x86)\HP JetAdvantage Security Manager) contains the following configuration settings to define the behavior

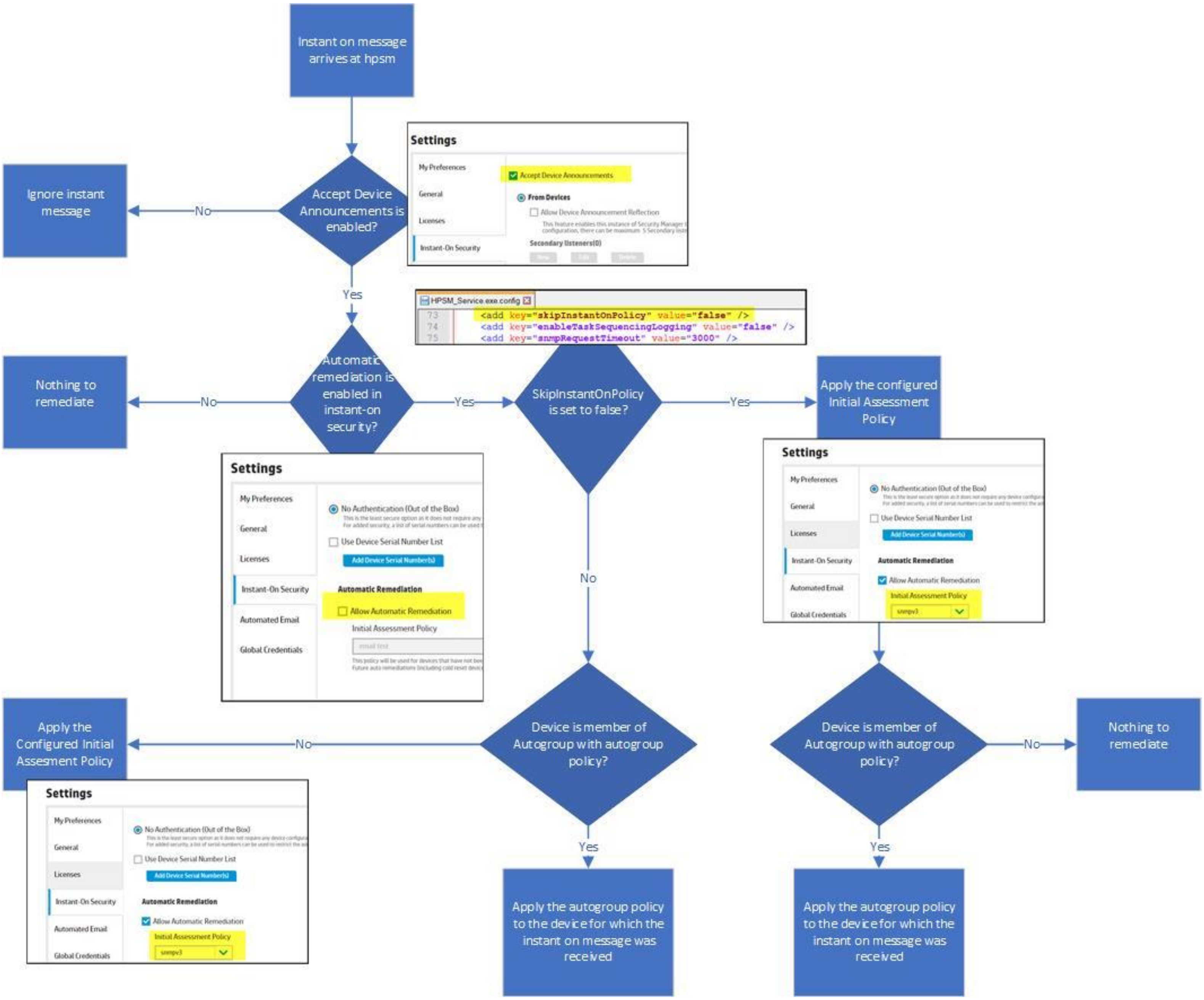
```
<add key="autoGroupDiscoveryAutoRemediationEnable" value="false" />
<add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
<add key="autoGroupFilterExecutionFrequency" value="1:0:0:0" />
```

The Web.config (in C:\Program Files (x86)\HP JetAdvantage Security Manager\WebApp) contains the following configuration settings to control this:

```
<add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
```

A. Autogroup remediation for devices discovered via instant-on

When a device must receive an autogroup policy after HPSM received the instant-on message, then **Allow Automatic Remediation** must be enabled with an Initial Assessment Policy. After receiving an instant on message HPSM will then first send the Initial Assessment Policy and after that the autogroup policy. It’s possible to send only the autogroup policy after receiving an Instant-on message by setting the skipInstantOnPolicy to true in the HPSM_service.exec.config file. The next picture shows the instant-on flow diagram for HPSM.



Instant on message arrives at hpsm
Accept Device Announcements is enabled?
No
Ignore instant message
Yes
Automatic remediation is enabled in instant-on security?
No
Nothing to remediate
Yes
SkipInstantOnPolicy is set to false?
Yes
Apply the configured Initial Assessment Policy
No
Device is member of Autogroup with autogroup policy?
No
Apply the Configured Initial Assesment Policy
Yes
Apply the autogroup policy to the device for which the instant on message was received
Device is member of Autogroup with autogroup policy?
No
Nothing to remediate
Yes
Apply the autogroup policy to the device for which the instant on message was received

Settings

My Preferences
General
Licenses
Instant-On Security

☑ Accept Device Announcements

● From Devices

□ Allow Device Announcement Reflection

This feature enables this instance of Security Manager t configuration, there can be maximum 5 Secondary liste

Secondary listeners(0)

HPSM_Service.exe.config

```
<add key="skipInstantOnPolicy" value="false" />
<add key="enableTaskSequencingLogging" value="false" />
<add key="snmpRequestTimeout" value="3000" />
```

Settings

My Preferences
General
Licenses
Instant-On Security
Automated Email
Global Credentials

● No Authentication (Out of the Box)

□ Use Device Serial Number List

Add Device Serial Number(s)

Automatic Remediation

□ Allow Automatic Remediation

Initial Assessment Policy

Settings

My Preferences
General
Licenses
Instant-On Security
Automated Email
Global Credentials

● No Authentication (Out of the Box)

□ Use Device Serial Number List

Add Device Serial Number(s)

Automatic Remediation

☑ Allow Automatic Remediation

Initial Assessment Policy: snmpv3

Settings

My Preferences
General
Licenses
Instant-On Security
Automated Email
Global Credentials

● No Authentication (Out of the Box)

□ Use Device Serial Number List

Add Device Serial Number(s)

Automatic Remediation

☑ Allow Automatic Remediation

Initial Assessment Policy: snmpv3

The same information, but in a different format can be seen in the following table:

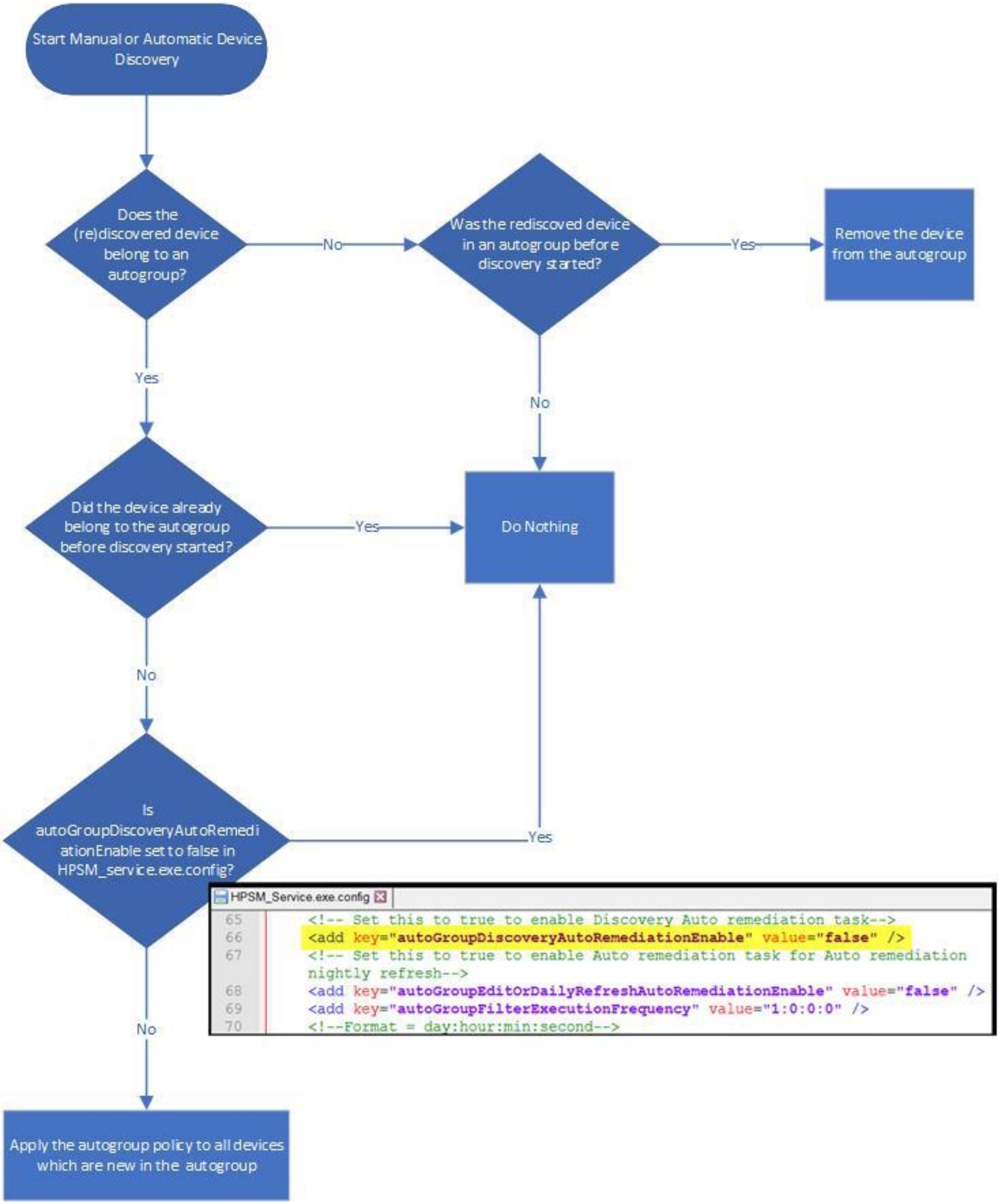
SkipInstantOnPolicy	TRUE		FALSE	
Policy Device membership	Apply Instant-On Policy (Initial assesment policy)	Apply Autogroup Policy	Instant-On Policy (Initial assesment policy)	Apply Autogroup Policy
Device member of AutoGroup with Policy	No	Yes	Yes (1st policy)	Yes (2nd policy)
Device member AutoGroup without Policy, or device member of manual group or device only belongs to all devices	Yes	No or NA as the device is not member of an autogroup with autogroup policy	Yes	No or NA as the device is not member of an autogroup with autogroup policy

This way at least one policy will always get applied when an Initial Announcement Policy has been activated

B. Autogroup remediation for devices discovered via manual or automatic discovery

By default when a device is discovered or re-discovered it's not getting remediated with the autogroup policy at the time of the discovery. A device might be added or removed from autogroups during discovery . It's possible to enforce an immediate remediation when a device is discovered via manual discover of automatic discovery and when the device is new in the autogroup. This can be done by setting the autoGroupDiscoveryAutoRemediationEnable to true in the HPSM_service.exe.config file.

The next picture shows the manual/automatic discovery flowchart for HPSM.

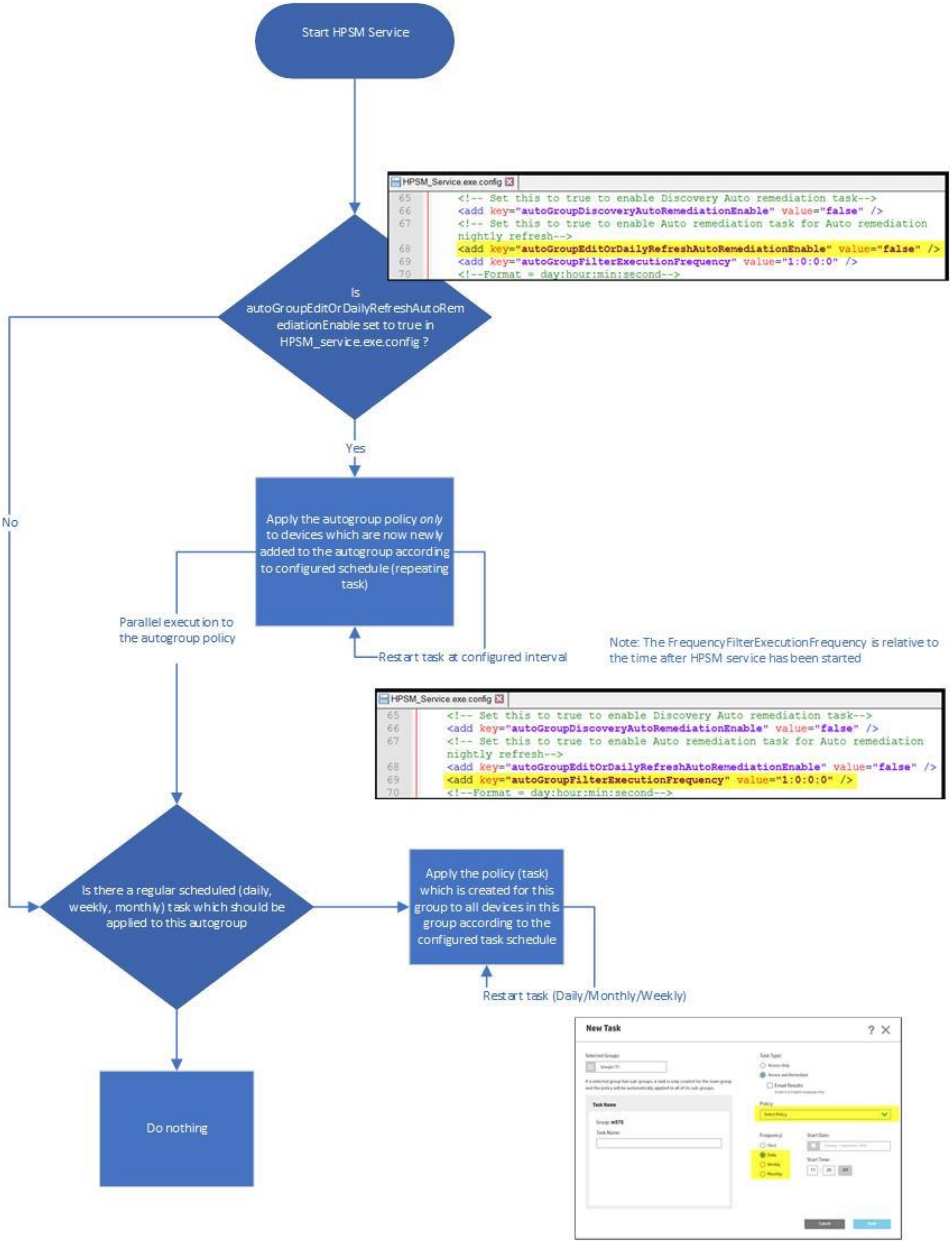

Start Manual or Automatic Device Discovery
Does the (re)discovered device belong to an autogroup?
No
Was the rediscoved device in an autogroup before discovery started?
Yes
Remove the device from the autogroup
Yes
No
Did the device already belong to the autogroup before discovery started?
Yes
Do Nothing
No
Is autoGroupDiscoveryAutoRemediationEnable set to false in HPSM_service.exe.config?
Yes
No
Apply the autogroup policy to all devices which are new in the autogroup
HPSM_Service.exe.config

```
<!-- Set this to true to enable Discovery Auto remediation task-->
<add key="autoGroupDiscoveryAutoRemediationEnable" value="false" />
<!-- Set this to true to enable Auto remediation task for Auto remediation
nightly refresh-->
<add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
<add key="autoGroupFilterExecutionFrequency" value="1:0:0:0" />
<!--Format = day:hour:min:second-->
```

C. Autogroup remediation at configured time intervals

Devices which are newly added to an autogroup can be remediated at specified time intervals with the configured autogroup policy. By default this is disabled. In order to enable this the setting autoGroupEditOrDailyRefreshAutoRemediationEnable must be set to true in the file HPSM_service.exe.config (in C:\Program Files (x86)\HP JetAdvantage Security Manager) file. After making this change the HP Jetadvantage Security Manager service needs to be restarted.

The actual frequency can be controlled by changing the value of autoGroupFilterExecutionFrequency (also located in the HPSM_Service.exe.config file). By default it's set to "1:0:0:0" which means once a day (meaning 24 hours after starting the HPSM service). If you need to apply a policy to an autogroup to *all* devices in that autogroup, then you have to schedule a (daily/weekly/monthly) task. The next picture shows the flowchart for autogroup remediation.



Start HPSM Service
Is autoGroupEditOrDailyRefreshAutoRemediationEnable set to true in HPSM_service.exe.config ?
Yes
No
Apply the autogroup policy *only* to devices which are now newly added to the autogroup according to configured schedule (repeating task)
Parallel execution to the autogroup policy
Restart task at configured interval
Note: The FrequencyFilterExecutionFrequency is relative to the time after HPSM service has been started
Is there a regular scheduled (daily, weekly, monthly) task which should be applied to this autogroup
Apply the policy (task) which is created for this group to all devices in this group according to the configured task schedule
Restart task (Daily/Monthly/Weekly)
Do nothing

HPSM_Service.exe.config

```
<!-- Set this to true to enable Discovery Auto remediation task-->
<add key="autoGroupDiscoveryAutoRemediationEnable" value="false" />
<!-- Set this to true to enable Auto remediation task for Auto remediation
nightly refresh-->
<add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
<add key="autoGroupFilterExecutionFrequency" value="1:0:0:0" />
<!--Format = day:hour:min:second-->
```

HPSM_Service.exe.config

```
<!-- Set this to true to enable Discovery Auto remediation task-->
<add key="autoGroupDiscoveryAutoRemediationEnable" value="false" />
<!-- Set this to true to enable Auto remediation task for Auto remediation
nightly refresh-->
<add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
<add key="autoGroupFilterExecutionFrequency" value="1:0:0:0" />
<!--Format = day:hour:min:second-->
```

New Task

Selected Groups

Task Name

Group: m576

Task Name:

Task Type:

○ Assess Only

● Assess and Remediate

□ Email Results

Policy

Select Policy

Frequency:

○ Once

● Daily

○ Weekly

○ Monthly

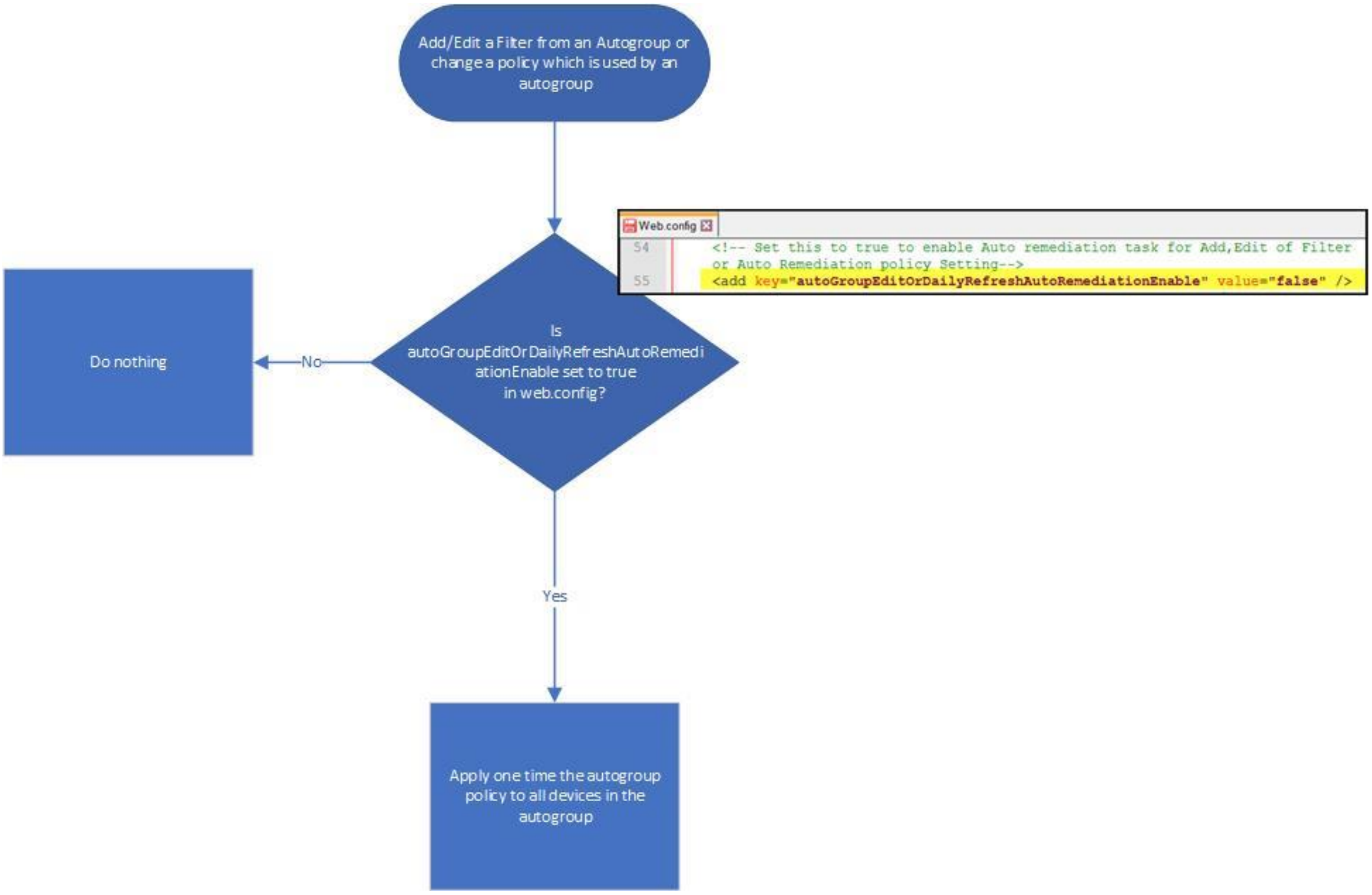
Start Date:

Start Time:

11 : 28

D. Autogroup remediation after editing an autogroup or autogroup policy

It's possible to apply an autogroup policy immediate to all devices in the autogroup after editing the autogroup or the autogroup policy. This can be done by changing the default value for autoGroupEditOrDailyRefreshAutoRemediationEnable from false to true in the Web.config file. The following picture shows the flow diagram for editing an autogroup or editing an autogroup filter.


Add/Edit a Filter from an Autogroup or change a policy which is used by an autogroup
Web.config
Is autoGroupEditOrDailyRefreshAutoRemediationEnable set to true in web.config?
No
Do nothing
Yes
Apply one time the autogroup policy to all devices in the autogroup

```
    <!-- Set this to true to enable Auto remediation task for Add,Edit of Filter
    or Auto Remediation policy Setting-->
    <add key="autoGroupEditOrDailyRefreshAutoRemediationEnable" value="false" />
```

Part 4 – Performance Implications

Performance on the Security Manager server can definitely suffer in cases of large amounts of device announcements being received and automatic assessments/remediations being performed. Comparing the threading model, it is easy to see why it takes much longer to assess 1000 devices discovered thru Instant On announcements vs. 1000 devices scheduled for an assessment as a scheduled task.

Instant On assessment tasks are processed at one device per task because they are received one at a time, and Security Manager processes a maximum of 10 tasks at a time by default. This number of maximum tasks at a time can be controlled using a configuration item in the HPSM_Service.exe.config file found under

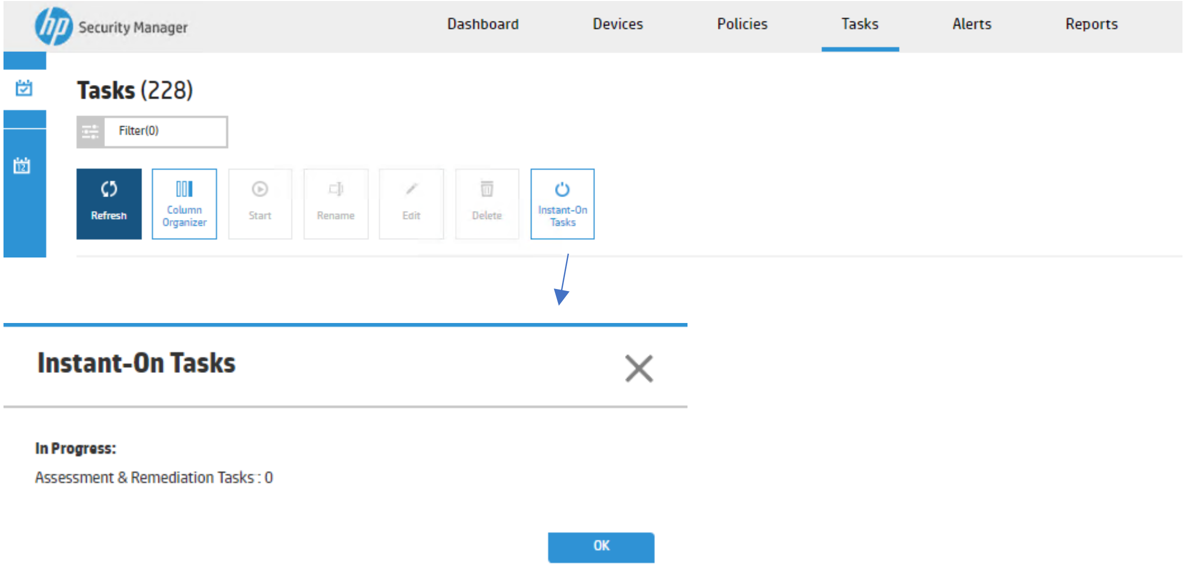
\Program Files (x86)\HP JetAdvantage Security Manager

```
<add key="maxNumberTasks" value="10" />
```

For scheduled assessment tasks, since the number of devices is predefined, a parent task is broken into child tasks of 25 devices each. Each child task of 25 devices is also threaded at 10 threads simultaneously, just like Instant On tasks. However the difference here is that instead of one device being assessed in a threaded task, 25 devices are being assessed. Any remediations or credential failures requiring additional credential retries are performed as one individual task each at the same maximum of 10 threads simultaneously.

A high volume of Instant On device announcements occurring in the background will absolutely affect performance. If Instant On is being enabled for the first time, expect delays as it takes time to process the fleet. Scheduled tasks will likely go into a waiting state until these Instant On devices can be processed. However, it is possible there are a few devices causing such a high volume even after the initial enabling on Instant On. If many of the messages are coming from one device, it could be because a faulty device is going off of the network and coming back again. There could also be devices constantly rebooting for some reason. Try eliminating such devices if suspicions arise they may be responsible for the bulk of Instant On tasks.

The Tasks tab contains a button to view all active Instant On tasks:



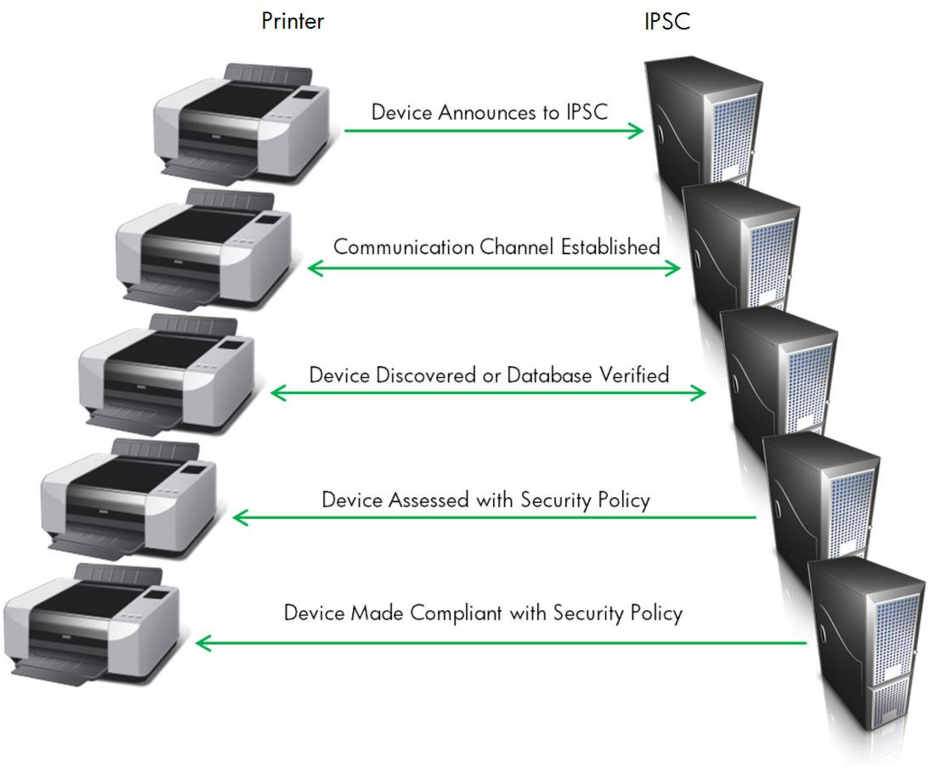
In Progress:

Assessment & Remediation Tasks : 0

This can help to determine if Instant On tasks are constantly bombarding the Security Manager server. It may boil down to if the fleet is exceptionally large and Instant On seems to be consuming a bulk of the bandwidth, a separate server may be required to process just the Instant On tasks. This will allow for the “instant” remediation benefit of Instant On in cases where a device is cold reset, for example. However, it won’t compromise the ability of the scheduled tasks to keep the entire fleet in compliance if running on a separate server. A second Security Manager server can be setup as a secondary Instant On listener so the primary server receiving the device announcements can forward those devices to the secondary server, thus preserving the discovery portion of Instant On.

Part 4 – Summary

Instant-On Security is a high value feature of HP JetAdvantage Security Manager. Enabling this feature allows supported devices to be automatically discovered, assessed and remediated with the configured security policy when first placed on the network. When security configuration loss scenarios are experienced by the device after placement on the network, Instant-On Security automatically keeps the device secure by remediating the settings out of compliance with the security policy. Used in conjunction with frequently scheduled assessment and remediation tasks, the supported fleet can be kept security policy compliant with minimal to no manual intervention. Instant-On supported devices announce themselves directly to the Security Manager server (mutual authentication is an option) and do not require special network configuration for successful operation. Instant-On supported devices are a subset of Security Manager supported devices. The following figure contains a summarized representation of the Instant-On process.


Printer
IPSC
Device Announces to IPSC
Communication Channel Established
Device Discovered or Database Verified
Device Assessed with Security Policy
Device Made Compliant with Security Policy

Appendix A

Links to other HP Security Manager Whitepapers

There are a lot of whitepapers/manuals available for HP Jetadvantage Security Manager.

The overview on the web, can be found by going to: http://www.hp.com/go/securitymanager

After that click on the link Whitepapers and Support Documents.

This will show the following list:

HP JetAdvantage Security Manager - Policy Editor Settings (white paper)

HP JetAdvantage Security Manager - Reporting, Email Alert Subscriptions & Remediation Summary, Auditing & Syslog Functionality (white paper)

HP JetAdvantage Security Manager - Using licenses and troubleshooting licensing issues (white paper)

HP JetAdvantage Security Manager - Securing the HP JetAdvantage Security Manager (white paper)

HP JetAdvantage Security Manager - User Guide

HP JetAdvantage Security Manager - Supported devices and features table

HP JetAdvantage Security Manager - Installation and Setup Guide

HP JetAdvantage Security Manager - Credential Management (white paper)

HP JetAdvantage Security Manager - Release Notes with Ports (white paper)

HP JetAdvantage Security Manager - Tracking Device Identity (white paper)

HP JetAdvantage Security Manager - Instant-On Security (white paper)

HP JetAdvantage Security Manager - Automation Output Feature (white paper)

HP JetAdvantage Security Manager - Sizing and Performance (white paper)

HP JetAdvantage Security Manager - Supported Devices (white paper)

HP JetAdvantage Security Manager - Certificate Management (white paper)

HP JetAdvantage Security Manager - Manage devices with FutureSmart 4.5 Firmware

HP JetAdvantage Security Manager - Using Microsoft® SQL Server (white paper)

HP JetAdvantage Security Manager - Troubleshooting Issues (white paper)

c04222990ENW, Rev. 10, Mar 2021