Technical white paper

FutureSmart configuration changes for Microsoft channel binding and LDAP signing requirements for Windows

Table of contents

March 2020 Public

Version 1.0

Introduction

Microsoft release a security advisory[1] in August 2019 providing guidance to increase security for communications between LDAP clients and Active Directory domain controllers. Unsafe default configurations for LDAP channel binding and LDAP signing exist on Active Directory domain controllers. See Microsoft Advisory “ADV190023 - Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing” for additional information.

On March 10th, 2020 Microsoft will include options to harden LDAP communications on Active Directory domain controllers in the March windows update. These include a new group policy object for LDAP channel binding and new event codes for LDAP signing and LDAP channel binding in the event viewer.

Important: The March 10, 2020 updates do not change LDAP signing or LDAP channel binding default policies or their registry equivalents on new or existing Active Directory domain controllers.

Detailed Description

The recommended LDAP security hardening guidance recommended in ADV 190023[1] is managed through two registry settings.

- “LDAPServerIntegrity” registry setting:

When enabled the server will

- ○ Reject LDAP simple binds on clear text (non-SSL encrypted) connections
- ○ Reject Simple Authentication Security Layer (SASL) LDAP binds that do not request signing (integrity verification)

Group Policy Setting	Registry Setting
None	1 (default)
Require Signing	2

- “LdapEnforceChannelBinding” registry setting

When enabled the server will

- Reject authentication requests that do not include channel binding tokens (CBT) that provide channel binding information to the server

Group Policy Setting	Registry Setting
Never	0 (default)
When Supported	1 (compatibility mode)
Always	2

HP FutureSmart Printer Configuration Changes

The following configuration changes are needed when enabling the LDAP hardening recommendations from Microsoft.

! A Certificate of Authority (CA) certificate and corresponding intermediate certificates (if required) will need to be installed into the printer certificate store to validate the Active Directory server public certificate. This CA certificate is required to be able to use TCP port 636 for Windows authentication and LDAP queries over an encrypted SSL connection.

1. Obtain a CA certificate for the Active Directory server by contacting your IT server administrator.

Note: For assistance in acquiring this certificate, please contact your account technical representative or HP customer support.

2. Install the CA certificate using the device Embedded Web Server

   a. Using a browser, enter the IP address of the printer. Logon to the EWS if required.

   b. Select the **Security Tab**, then select **Certificate Management** from the left navigation menu

   c. In the **CA Certificates** section, select **Choose File to** browse to the certificate file (with extension .p7b, cer, etc.)

   d. Choose **Install**

   e. Verify the certificate is listed in the Certificates table.

   Note: for instructions to install Active Directory CA certificates and configure Windows authentication using Web Jetadmin or HP Security Manager please see the Configuring printers using HP Fleet Management Tools section.

2. Configure Windows Authentication to use a secure encrypted SSL connection

   a. Select the **Security Tab**, then select **Access Control** from the left navigation menu

   b. In the **Enable and Configure Sign-in Methods** section, Select **Setup Windows**

   c. Select the **Use a secure connection (SSL)** checkbox

   d. Complete or verify remaining Windows Sign-In settings

   e. Select **OK**

3. Configure the printer to use an encrypted connection to LDAP for Network Contacts

   a. Select the **Scan/Digital Send Tab**, then select **Contacts** from the left navigation menu

   b. In the **Network Contacts Setup** section, Select the **Enable Network Contacts (use LDAP server)** checkbox

   c. Select **Add** for a new connection or **Edit** for an existing connection

   d. Select the **Use a secure connection (SSL)** checkbox

   e. Verify the **Port:** value now show **636**

   f. Complete or verify remaining Network Contacts Setup settings

   g. Select **OK**

Configuration changes using HP Fleet Management Tools

The following HP fleet management software tools can be used to manage CA certificates across a fleet of printing devices.

Note: It is recommended to test the CA certificate integration using the EWS method before beginning a fleet wide installation.

HP Web Jetadmin

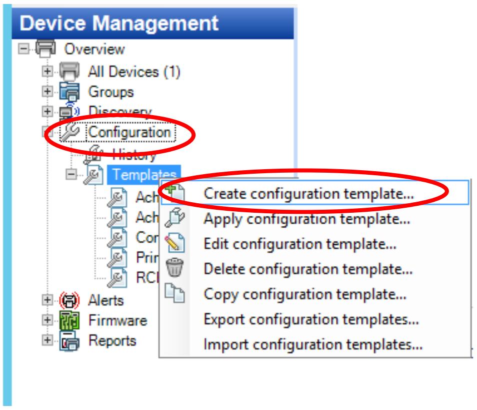
HP Web Jetadmin is the primary HP fleet management tool It is available for download at www.hp.com/go/webjetadmin.

Use the following steps to install the LDAP server CA certificate on multiple printing devices.

Create a configuration template and attach the Active Directory server CA certificate

1. Click the “+” sign to expand the “Configuration” tree options

2. Right-Click on Templates and select “Create configuration template…”


Device Management
Overview
All Devices (1)
Groups
Discovery
Configuration
History
Templates
Ach
Ach
Cor
Prir
RCI
Alerts
Firmware
Reports
Create configuration template...
Apply configuration template...
Edit configuration template...
Delete configuration template...
Copy configuration template...
Export configuration templates...
Import configuration templates...

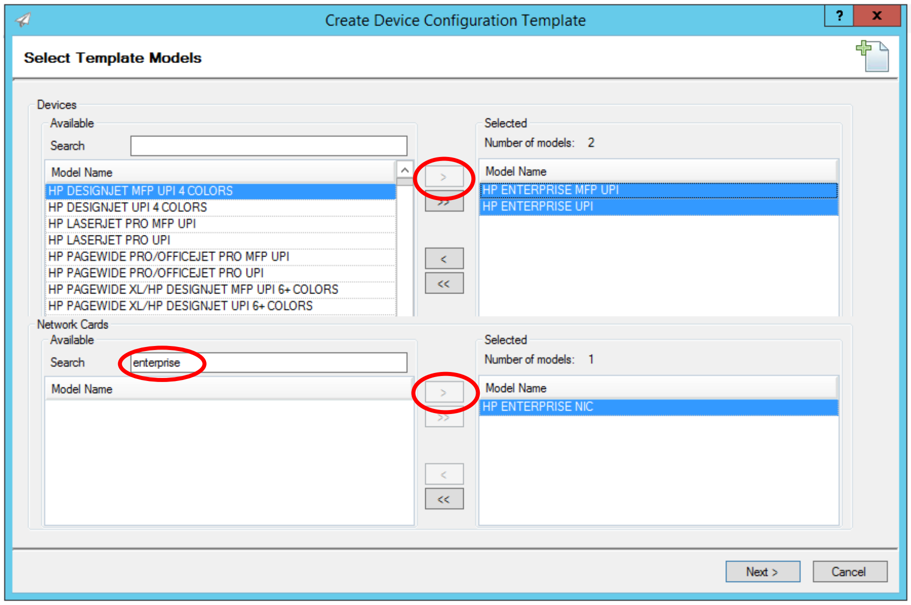
3. In the “Devices-Search” field, enter “Enterprise”, then highlight “HP ENTERPRISE MFP UPI” from list.

4. Click the “>” button to move “HP ENTERPRISE MFP UPI” to the Selected models dialog

5. In the “Network Cards-Search” field Enter “Enterprise”, then highlight “HP ENTERPRISE NIC” from list.

6. Click the “>” button to move “HP ENTERPRISE MFP UPI” to the Selected models dialog

7. Click Next



Devices – Available

Model Name
HP DESIGNJET MFP UPI 4 COLORS
HP DESIGNJET UPI 4 COLORS
HP LASERJET PRO MFP UPI
HP LASERJET PRO UPI
HP PAGEWIDE PRO/OFFICEJET PRO MFP UPI
HP PAGEWIDE PRO/OFFICEJET PRO UPI
HP PAGEWIDE XL/HP DESIGNJET MFP UPI 6+ COLORS
HP PAGEWIDE XL/HP DESIGNJET UPI 6+ COLORS

Devices – Selected: Number of models: 2

Model Name
HP ENTERPRISE MFP UPI
HP ENTERPRISE UPI

Network Cards – Search: enterprise

Network Cards – Selected: Number of models: 1

Model Name
HP ENTERPRISE NIC

8. In the Name field, enter “CA_ Certificate_Template”

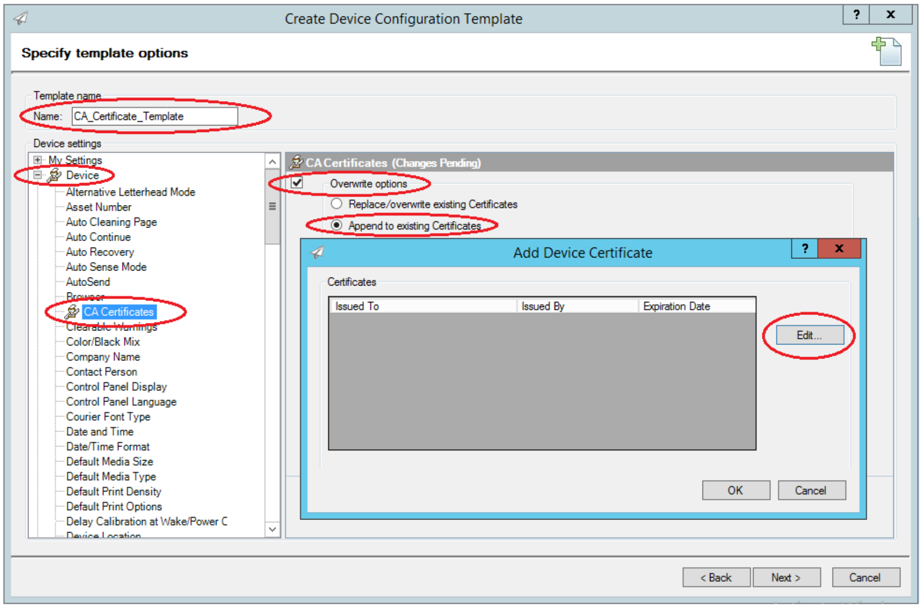
9. Click the “+” sign to expand the Device tree options

10. Click “CA Certificates” to select it in the Device options list

11. Select the Overwrite Options checkbox; then select the “Append to existing Certificates” radio button

12. In the Certificates section, select “Add”

13. In the Add Device Certificate dialog, select Edit



Create Device Configuration Template

Specify template options

Template name

Name: CA_Certificate_Template

Device settings

CA Certificates (Changes Pending)

☑ Overwrite options

○ Replace/overwrite existing Certificates

● Append to existing Certificates

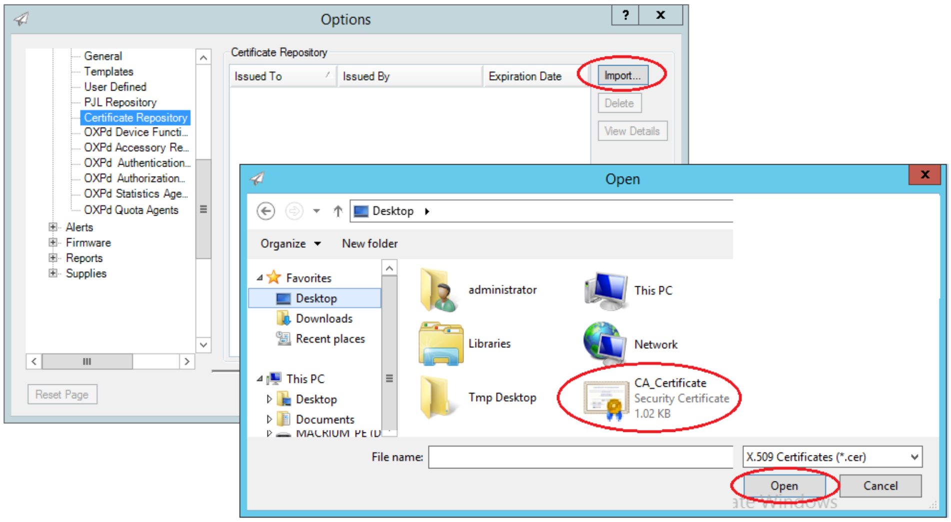
Add Device Certificate

Certificates

Issued To	Issued By	Expiration Date

14. In the Options dialog, select Import

15. Browse to the location of the Active Directory CA Certificate and select Open



Options

Certificate Repository

Issued To	Issued By	Expiration Date

Open

File name:

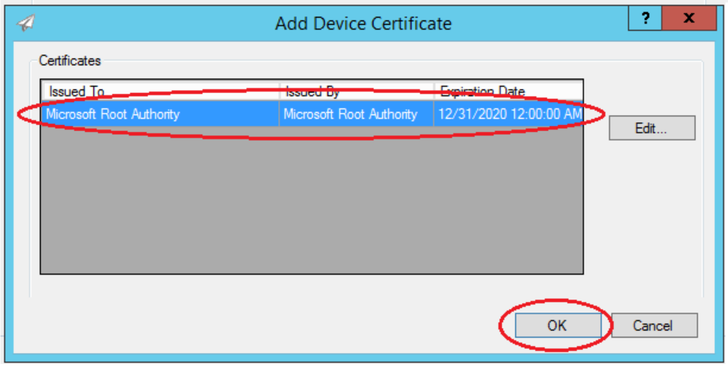
X.509 Certificates (*.cer)

16. Select OK to close the Options dialog

17. Select the imported certificate now listed in the Certificates list (certificate entry will be highlighted)

18. Select OK to close the Add Device Certificate dialog

Note: if the Certificates list is empty when returning to the template, go back to Step 17 to highlight the imported certificate.



Add Device Certificate

Certificates

Issued To	Issued By	Expiration Date
Microsoft Root Authority	Microsoft Root Authority	12/31/2020 12:00:00 AM

19. Select Next in the “Specify Template options” dialog

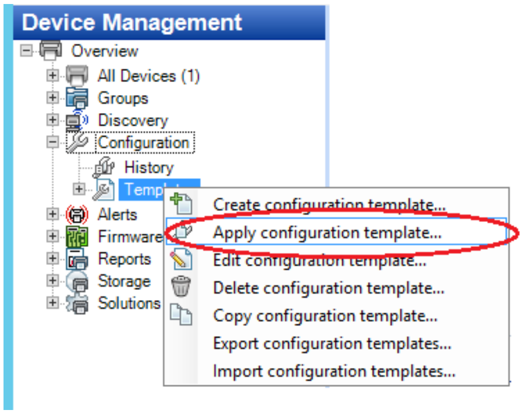
20. Select Create Template

21. Select Done

Apply the Active Directory CA certificate template to printing devices

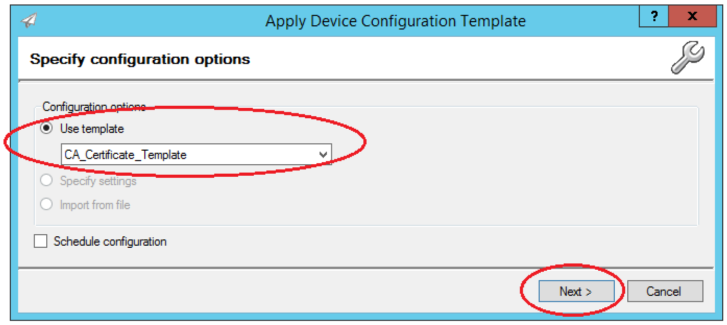
1. Click the “+” sign to expand the “Configuration” tree options

2. Right-Click on Templates and select “Apply configuration template…”


Device Management
Overview
All Devices (1)
Groups
Discovery
Configuration
History
Templates
Alerts
Firmware
Reports
Storage
Solutions
Create configuration template...
Apply configuration template...
Edit configuration template...
Delete configuration template...
Copy configuration template...
Export configuration templates...
Import configuration templates...

3. Select the “CA_Certificate_Template” template for the “Use template” drop-down list

4. Select Next



Specify configuration options

Configuration options

● Use template

CA_Certificate_Template

○ Specify settings

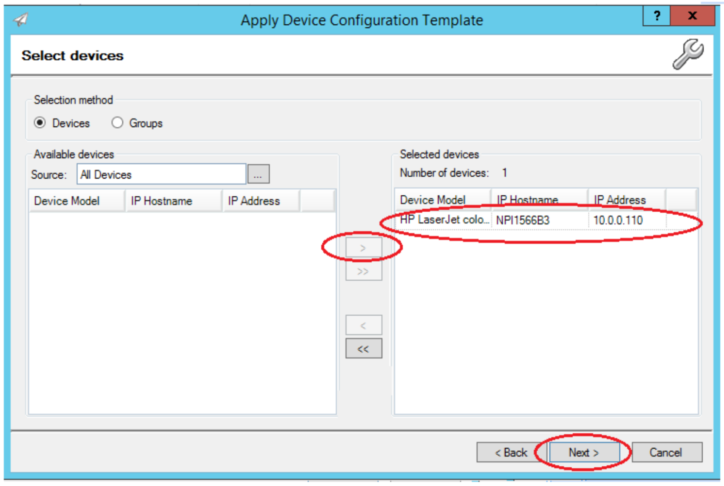
○ Import from file

□ Schedule configuration

5. Select previously discovered devices from the “Available Devices” dialog (use the CTRL key to select multiple devices)

6. Select the “>” button to move devices to the Selected Devices dialog (or use the “>>” button to move all listed devices

7. Select Next



Select devices

Selection method

● Devices ○ Groups

Available devices

Source: All Devices ...

Device Model	IP Hostname	IP Address

Selected devices

Number of devices: 1

Device Model	IP Hostname	IP Address
HP LaserJet colo...	NPI1566B3	10.0.0.110

8. Select Apply Template
9. Monitor the Results dialog to validate Success or Error

HP Security Manager

Use the steps outlined in the "HP JetAdvantage Security Manager Certificate Management" whitepaper to install the CA Certificate on multiple printing devices.

- "Using Security Manager to Manage CA Certificates" (page 34)

  http://h10032.www1.hp.com/ctg/Manual/c04677863.pdf

References

1. Microsoft Security Advisory ADV190023 - Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing

   https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023

2. 2020 LDAP channel binding and LDAP signing requirements for Windows

   https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows

3. Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure

   https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry

4. How to enable LDAP signing in Windows Server 2008

   https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008

5. Using Security Manager to Manage CA Certificates

   http://h10032.www1.hp.com/ctg/Manual/c04677863.pdf

hp.com/go/support

Current HP driver, support, and security alerts
delivered directly to your desktop

Created March 2020
Public