



HP Security Manager

Certificate Management

Overview	3
What is a Certificate?	3
Certificate Use Cases	3
Self-Signed Certificates	3
Identity Certificates	5
CA Certificates	6
Certificate Authorities (CA)	6
Creating a Certificate Request Using EWS	7
Using Security Manager to Manage Identity Certificates	8
Certificate Authority Access Details	9
Certificate Authority Template Access	10
Certificate Revocation Lists	15
General CRL Knowledge	15
Certificate Revocation	16
CRL Distribution Point (CDP)	17
Security Manager Certificate Policy Settings	19
Microsoft Enterprise	19
Microsoft Standalone	24
Symantec	24
OpenTrust	25
SCEP Connector	27
EST Connector	30
Certificate Assessment Detail	31
Initial Certificate Assessment	31
Initial Certificate Remediation	32
Subsequent Certificate Assessment & Remediation	33

Security Manager Assessment Behavior (CRL).....	33
Using Security Manager to Manage CA Certificates	37
Troubleshooting Certificate Remediations	40
Summary	40
Appendix A	41
Symantec Certificate Authority.....	41
Setting Up the Symantec PKI Service.....	42
OpenTrust Certificate Authority.....	46
Installing the root and client certificates	46
Creating the Security Manager Policy	47
Appendix B.....	48
Links to other HP Security Manager Whitepapers.....	48

Overview

Digital certificates are a primary foundation of security providing authentication and encryption between two nodes. HP printers use certificates for authentication in a variety of use cases such as IPPS, IPSEC, 802.1x, etc. Installing and managing certificates through a device's embedded web server (EWS) can be a tedious and time-consuming venture for a fleet of devices. This document explains the importance of certificates as they pertain to HP Jetdirect devices and how HP Security Manager (HPSM) provides an excellent avenue for managing certificates on a fleet of devices.

What is a Certificate?

Certificates are used on HP printers to provide the following:

- Authentication/trust - verifies the identity of a recipient which ensures that information is only available to the intended audience.
- Encryption - disguises information so that unauthorized readers are unable to decipher it.

The most common use of a digital certificate is to verify that a client sending a message is who it claims to be, and to provide the receiver with the means to encode a reply. In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

Certificate Use Cases

Common use cases for certificates include:

- Self-signed certificates are a security audit failure.
- The deployment of a secure printing protocol / encrypted data with trusted destination (ex. IPPS)
- The deployment of certificates as an 802.1x best practice. (ex. EAP-TLS)
- Using both the CA certificate and Jetdirect certificate for IPsec.

Some of these use cases involve one-way trust between client and server where the client must prove its identity to a server in order to pass data. Others involve mutual authentication where a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.

Self-Signed Certificates

By default, HP Jetdirect creates a "self-signed" certificate the first time it is powered on. This certificate is not secure for identity purposes because it has not been signed by a trusted Certificate Authority (CA). An important step in the security of a Jetdirect product is to replace the default self-signed Identity certificate with one that has been signed by a trusted CA.

Information General Copy/Print Scan/Digital Send Fax Supplies Troubleshooting Security HP Web Services **Networking**

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

Authorization

Certificates Access Control

Certificates are used to identify devices on the network.

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

Status: **Installed**
 View... Configure...

CA Certificate
 A Certificate Authority (CA) certificate is required for some authentication metho

Status: **Installed**
 View... Configure...

Jetdirect Certificate Contents

Version:	3 (0x2)
Serial Number:	61:00:00:00:20:07:3d:56:76:1b:a9:4e:e5:00:00:00:00:00:20
Signature Algorithm:	sha256WithRSAEncryption
Issuer:	
CN:	UPD-TME-SCEP2019-CA-1
O:	net
DC:	UPD-TME
Validity:	
Issued On:	2020-04-09 16:07 UTC
Expires On:	2021-04-09 16:17 UTC
Subject:	
CN:	M575.test
O:	HP
OU:	POU
Public Key Algorithm:	rsaEncryption

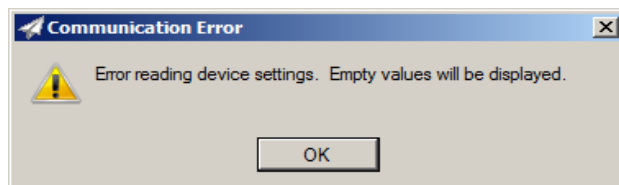
The Jetdirect certificate (identity certificate) on the device has two roles: to provide encryption of the data stream and to provide authentication of the holder of the certificate, the Jetdirect device in this case. In the specific case of the Jetdirect self-signed certificate, both the contents of the certificate as well as how it was signed prevent its use for authentication.

The self-signed certificate can however assist with encrypting data (SSL/TLS) as in secure port communication (HTTPS, IPPS). Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that allow client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

Many tools rely on the presence of at least a self-signed certificate to encrypt data. For example, HP Web Jetadmin will use TLS/SSL for HTTPS communications to devices for some of the device configuration options. HP Security Manager as well will use TLS/SSL for HTTPS communication on many items it assesses and remediates.

NOTE: Before a client and server can begin to exchange information protected by TLS, they must securely exchange or agree upon an encryption key and a cipher to use when encrypting data. The client and the server use the session keys to encrypt and decrypt the data they send to each other and to validate its integrity. If TLS 1.2 is enabled in the operating system and on the device, it will be attempted for use first. The newer operating systems supporting TLS 1.1/1.2 have dropped MD5 as an acceptable hashing algorithm to be used in the handshake. MD5 is a hashing function that converts an arbitrarily long data stream into a hash of fixed size (16 bytes). Due to significant progress in cryptanalysis, MD5 no longer can be considered a 'secure' hashing function. If an SSL negotiation starts with TLS 1.2 and encounters a certificate with "md5withRSAEncryption" for the "Signature algorithm", the connection will fail. Older Jetdirect devices using older Jetdirect firmware, such as those found in older Non-FutureSmart firmware models including HP LaserJet M3035 MFP/M5035 MFP, will default to using MD5 as the signature algorithm for any self-signed certificates that are generated and installed. Newer Jetdirect firmware on these devices will use SHA1 as the signature algorithm for any self-signed certificates that are generated and installed. If the self-signed certificate installed uses MD5 for the signature algorithm, and if TLS 1.1/1.2 is enabled on the device, Web Jetadmin will display an **Error reading Device Settings**.

This same issue can occur in Security Manager for these same Non-FutureSmart devices or any device that defaulted to using MD5 as the hash when the self-signed certificate was first

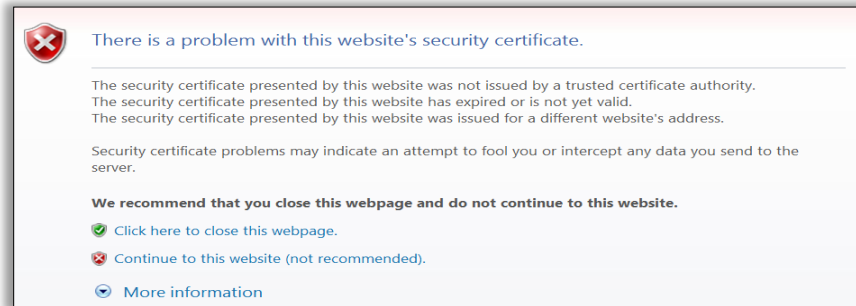


generated, but the status will appear as **Connection Refused** because of the unsupported hash being attempted in the negotiation. Regenerating the self-signed certificate with newer firmware will certainly solve this situation. The very latest HP Jetdirect firmware added a fix to automatically regenerate a self-signed certificate upon startup if MD5 is seen as the hash. Another workaround could include exporting

the self-signed certificate from one of the devices and using a tool such as Web Jetadmin to install it on the affected devices in one easy step. Since self-signed certificates cannot provide authentication/trust, having the same self-signed certificate on multiple devices still provides the desired encryption.

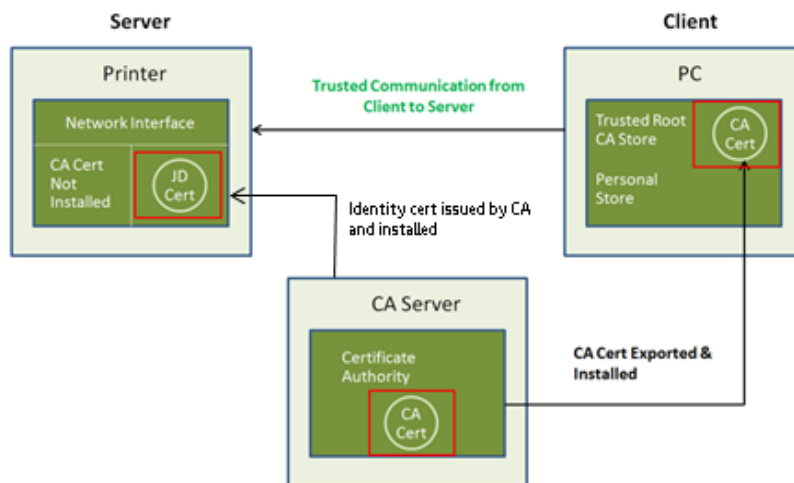
Identity Certificates

Identity certificates (also known as Jetdirect or CA signed certificates) are installed to replace self-signed certificates to provide identity in addition to encryption. Have you ever seen the warning dialog below when using https:// to access a printer in a web browser? This



dialog talks about a “security certificate” being invalid. A security certificate is there to help identify the web site as one that can be trusted. However, the dialog is telling us that we may not want to trust this security certificate – which indirectly means that this web site may not be the web site we think it is. This is because the certificate on the printer is a self-signed Jetdirect certificate, which is the Jetdirect device saying “you can trust me because I say I am Jetdirect.”

An identity certificate that is signed by a Certificate Authority can be generated and installed on the printer to eliminate this message (once the client machine has knowledge of the Certificate Authority through something called a “CA certificate” being installed). Since Jetdirect only has one Identity certificate that can be configured, it must be capable of being used in a variety of situations. Jetdirect can act as a client or a server, depending on the protocol being used. For instance, if a web browser is using HTTPS to communicate to Jetdirect, Jetdirect will return its Identity certificate as part of the SSL/TLS negotiation process, which will identify Jetdirect as a server. IPPS also involves a client pc submitting a job to Jetdirect as the server and using the Jetdirect identity s=certificate for authentication. These are both examples of one-way trust or authentication. In other cases, like EAP-TLS in 802.1x environments, Jetdirect will send its Identity certificate for client authentication to access a protected network. This would be an example of **Mutual Authentication** in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.



CA Certificates

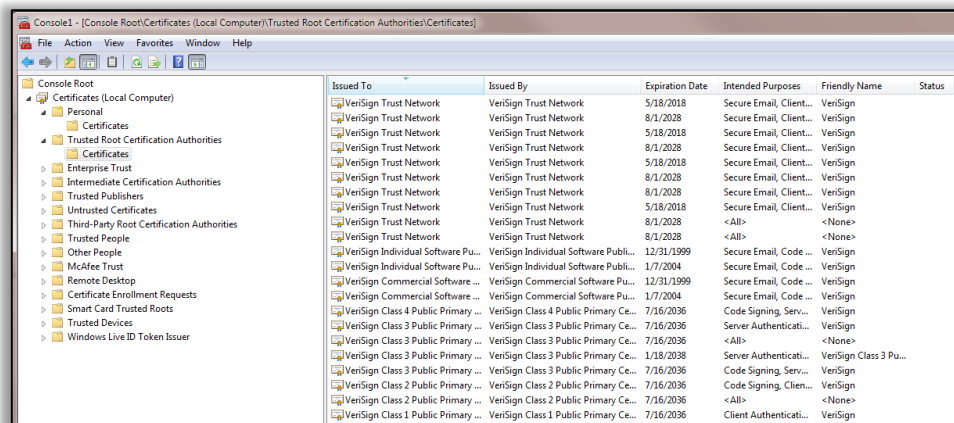
HP Jetdirect can store an Identity certificate and a CA (Certificate Authority) certificate. The CA certificate tells Jetdirect which identity certificates should be trusted (i.e. must be signed by that CA) when Jetdirect is receiving a certificate from another entity. Jetdirect's identity certificate is the certificate that is sent out when another entity requests it. It is important to note that the CA certificate on Jetdirect is configured strictly to provide the trust point for identity certificates that are sent to Jetdirect – the identity certificates received from other entities must be signed by that CA or be part of a chain which ends in that CA. Think of the CA certificate as the self-signed certificate of the certificate authority. Once this CA certificate is installed, any identity certificates signed by that certificate authority can be trusted.

Certificate Authorities (CA)

When browsing to various online shopping web sites, the reason those sites can be trusted is that the browser includes CA certificates for those sites from well-known certificate authorities such as Verisign.

There is usually a difference between Internet trust using certificates and Intranet trust using certificates. Internet trust involves well-known certificate authorities such as Verisign and Entrust. However, Intranet models usually revolve around Microsoft's Certificate Authority that comes with Windows 2003 server and beyond. Each company establishes their own Public Key Infrastructure (PKI) that includes an entire policy around certificates.

When creating a certificate request from either the embedded web server (EWS) of a device or Security Manager, the request is submitted to a Certificate Authority and a certificate is



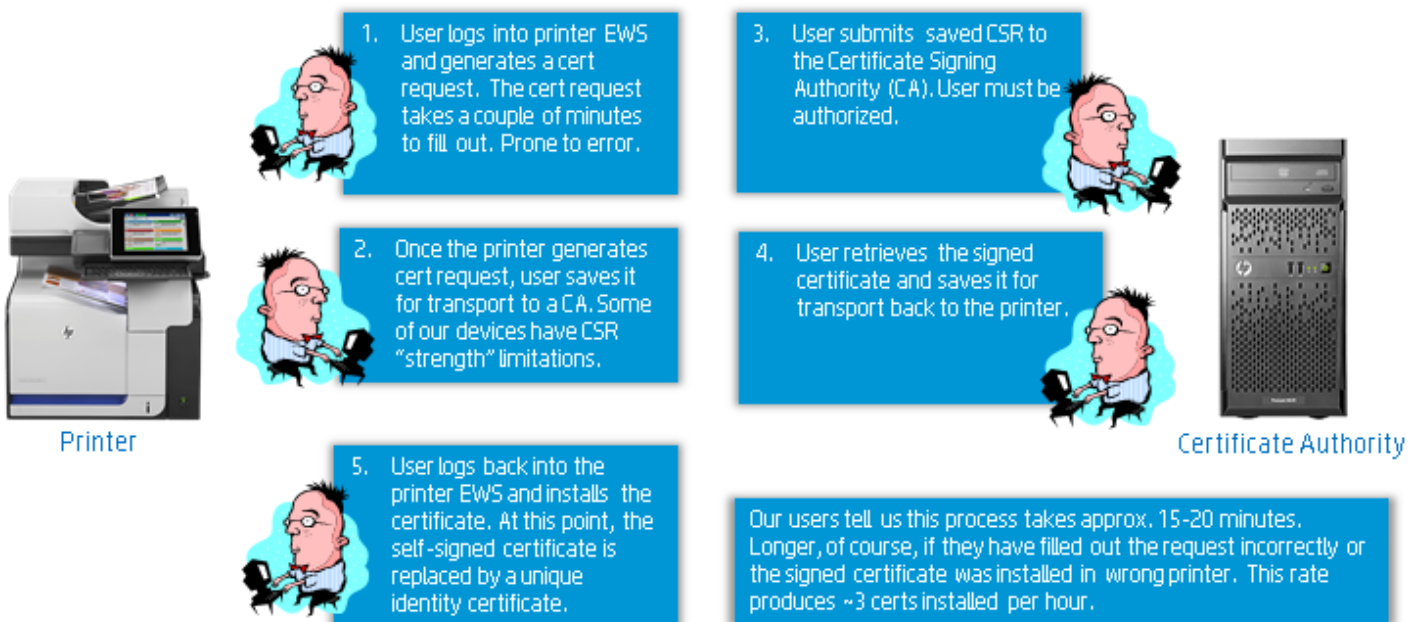
returned. Microsoft, Symantec and OpenTrust Certificate Authorities are supported by default in Security Manager, but the architecture is present for plug-ins to be developed and added to Security Manager to support other Certificate Authorities as required. See the Appendix for information specific to Symantec and OpenTrust. This remainder of this document focuses on Microsoft Certificate Authorities. For Microsoft Certificate Authorities, machine to machine access needs to be provided between Security Manager and the Certificate Authority with rights to submit requests. Both Enterprise and Standalone Microsoft Certificate Authority types are supported. Enterprise requires the Active Directory service. When you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. Enterprise Certificate Authorities require a certificate template and a CSR to generate a certificate and are typically setup to automatically generate certificates from received requests.

Standalone Certificate Authorities are primarily intended to be used as Trusted Offline Root CAs in a CA hierarchy. (ex. staging, etc.). Standalone Certificate Authorities do not require certificate templates.

Typically intermediate authorities that can be trusted back to root will be setup for generating certificates on behalf of the root CA.

Creating a Certificate Request Using EWS

Anyone who has ever attempted to install an identity certificate (Jetdirect certificate) using EWS would appreciate any other technique that can save time and effort. The image below demonstrates the steps required to install just one Jetdirect certificate on a device using EWS. Imagine having to follow these steps for 1000 devices one at a time via EWS. Even in cases where all steps are performed without error or issues, each device can take upwards of 15 minutes to complete even with a streamlined technique for delivering requests to the CA and retrieving certificates in return. Some steps are quite error prone and may require starting the entire process again. It is easy to see why administrators who have to install identity certificates need an easier technique to do so for a fleet of devices.



Step 1 above involves logging into EWS for a device via browser, selecting **Networking, Authorization, Certificates**, selecting **Configure** under **Jetdirect Certificate** and filling out a form.

The screenshot shows the 'Authorization' page in the HP EWS interface. The 'Certificates' tab is active, and the 'Jetdirect Certificate' is shown as 'Installed'. There are two main sections: 'CA Certificate' and 'Create New Self-Signed Certificate'. The 'Create New Self-Signed Certificate' section has a 'Create Certificate Request' button highlighted with a red arrow. Below this is a form for 'Certificate Information' with fields for 'Common Name', 'Organization', 'City/Locality', and 'State/Province'. A 'Next >' button is also highlighted with a red arrow.

The form itself can take time to complete and is prone to error especially when completing many times over. The **Common Name** will be either an IP Address or hostname, and whatever is chosen must be used when attempting to communicate to the device using the certificate. Once the form is complete, a private key is stored on the device, and the certificate request (CSR) is saved to file and delivered to the Certificate Authority (CA). The CA takes the request and generates the certificate. This may be automatically created or may require administrator intervention to process the request depending upon how the CA was setup. Now the certificate is retrieved and imported into the browser assuming the user has not navigated off the EWS page where the CSR was generated. A new radio button to **Install certificate** should now be present on the **Certificate Options** page. If it is not, that means EWS was navigated away from this page or EWS timed out waiting for input, which means the whole process needs to start over again. If Install certificate does appear, check that button, proceed to browse to where the certificate resides and install it. Imagine performing these steps over and over again for a fleet of devices and it is likely the first attempt to perform this on a fleet will be the last.

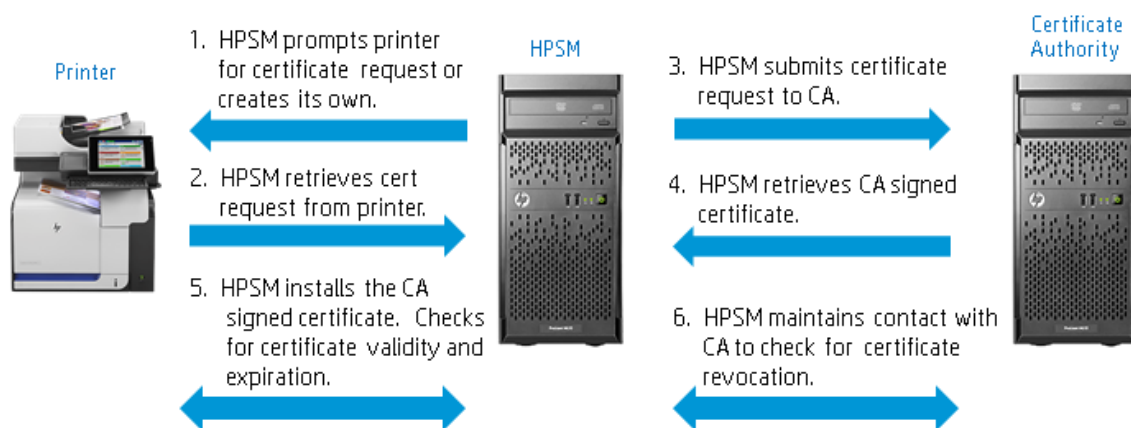
Using Security Manager to Manage Identity Certificates

Now there is a tool (Security Manager) that can not only eliminate the tedious manual task of installing certificates one at a time using EWS but also manages the certificates on the fleet to replace them before expiration or in cases where they have been revoked or deleted. The benefits of using a solution such as Security Manager to install certificates instead of EWS include:

- ❑ Remediation is a ~1-2 minute per device “background” process vs a 15-20 minute highly interactive, error prone, scheduled process.
- ❑ Automatically assesses for missing, invalid, expired and revoked certificates. Remediates as necessary.
- ❑ Security Manager can create a CSR that the device can’t create (encryption algorithm/key length).
- ❑ Security Manager uses device database information to allow certificate-based connection via IP address or hostname.

- ❑ Security Manager incorporates the certificate management solution into the standard assess and remediate lifecycle. Not a separate add-on or plug-in.

The image below illustrates the steps required to install certificates on the entire fleet of devices. Remember, these steps are performed only once to accommodate the entire fleet vs. the previous steps for EWS where the steps must be performed over and over for each device one at a time. Imagine the time savings that can be gained by using a tool such as Security Manager not to mention the reduction in potential errors.

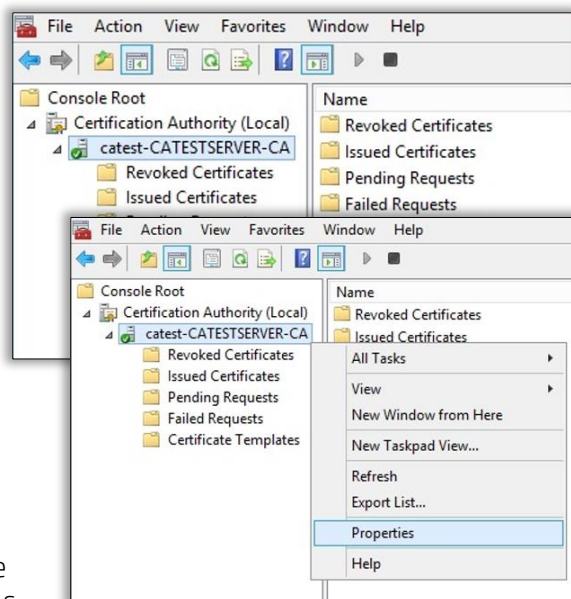


Certificate Authority Access Details

HP Security Manager must make itself known to the designated Certificate Authority (CA) in order to generate requests for signed certificates. The CA typically utilizes the information sent in the certificate request to authenticate the certificate requestor. The HP Security Manager service runs as **NT AUTHORITY/NETWORK SERVICE** by default.

When the service accesses any Security Manager resource across the network, it uses an account named **<Domain Name>\<Computer Name>\$** as the service computer's credentials. This account must have access to the Certificate Authority to allow Security Manager to request signed certificates. The Certificate Authority management console (user interface) provides the name of the Certificate Authority. This name differs from the server hostname that hosts the Certificate Authority. Both the server hostname and CA name is required when configuring a Security Manager policy for certificate assessment. In the following image, the CA is named **catest-CATESTSERVER-CA**.

Note: The Certification Authority management console is the MMC snap-in used to administer and manage CAs.



To begin the process of granting Security Manager access to the designated CA, select the CA name, right-click, and select **Properties**.

Next, with **Authenticated Users** highlighted, select the **Security** tab, click **Add**.

Select **Object Type**, then select **Computers**.

Select **OK** and enter the Security Manager server hostname in the **Object Names** field.

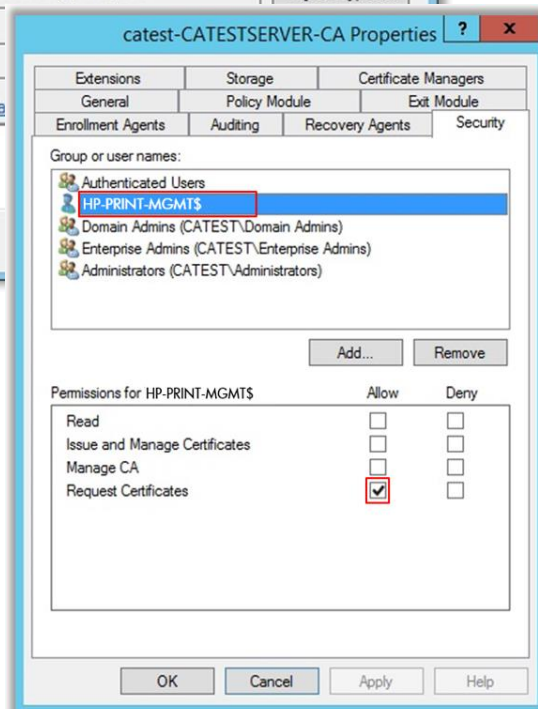
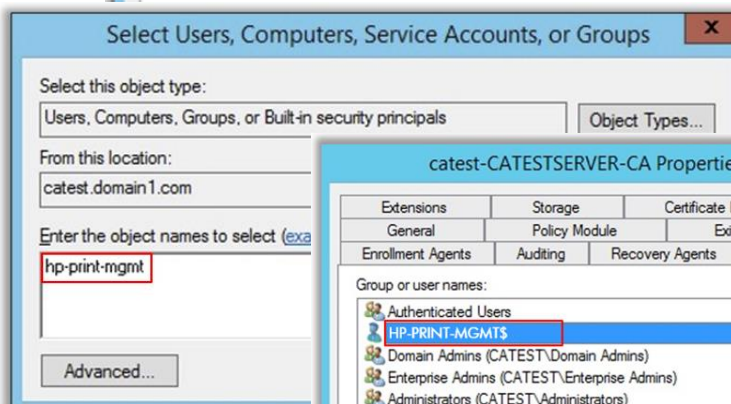
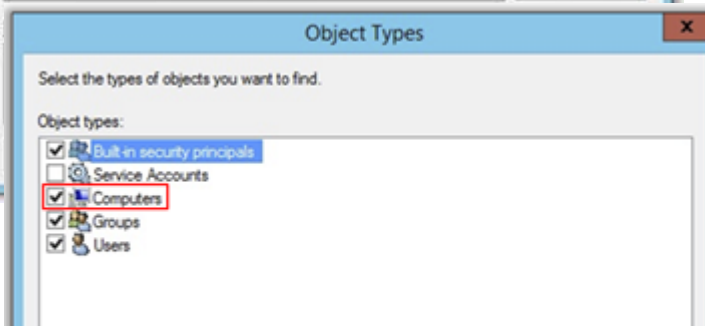
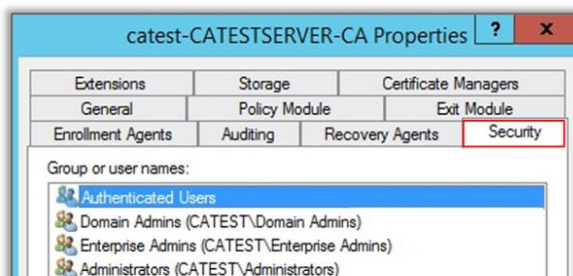
Note: (**hp-print-mgmt**) is the hostname of the Security Manager server in this example. This hostname will be used throughout the remainder of this document.

After selecting **OK**, the **Security** tab window will reflect the hostname of the Security Manager server (**hp-print-mgmt**) followed by a **\$**. Select the box to allow **Request Certificates**.

Note: The **\$** indicates a computer or machine account, not a user account. After selecting **OK**, the Security Manager server (**hp-print-mgmt**) will now have access to the CA for the purpose of requesting signed certificates.

Certificate Authority Template Access

A Microsoft Enterprise Certificate Authorities (CA) uses certificate templates to define the format and content of certificates, specify which users and computers can enroll for which types of certificates, and define the enrollment process. Microsoft Standalone Certificate Authorities do not require certificate templates. Before certificates can be issued by an Enterprise CA, a certificate template must be referenced in conjunction with the certificate request. When **Enterprise** is selected as the Certificate Authority Type in the Security Manager identity certificate policy settings, a CA authorized template name is required.

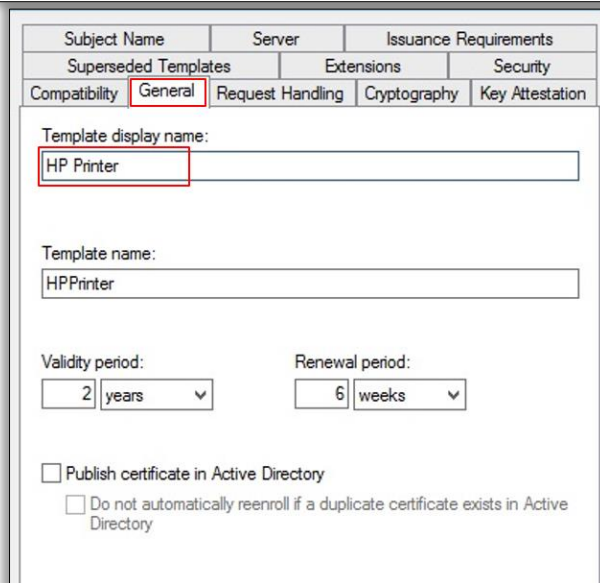
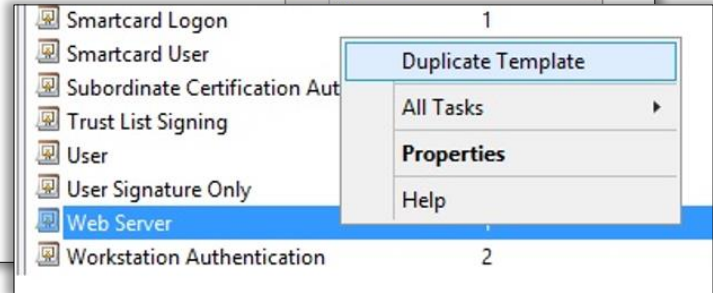
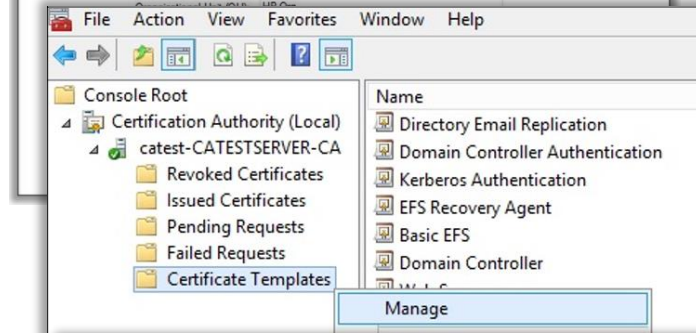
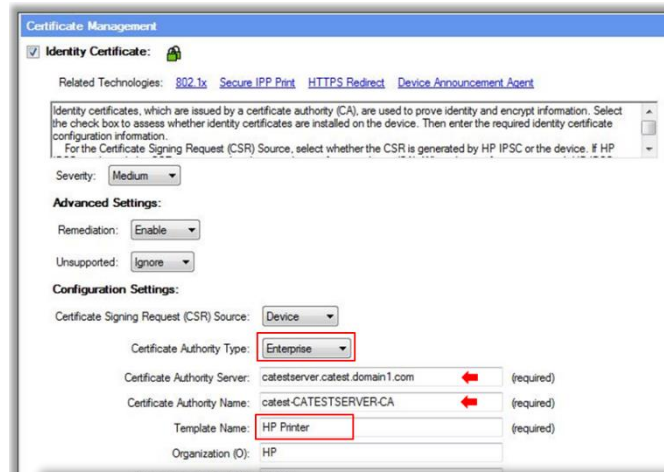


This template must be created at the Certificate Authority and customized for printer certificate generation. Relative to HP printers, identity certificates must have server and client authentication assigned as an application policy extension. The remainder of this section will cover the steps necessary to create the Enterprise CA template to be used by Security Manager. In this example, **HP Printer** will be the name of the certificate template. Begin by performing a right mouse click on **Certificate Templates** and selecting **Manage**.

You will be presented with a list of default and specific templates. Select the **Web Server** default template, right-click, and select **Duplicate Template**.

The next window will represent the properties of the new template that was created as a duplicate of the **Web Server** template. Starting with the **General** tab, enter the name of the new template. As an example, **HP Printer** is used as the new template name.

The **Compatibility** tab helps to configure the options that are available in the certificate template. The options available in the certificate template properties change depending upon the operating system versions that are selected for the certification authority and certificate recipient. Compatibility should be selected in accordance with what is approved for similar CA templates in the customer environment. In this example, **Windows Server 2012 R2** is selected for the certificate authority and **Windows 7/Server 2008 R2** is selected for the certificate recipient. **Show resulting changes** is selected to display the options that were either removed or added based on a change to the certification authority or certificate recipient operating system versions.



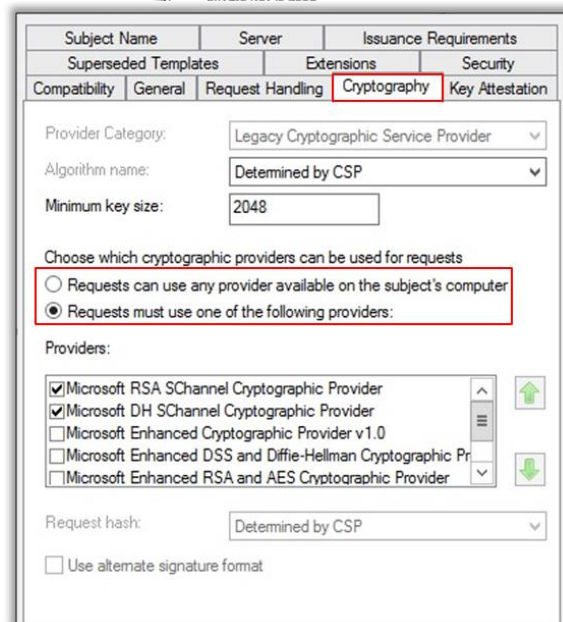
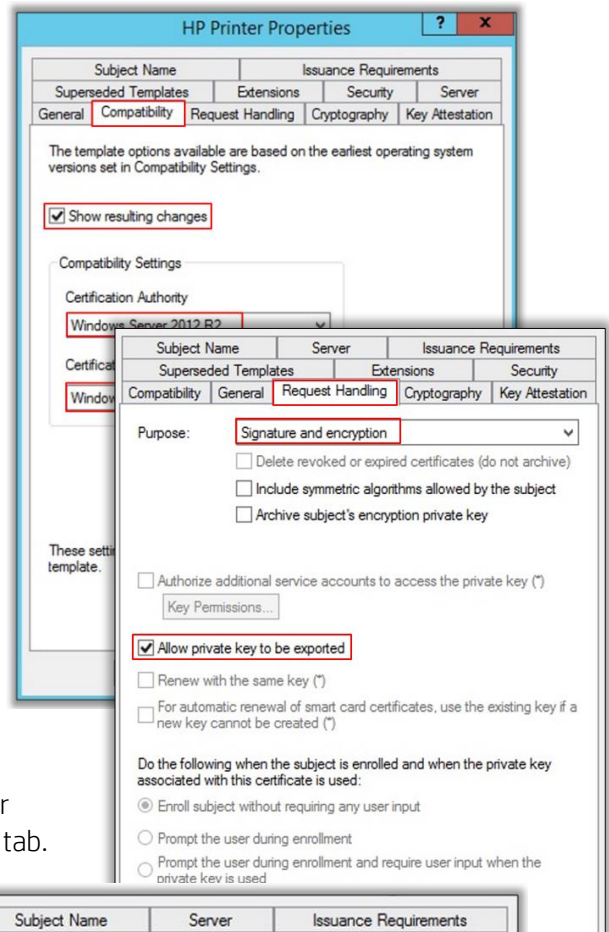
Note: The Security Manager certificate management solution does not support Windows Server 2003 certificate authorities.

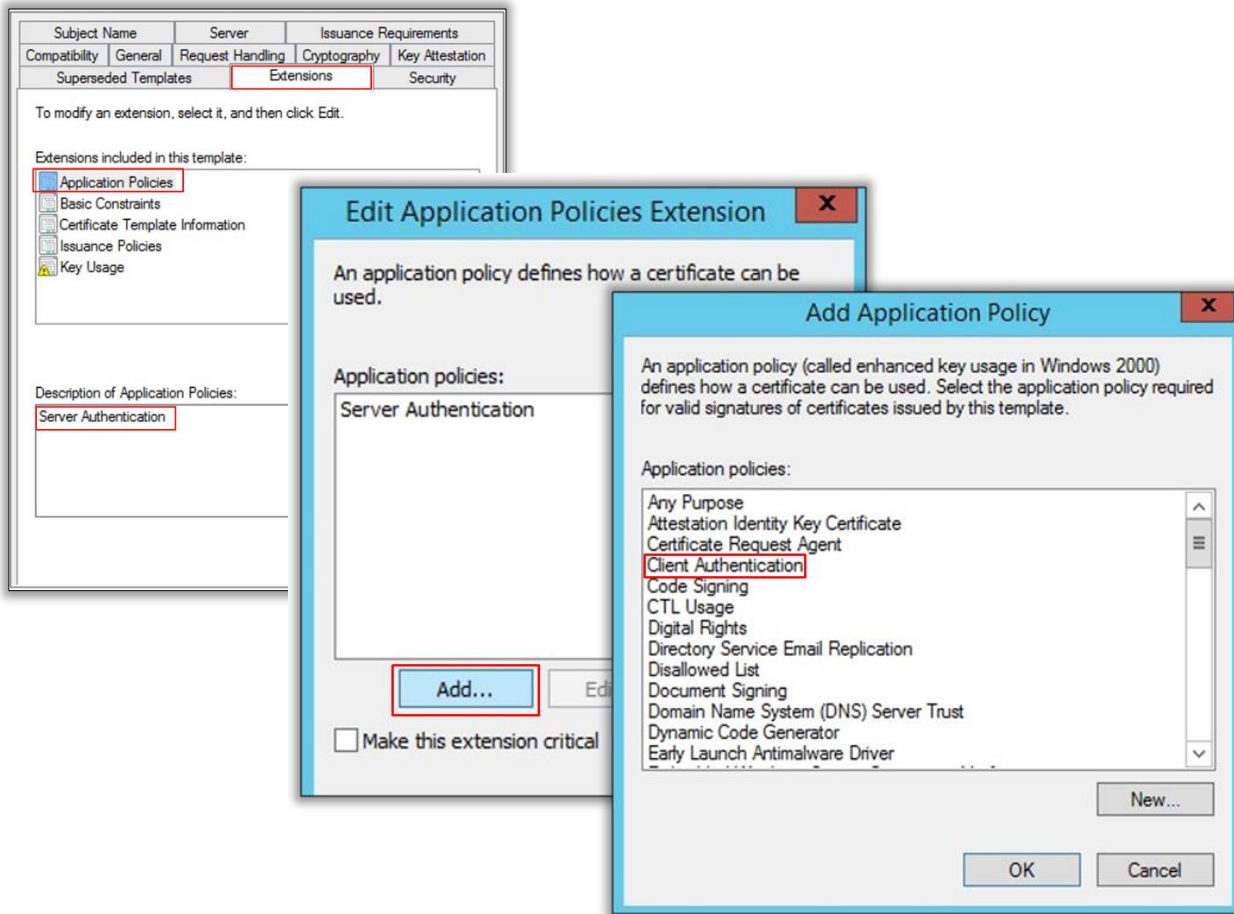
Under the **Request Handling** tab, **Signature and encryption** should be selected as the **Purpose**. **Allow private key to be exported** can be selected or not, it doesn't affect the ability to install certificates.

From the **Cryptography** tab, options exist to select specific or any of the available cryptographic service providers. Cryptographic service providers should be selected in accordance with what is approved for similar CA templates in the customer environment. Windows Server 2012 introduces the option to order the cryptographic service providers (CSPs). When **Requests must use one of the following providers** is selected, the different providers can be selected and ordered. The certificate template administrator can select the providers to make available to the certificate clients and use the up and down arrow buttons to organize those providers in order of preference.

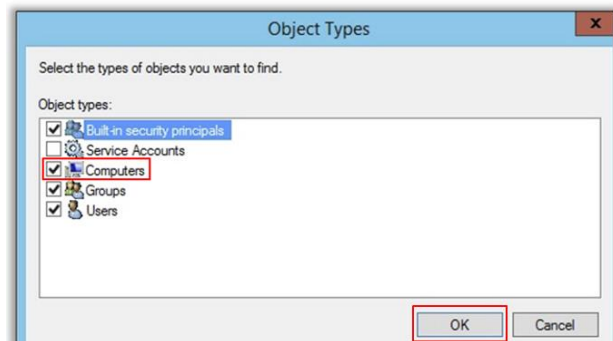
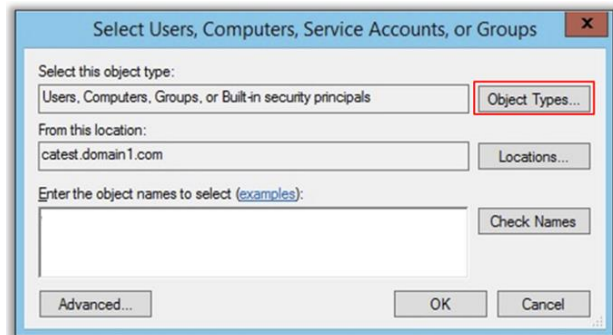
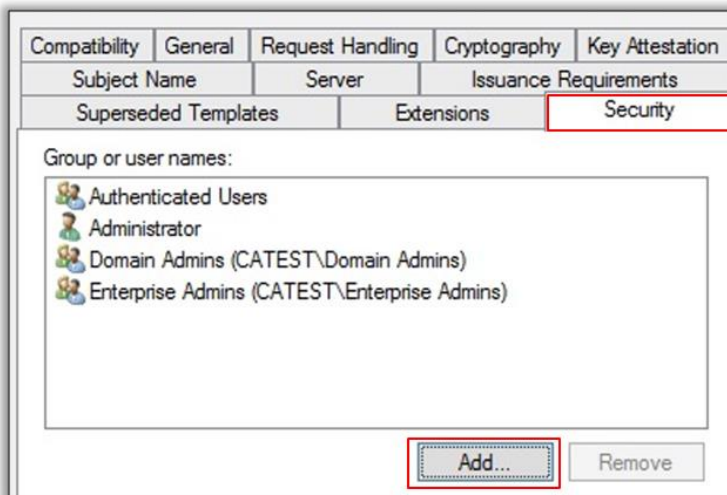
Note: Cryptographic Service Provider configuration on other operating systems may be found on the **Request Handling** tab.

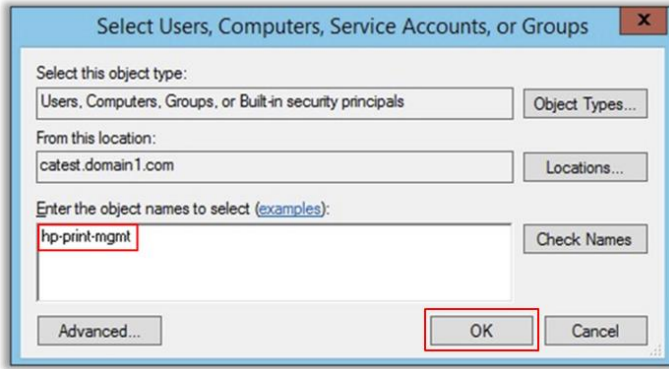
Application policies provide certificate administrators the ability to decide the "purpose" of each deployed certificate. Application policies are sometimes referred to as extended or enhanced key usage. Both server and client authentication are required for HP printer identity certificates. As a duplicate of the **Web Server** default template, server authentication is already included in the new (**HP Printer**) template. However, client authentication will need to be added as an extension. HP printers assume a client role anytime mutual authentication is required. The Security Manager Instant-On Security solution and 802.1x are two examples of possible mutual authentication scenarios. On the **Extensions** tab, select **Application Policies**. You will notice **Server Authentication** is already present. Select **Edit**, then add **Client Authentication**.





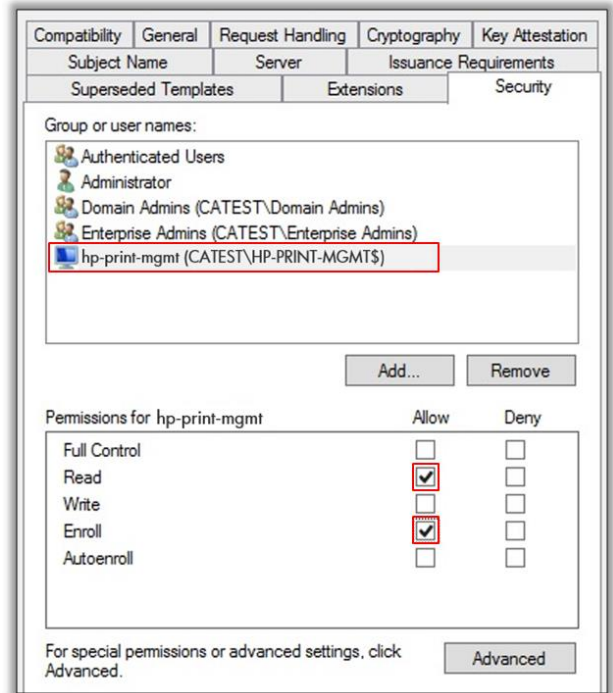
As is the case when granting the Security Manager server “machine” access to the designated certificate authority, Security Manager access to the new template is also required. Navigate to the **Security** tab and select **Add**. Select **Object Types, Computers**, then select **OK**.



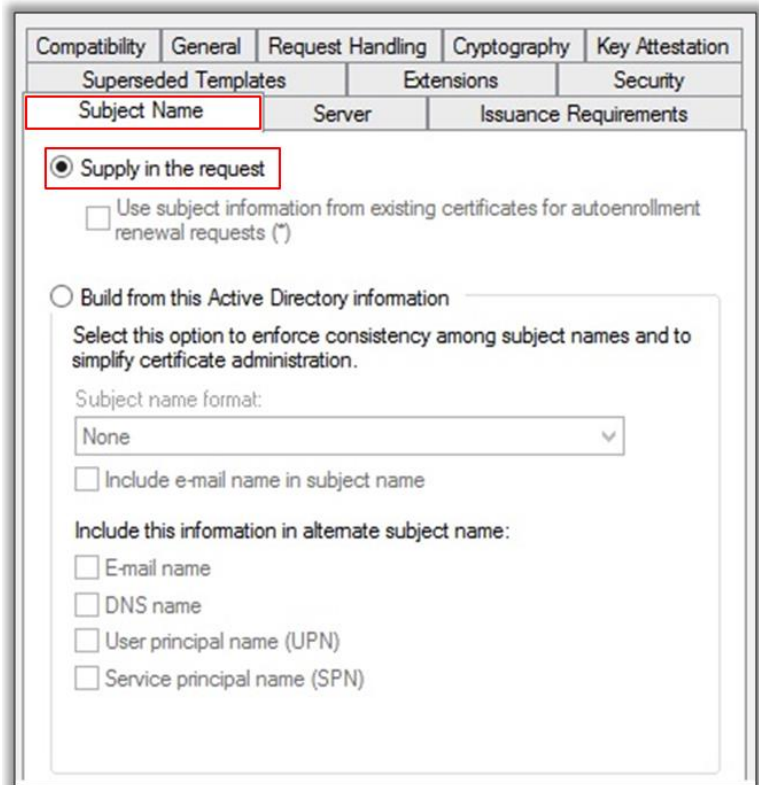


Enter the name of the Security Manager server requiring template access (**hp-print-mgmt**), then select **OK**. Granting the Security Manager server both **Read** and **Enroll** permissions will complete the template access process.

Note: In addition, ensure that **Authenticated Users** has **Read** permission allowed.

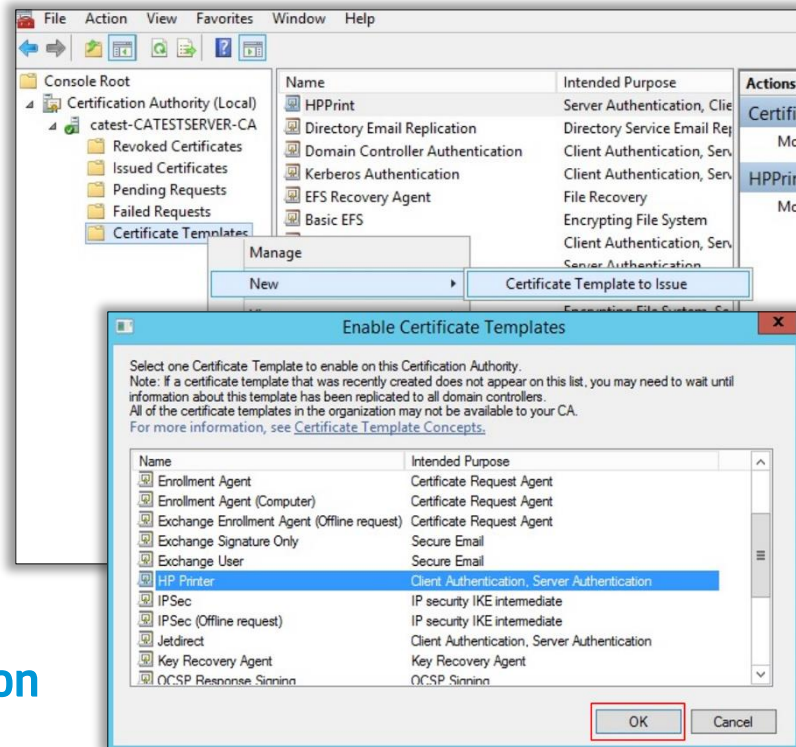


The holder of the private key associated with a certificate is known as the **Subject**. This can be a user, a program, or virtually any object, computer, or service. The **Subject Name** tab allows for great flexibility regarding subject identification. The Windows based CA can build the subject name and/or subject alternate names automatically from subject information stored in Active Directory Domain Services (AD DS) or they can be supplied manually by the subject. Security Manager acts on behalf of the HP printer and handles the requesting of a certificate based on subject information generated directly from the printer or by Security Manager. Either way, the Security Manager Certificate Management solution requires the CA to produce a certificate based on the subject information provided in the Certificate Signing Request (CSR), not from Active Directory. Otherwise, the CA will generate a certificate for the Security Manager server and not the printer if Build from Active Directory Information is selected. Therefore, **Supply in the request** should be selected on the **Subject Name** tab. Security Manager can also provide subject alternate names in the request. At this point, all Security Manager template configuration requirements are met. Configuration



of other tabs under the template properties are left to the discretion of the Certificate Authority administrator.

Now that template configuration is complete, a final step is required to complete the template access process. The new template must be enabled for use. From the Certificate Authority console, right mouse click **Certificate Templates**, select **New**, then select **Certificate Template to Issue**. You will be presented with a list of templates to be enabled. Select the new template (**HP Print**), then **OK**. At this point, Security Manager template access is complete.



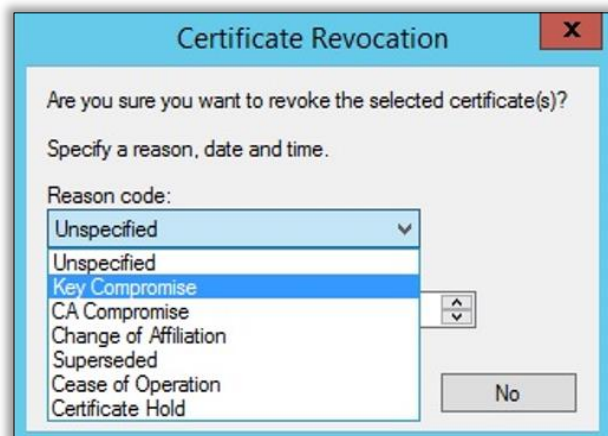
Certificate Revocation Lists

One more tab to configure on the CA is the **Extensions** tab where something called a Certificate Revocation List can be created.

General CRL Knowledge

Certificate Revocation Lists (CRLs) are used to distribute information about revoked certificates to individuals, computers, and applications attempting to verify the validity of certificates. A CRL is actually a list of certificate serial numbers used to identify the revoked certificates and provide some detail about why the certificate was revoked and when. Every certificate is issued with a specific validity period. For example, the issued certificate in the previous image shows a validity period of April 28, 2015 to April 27, 2015. Revoking a certificate invalidates it as a trusted security credential before this validity period expires. The images below provide a list of reasons that could be used to revoke a certificate and details of a revoked certificate.

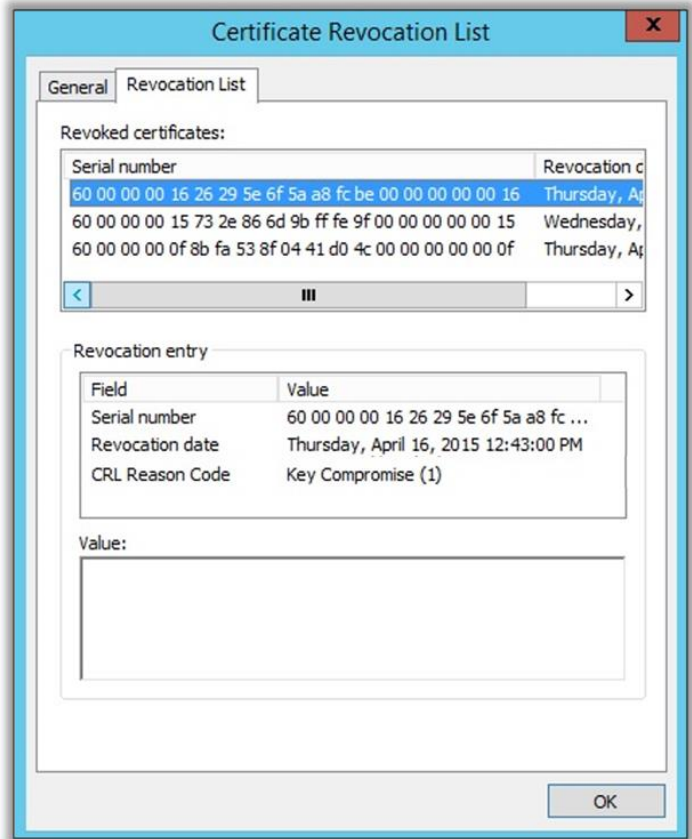
Note: The number one reason for certificate revocation is Key Compromise. In other words, every certificate signed by the CA becomes a security risk because the CA's key was compromised.



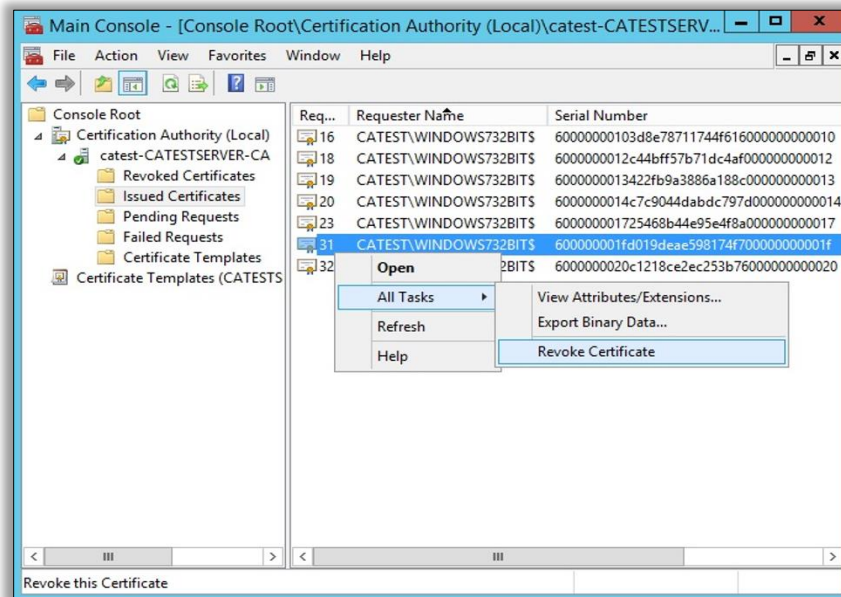
To support a variety of scenarios, Microsoft Active Directory Certificate Services (AD CS) supports industry-standard methods of certificate revocation. These include publication of CRLs and Delta CRLs, which can be made available to clients from a variety of locations, including Active Directory Domain Services (AD DS), Web servers, and network file shares. Depending on the number of certificates issued and revoked by a CA, the CRL can become quite large. Smaller, interim CRLs can also be published to address the size of the full CRL. These smaller CRLs are referred to as Delta CRLs and contain only the certificates that have been revoked since the last published update. The CRL file is itself signed by the authorized CA to prevent tampering. The CRL is always issued by the CA that issues the corresponding certificates.

Certificate Revocation

To understand how the CRL is populated with revoked certificates, the task of revoking a certificate will be briefly covered. Certificate revoking can be performed at the AD CS console or via command line.



AD CS console method: If the CA administrator determines a CA signed certificate must be revoked, the process is fairly simple. Signed certificates are located in the **Issued Certificates** queue targeted for revocation by serial number. After the appropriate certificate is selected, right click and select **Tasks**, then **Revoke Certificate**.



and

All

When a reason for revocation is provided and the certificate has been revoked, it is moved from the Issued Certificates queue to the Revoked Certificates queue. The properties of the revoked certificate will provide new details showing the certificate has truly been revoked.

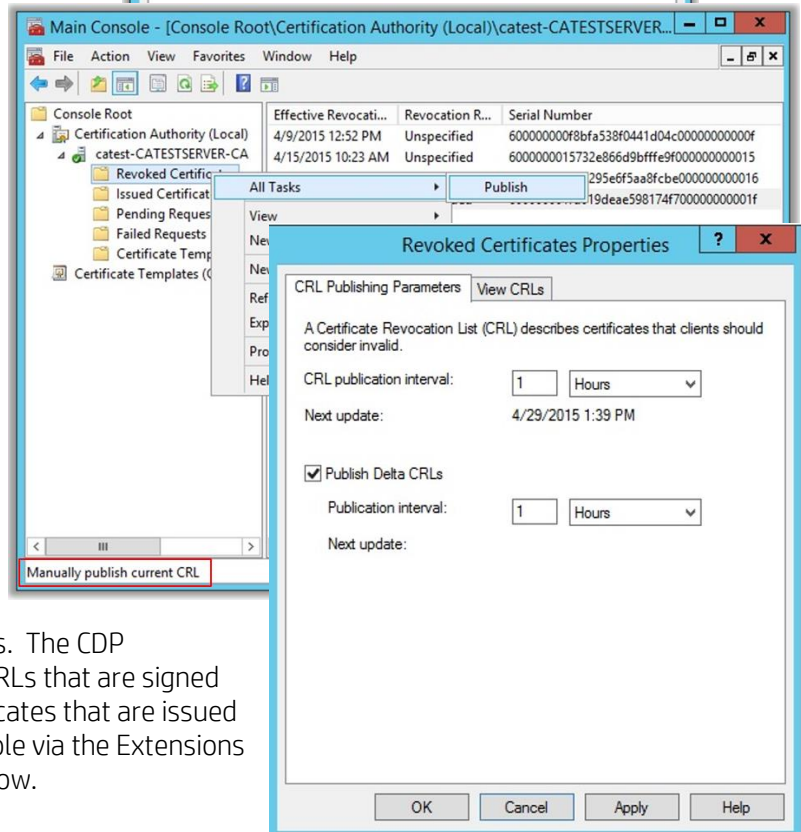
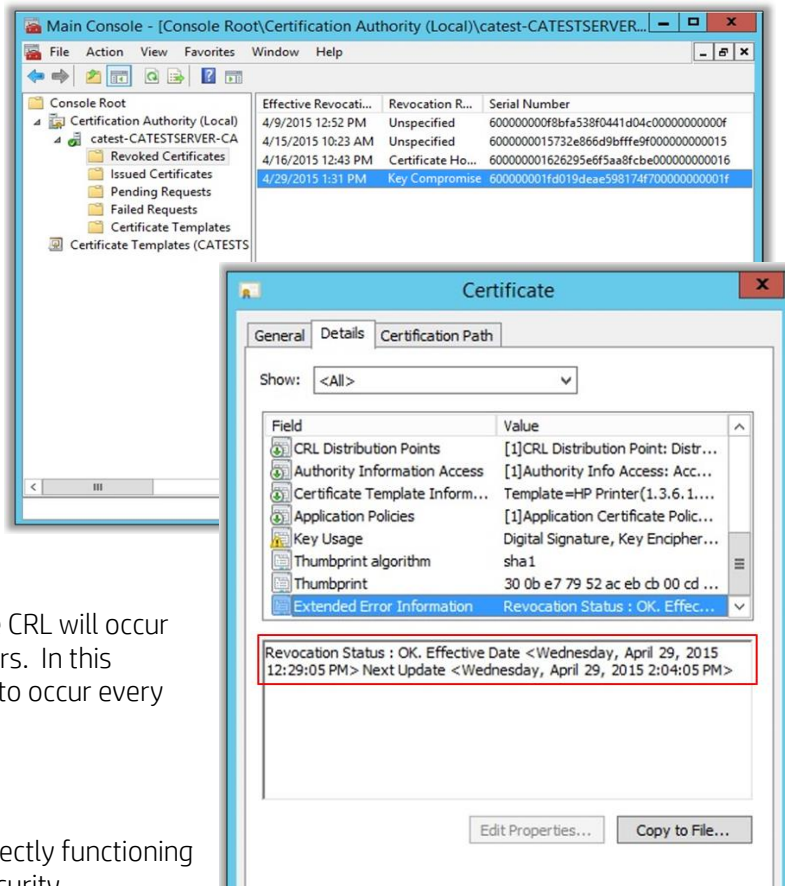
The act of revoking a certificate itself doesn't place the certificate in the CRL until the next publish of the CRL occurs. Publishing of the CRL can occur instantly via a manual "Publish" task.

Otherwise, an automatic publish of the CRL will occur based on the CRL publishing parameters. In this example, the publishing interval is set to occur every hour.

CRL Distribution Point (CDP)

Certificate validation is critical to a correctly functioning public key infrastructure (PKI). As a security best practice, certificate validation should fail if clients aren't able to locate and/or gain access to the CRL to check certificate revocation status. This is the exact behavior of Security Manager that relies upon CRL access to continually assess the CA signed certificate for validity. In the last section, we've walked through the revocation of an issued certificate and the publishing of the CRL to reflect the revoked certificate. So, how does a client receive CRL location information in order to continually validate an installed certificate?

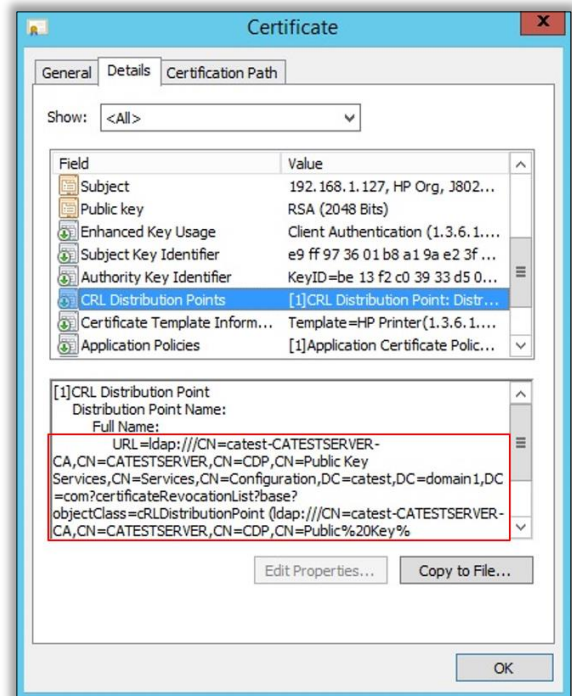
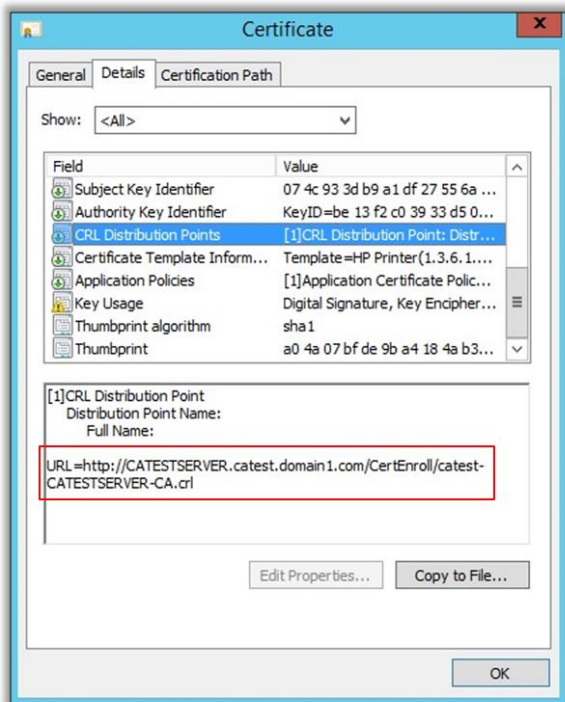
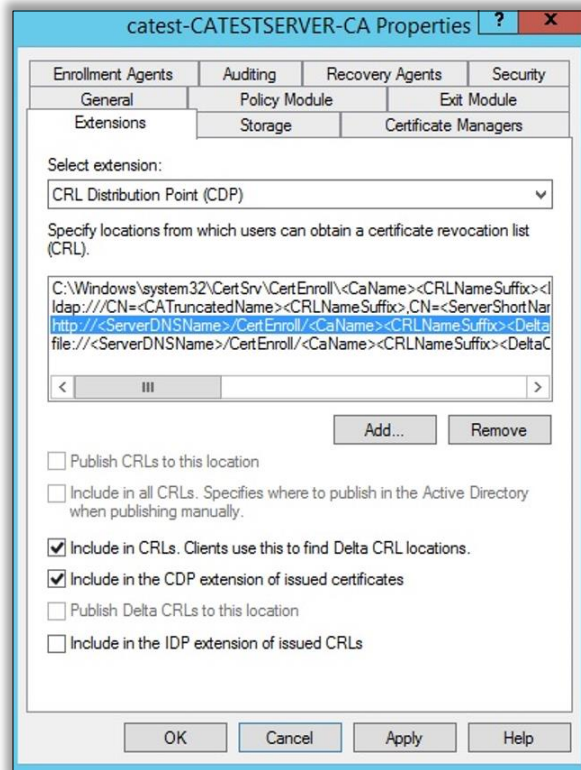
The answer: In the certificate. After a Certificate Authority is installed, CRL Distribution Point (CDP) extensions must be configured before the CA issues any certificates. The CDP extension specifies where to find up-to-date CRLs that are signed by the CA. These extensions apply to all certificates that are issued by that CA. Configuring the CDP is made possible via the Extensions tab of the Certificate Authority properties window.



CDP repositories can either be an LDAP or HTTP location. This example shows CDP configuration if CRL access is to occur via HTTP. The CDP information is included in the certificate when it is issued by the Certificate Authority.

Any client receiving a signed certificate from this CA would use this CDP information to access the CRL. The image below provides another example of CDP information, this time using LDAP.

There are advantages to using HTTP over LDAP and vice versa. One of the advantages of using LDAP as a repository is the high availability of the CRL through Active Directory replication to all domain controllers in the forest. One of the advantages of using HTTP is because it is firewall friendly and typically doesn't require authentication. Many customers configure both HTTP and LDAP methods of access for redundancy and comfort level. Now that basic certificate revocation has been covered, the next section will cover the Security Manager assessment behavior as it relates to CRL access.



Security Manager Certificate Policy Settings

The identity certificate policy setting offers a choice of the following certificate authorities:

- Microsoft Enterprise
- Microsoft Standalone
- OpenTrust
- Symantec
- SCEP Connector
- EST Connector

Each certificate authority selection offers unique settings to manage identity certificates.

Microsoft Enterprise

The image below provides a graphic representation of the configurable identity certificate settings found in the Security Manager policy editor when Microsoft Enterprise is selected as the Certificate **Authority**. An explanation of the pertinent settings is provided below the image.

Identity Certificate

Security Manager Settings

Severity: Low Medium High

Remediation: Disable Enable

Unsupported: Fail Ignore

Device Settings
*Required

Certificate Authority: MS StandAlone

Certificate Signing Request (CSR) Source: Best Possible

Organization (O):

Organizational Unit (OU):

City (L):

State (ST):

Country (C): No Value

Certificate Authority Server: *

Certificate Authority Name: *

Include Subject Alternative Name: Disable Enable ⓘ

UPN User Name: ⓘ

Domain Name: ⓘ

Key Length: 2048

Certificate Request Signature Algorithm: SHA-256

Renewal Threshold (days): 15 *

1. Certificate Signing Request (CSR) Source

This setting allows the administrator to select between **Device**, **HP Security Manager**, or **Best Possible** as the source of the actual certificate request. When **Device** is selected, Security Manager will prompt the device to generate the CSR. Knowledge of the private key remains with the device and Security Manager does nothing more than pass the CSR to the CA for signing and issuance. When **HP Security Manager** is selected, Security Manager actually becomes the source of the request. Security Manager will have knowledge of the private key as the source of the request. After installing the signed certificate, Security Manager will remove knowledge of the private key. Why select **HP Security Manager** as the CSR source? When **HP Security Manager** is selected as the CSR source, stronger encryption algorithms and key lengths become available. Key length choices are **1024, 2048, 4096**

and 8192. Algorithm choices are **SHA-1, SHA-256, SHA-384 and SHA-512.** When **Device** is selected, CSR strength is now limited by what the device is capable of generating. When **Best Possible** is selected, Security Manager will choose between **Device** and **HP Security Manager** to match the desired settings on a device by device basis. Therefore, if a device cannot generate the desired CSR strength in the CRS, HP Security Manager will automatically be used as the best possible choice for that device.

Note: Many HP device models can accept a stronger, more secure certificate than what they can generate a request for. Choosing **HP Security Manager** as source also allow for generation of Subject Alternate Names (SANs) as explained below.

2. Certificate Authority

The Security Manager Fleet Certificate Management solution supports Microsoft Standalone and Enterprise Certificate Authorities. Symantec Certificate Authorities. Or OpenTrust Certificate Authorities. As a point of reference, Enterprise CAs are the most widely deployed and essentially dependent on Active Directory to store and replicate certificate data, while a Standalone CA stores its certificate data in a shared folder which can be accessed through a Web URL. The Certificate Authority Type setting allows the administrator to appropriately select the CA implementation to be used for the Security Manager Certificate Management solution. The settings that can be configured will change when a Microsoft CA is selected vs. a Symantec CA. Each selection will dictate which remaining options are displayed for the policy.

3. Organization (O)

This is part of the subject information. From a printing device perspective, subject information is typically based on server and client trusted identity over the network. (For example, secure printing or 802.1x mutual authentication). Subject settings include the **Common Name (CN), 7-Organization (O) 8-Organization Unit (OU), 9-City/Locality (L), 10-State or Province (S) and 11-Country Name (C).**

The **Common Name (CN)** identifies the fully qualified domain name associated with the certificate. It is typically composed of the FQDN or IP address of the device. The certificate is valid only if the request hostname matches the certificate common name. In the Security Manager identity certificate policy settings, you will notice that the **Common Name** field is non-existent. By default, Security Manager devices are resolved to a hostname when discovered. If there is a hostname reference of an Security Manager device in the database, Security Manager will generate the request (CSR) with the hostname in the **Common Name** field. If an IP Address based **Common Name** is desired, the Security Manager discovered device will have to be rediscovered without resolving to a hostname. Without hostname reference in the Security Manager database, Security Manager will generate the request (CSR) with the IP address in the **Common Name** field. The other fields; **OU, O, L, S** and **C** are used to complete the subject information and usually reflect company and location information.

Identity certificate subject settings should be set in accordance with company policy.

Authorization

Certificate Information

Please specify the following values to uniquely identify the certificate. The Certificate Authority will check the fields for accuracy and completeness to ensure that the certificate is being issued to a legitimate organization.

Caution: You are now creating a new certificate request. By doing so, you will be erasing any existing request.

Common Name

Fully qualified domain name or IP Address of the Jetdirect device.

Organization

Full legal name of your company. Do not abbreviate, except for Inc., Corp, etc. (Ex: HP Inc.)

Organizational Unit Specific department or division within your organization. (optional)

Specific department or division within your organization. (optional)

City/Locality

City in which your organization is physically located.

State/Province

State in which your organization is physically located.

Country/Region

Two-character ISO 3166 country/region code. (Ex: "us" for USA).

RSA Key Length:

1024 bits 2048 bits 3072 bits 4096 bits

⚠ To generate a private key on the Trusted Platform Module (TPM), Mark private key as exportable must not be checked and a RSA Key Length of 1024 bits or 2048 bits must be selected.

Signature Algorithm :

SHA1 SHA224 SHA256 SHA384 SHA512

4. Organization Unit (OU)

See above

5. City (L)

See above

6. State (S)

See above

7. Country (C)

See above

8. Certificate Authority Server

The hostname of the server hosting the Certificate Authority to be used by Security Manager is entered here. Fully qualified hostname (FQDN) is preferred to assist in eliminating hostname resolution issues. This can also be an IP Address if hostname resolution issues are feared.

9. Certificate Authority Name

The actual name of the Certificate Authority hosted by the Certificate Authority server is entered here. The Certificate Authority name can be found at the Certificate Authority management console. Type it exactly as it seen in the console. Don't add a domain name and backslash in front as that will only

trigger Microsoft errors. You have already made connection to the server via the Certificate Authority Server entry, this is strictly the name of the CA itself, nothing to do with the domain or server name.

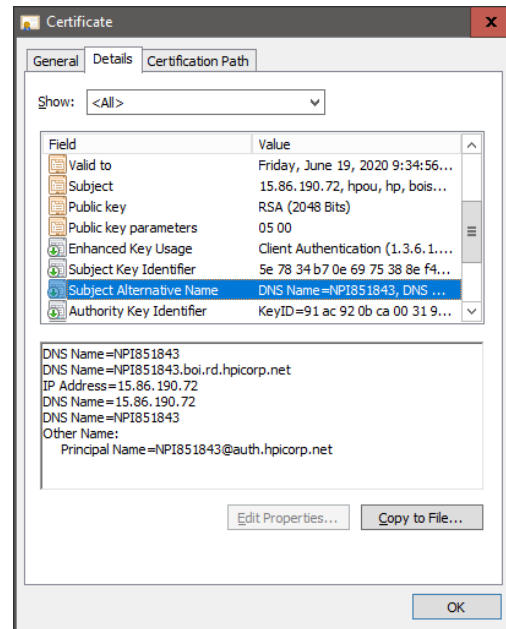
10. Template Name

When **Enterprise** is selected as the CA implementation of choice, a template name is required. This is the name of the template created at the CA to be used in conjunction with the Security Manager Certificate Signing Request. If the **Standalone** CA implementation is selected, the template name field is not enabled because templates are not required by a standalone CA.

11. Include Subject Alternate Name

Subject Alternate Names (SANs) allow for more than one fully qualified domain name to be protected using a single certificate. When this slide bar is enabled, Security Manager will include SANs for IP Address, FQDN, hostname, System Name, and optionally User Principal Name (UPN) into the certificate. One purpose would be to browse to IP Address, hostname or FQDN without receiving an error regarding the certificate being invalid. Another purpose would be to ensure the device can properly validate onto an 802.1x network by having the UPN match the AD User Account or FQDN match the AD computer account.

You must choose HP Security Manager as the CSR Source in order to write SANs into the certificate.



SANs will appear as such on a device if enabled:

- **DNS Name=ats-n-ojx576-df8.boi.rd.hpcorp.net** - this is the FQDN retrieved from DNS. If DNS returns nothing, FQDN is formed by querying SNMP objects for hostname and domain.
- **DNS Name=ats-n-ojx576-df8** - this is the FQDN retrieved from DNS with the domain portion stripped off
- **DNS Name=ATS-N-OJX576-DF8** - this is the device Hostname as seen under EWS
- **IP Address=15.13.175.138** - this is the IP Address
- **DNS Name=15.13.175.138** - this is the IP Address again to accommodate a Microsoft defect
- **DNS Name=8021xname** - this is the 802.1x User name as seen under EWS
- **Other Name: Principal Name=UpnUserName@hp.com**
 this is the UPN constructed by combining 802.1x User Name @domain or UPN User Name @domain

12. UPN User Name

Enter a User Principal Name (UPN) user name in order for a unique and customized UPN User Name to be used to form the UPN Name as a Subject Alternate name. If Domain Name below is entered, a UPN Name will be added to SANs by concatenating the device 802.1x User name with the Domain Name. If UPN User Name is entered, the UPN User name will be used to form the UPN Name as SANs by concatenating UPN User name with Domain Name. This option is useful if only one Active Directory User account is being used for the entire printer fleet for authentication, thus the same UPN Name would be required for every printer to authenticate.

13. Domain Name

Enter a Domain Name in order for a User Principal Name (UPN) to be added as a Subject Alternate name (SAN) into a certificate. UPN is formed by taking the 802.1x User Name from the device and appending the entered Domain Name after an @ symbol.

14. Key Length

Key length is the size measured in bits of the key used in a cryptographic algorithm. The algorithm's key length is distinct from its cryptographic security. Use the drop-down menu to select the desired key length. More selections are available when HP Security Manager is selected as the CSR source.

15. Certificate Request Signature Algorithm

The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. Use the drop-down menu to select the desired hash algorithm to include in the CSR. **Only SHA (Secure Hash Algorithm)** based selections are available.

16. Renewal Threshold (days)


Use this setting to dictate certificate replacement prior to actual certificate expiration. The default is 15 days but should be set to reflect company certificate replacement policy. For testing purposes, you can set this value to 366 and force a certificate replacement during every assessment.

Microsoft Standalone

Microsoft Standalone is identical to Microsoft Enterprise except the Template Name is grayed out as it does not apply to MS Standalone.

Symantec

The image below provides a graphic representation of the configurable identity certificate settings found in the Security Manager policy editor when **Symantec** is selected as the **Certificate Authority**. An explanation of the pertinent settings is provided below the image.


Identity Certificate 



Security Manager Settings

Severity Remediation Unsupported

Low Medium High
 Disable Enable
Fail Ignore

Device Settings
*Required

Certificate Authority 


Certificate Signing Request (CSR) Source  

Organization (O)

Organizational Unit (OU)


City (L)


State (ST)


Country (C) 



Symantec Certificate SubjectName *


Symantec Certificate Profile OID *

Include Subject Alternative Name Disable Enable 

UPN User Name 

Domain Name 

Key Length  

Certificate Request Signature Algorithm 

Renewal Threshold (days) *

17. Symantec Certificate Subject name

18. Certificate profile OID

A Symantec creator is a cloud based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

OpenTrust

The image below provides a graphic representation of the configurable identity certificate settings found in the Security Manager policy editor when **OpenTrust** is selected as the **Certificate Authority**. An explanation of the pertinent settings is provided below the image.

The screenshot shows the 'Identity Certificate' configuration window. At the top, there are three sections: 'Severity' with a slider set to 'Medium', 'Remediation' with a toggle set to 'Enable', and 'Unsupported' with a toggle set to 'Ignore'. Below these is the 'Device Settings' section, which includes several fields and toggles:

- Certificate Signing Request (CSR) Source:** HP Security Manager (dropdown)
- Certificate Authority:** OpenTrust (dropdown)
- Organization (O):** (text input)
- Organizational Unit (OU):** (text input)
- City (L):** (text input)
- State (ST):** (text input)
- Country (C):** No Value (dropdown)
- OpenTrust Certificate SubjectName:** (text input, marked as required with a red asterisk)
- OpenTrust Profile Name:** (text input, marked as required with a red asterisk)
- OpenTrust Endpoint:** (text input, marked as required with a red asterisk)
- OpenTrust Contact Email:** (text input, marked as required with a red asterisk)
- OpenTrust Zone:** (text input, marked as required with a red asterisk)
- Include Subject Alternative Name:** Toggle set to 'Enable' (with an info icon)
- Domain Name:** (text input, marked as required with a red asterisk)
- Key Length:** 2048 (dropdown)
- Certificate Request Signature Algorithm:** SHA-256 (dropdown)
- Renewal Threshold (days):** 15 (text input, marked as required with a red asterisk)

19. OpenTrust Certificate Subject Name

A Symantec creator is a cloud-based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

20. OpenTrust Profile Name

A Symantec creator is a cloud-based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

21. OpenTrust Endpoint

A Symantec creator is a cloud-based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

SCEP URL - Supports either HTTP or HTTPS

22. OpenTrust Connect Email

A Symantec creator is a cloud-based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

23. OpenTrust Zone

A Symantec creator is a cloud-based PKI by Symantec whereby the user creates certificate profiles on the Symantec cloud and specifies an OID in this Certificate profile OID field. A certificate profile is similar to a template used by an Enterprise Microsoft Certificate Authority.

OpenTrust Certificate SubjectName	<input type="text" value="Subject Name of the Client Certificate"/>	*
OpenTrust Profile Name	<input type="text" value="SimpleAuthenticationDecentralized"/>	*
OpenTrust Endpoint	<input type="text" value="https://pki-demo.idnomic.net/RA/connector.cgi"/>	*
OpenTrust Contact Email	<input type="text" value="admin@hp.com"/>	*
OpenTrust Zone	<input type="text" value="hp"/>	*

SCEP Connector

Simple Certificate Enrollment Protocol (SCEP) is an Internet Draft in the Internet Engineering Task Force (IETF). This protocol is used by numerous manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation. SCEP is the most popular, widely available, and tested certificate enrollment protocol. When implemented as a client by HP within Security Manager, this allows HP to integrate with a broad range of certificate authorities, registration authorities and trust platforms whether internal or external if that protocol is enabled. The SCEP connector for Security Manager is designed to be compatible with the draft specification including vendors that support the SCEP protocol/service. While there are risks with implementing/testing draft specifications, HP will assure the initial design and testing verifies compatibility with Venafi and Comodo/Sectigo.

SCEP defines the communication between network devices and a Registration Authority (RA) for certificate enrollment. For example, while Security Manage supports direct communication with Microsoft Certificate Authorities using the DCOM protocol, SCEP can also be enabled on the Microsoft Certificate Authority and

used as an alternative if desired. The Network Device Enrollment Service (NDES) is one of the role services of the Active Directory Certificate Services (AD CS) role. It implements the Simple Certificate Enrollment Protocol (SCEP).

Whether using SCEP with certificate authorities such as Microsoft or “man-in-the-middle” products such as Venafi that exist between the requester and the CA to provide benefits such as on-premise support and in some cases improved compliance enforcement and a common way to swap in other authority types, the rules to request and receive certificates are the same. Security Manager uses the following url <https://localhost/certsrv/mscep> for all communication to the registration authority. Passwords are used by the service to authenticate the device before forwarding its enrollment request to the CA. This password can be obtained dynamically each request through a call to the administration virtual application at https://localhost/certsrv/mscep_admin. Security Manager can use this location to request a dynamic password each time, or the administrator can setup the registration authority to support static passwords. In some environments, such as manufacturing, it may be desirable to reuse the same challenge for more than one device. When the registration authority is configured to use a single static password, Security Manager uses the same password every time that the administrator retrieves using the url above.

Security Manager Settings

Severity



Remediation


Disable Enable

Unsupported

Fail Ignore

Device Settings

*Required

Certificate Signing Request (CSR) Source 

Certificate Authority

Organization (O)

Organizational Unit (OU)

City (L)

State (ST)

Country (C)

SCEP URL *


Enable Static Challenge Password Disable Enable *


Static Challenge Password


SCEP Challenge Password URL *

Server Username *

Server Password *

Include Subject Alternative Name Disable Enable 

UPN User Name 


Domain Name 

Key Length

Certificate Request Signature Algorithm

Renewal Threshold (days) *

EST Connector

Identity Certificate 

Security Manager Settings


Severity Low Medium High



Remediation Disable Enable

Unsupported Fail Ignore

Device Settings

***Required**

Certificate Authority 


Certificate Signing Request (CSR) Source  

Organization (O)

Organizational Unit (OU)


City (L)

State (ST)

Country (C) 

Est URL *


Est Port *


Use Credential Authentication Disable Enable * 


Certificate SerialNumber


Server Username *


Server/Certificate Password *

Include Subject Alternative Name Disable Enable 

UPN User Name 

Domain Name 

Key Length 

Certificate Request Signature Algorithm 

Renewal Threshold (days) *

Certificate Assessment Detail

Security Manager handles certificate assessment in two different ways:

- during initial assessment and self-signed certificate replacement
- during ongoing assessment of the identity certificate that replaced the self-signed certificate

The next section covers both of these methods.

Initial Certificate Assessment

HP printing devices are never without a network certificate. Self-signed certificates are installed by default on HP devices and are primarily used to provide secure web communication (SSL/TLS). Because these certificates are not signed by an approved certificate authority within the customer environment, their identity can't be trusted. After Security Manager has been configured to access the approved customer Certificate Authority, it can be used to replace the self-signed certificate with a CA signed identity certificate.

When the Identity Certificate setting in the Security Manager policy editor is configured similar to what is displayed in the image below, you are ready to replace the HP device self-signed certificate with a CA signed identity certificate. Performing an initial **Assess Only** will compare the installed device certificate (self-signed) to what is desired in the Identity Certificate policy editor settings and report on the assessment recommendations.

Authentication > Certificate Managem...		
Identity Certificate		
Common Name (CN)	Value Mismatch	{Policy: 15.8
Organization (O)	Value Mismatch	{Policy: HP, D
Organizational Unit (OU)	Value Mismatch	{Policy: IPSC
City (L)	Value Mismatch	{Policy: Bois
State (ST)	Value Mismatch	{Policy: ID, D
Country (C)	Value Mismatch	{Policy: US, D
Validity	The certificate chain of trust is invalid due to an untrusted root certificate.	

This recommendation report shows a failed assessment of the device with the self-signed certificate. Explanation as follows:

1. **Common Name Mismatch:** Security Manager expected the hostname of the device, but received a Jetdirect name with a partial MAC address. This is indicative of a self-signed certificate.
2. **Subject Information Mismatch:** Security Manager expected specific values in the Organization, Organizational Unit, City, State and Country fields. Mismatches were presented for all.

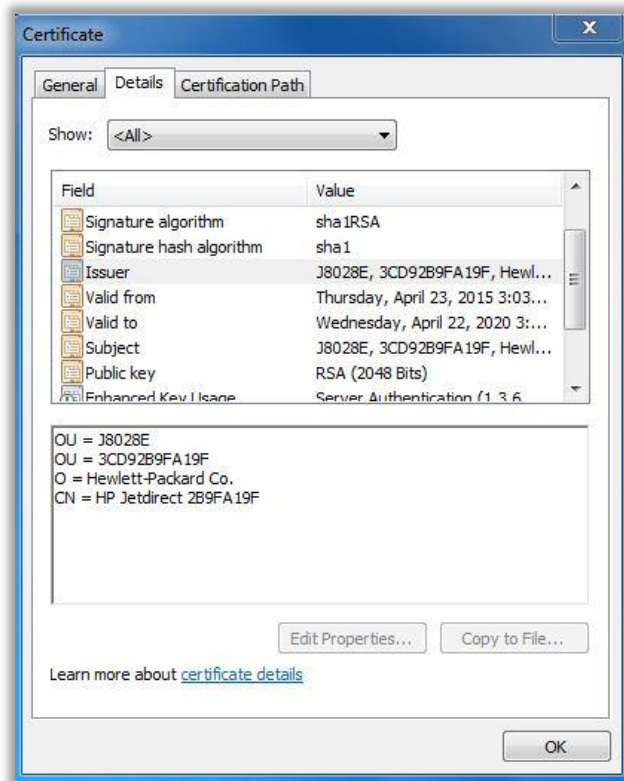
4. **Validity Failure:** Chain of certificate trust couldn't be traced back to the Certificate Authority's root certificate. This is normal failure when the certificate is self-signed.

To verify the accuracy of the recommendations, you can view the self-signed certificate on the device to see how it compares.

From here, you can confirm that Security Manager assessed the certificate correctly as being self-signed (issued by the Jetdirect network interface) and not issued by the customer designated Certificate Authority.

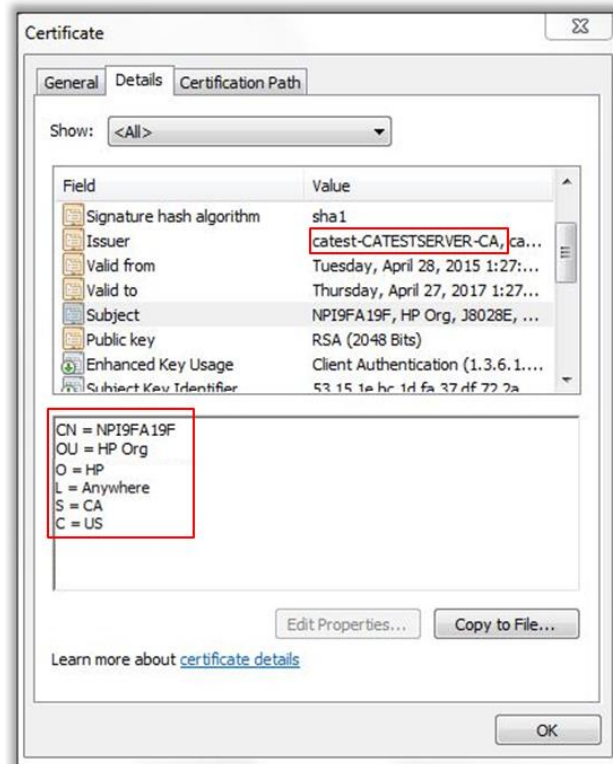
Initial Certificate Remediation

The **Assess Only** task provided an assessment of the device's certificate based upon the Identity Certificate settings in the Security Manager policy editor. If recommendations were provided as a result of the certificate assessment, an **Assess and Remediate** task will then remediate (replace) the installed certificate with a Certificate Authority (CA) signed certificate that is unique to the device and in accordance with the Identity Certificate settings in the Security Manager policy editor. When the **Assess and Remediate** task is launched, Security Manager will handle the remediation of the installed certificate as follows:



1. Security Manager will assess the device based upon the Identity Certificate policy editor settings and determine if remediation is necessary.
2. If remediation is necessary, Security Manager will either prompt the device for a device generated Certificate Signing Request (CSR) or generate a CSR from the Security Manager application, depending on what is selected as the CSR source.
3. The CSR is then submitted to the Certificate Authority (CA) named in the Identity Certificate policy editor settings.
4. The CA processes the CSR and issues a signed certificate back to Security Manager.
5. Security Manager will then install the signed certificate and reassess.
6. If the newly installed certificate is successfully reassessed, the Security Manager status for the device will report as Passed.

When the certificate remediation is complete, verification can be accomplished by viewing the certificate on the device.



Subsequent Certificate Assessment & Remediation

The Security Manager assessment and remediation process is an ongoing task, either scheduled at some customer selectable frequency or through Instant-On Security scenarios. After a CA signed certificate is initially installed on the device and verified by Security Manager, an additional assessment item is included during subsequent assessments of the device. This additional assessment item is the Security Manager check of a published Certificate Revocation List (CRL). Checking the CRL to see if the certificate has been revoked is most certainly a certificate management best practice and a crucial component of maintaining certificate trust. Without the CRL check, a revoked certificate may be incorrectly accepted as valid. To use a Public Key Infrastructure effectively, the Security Manager Certificate Management solution must have access to current CRLs. Information of the CRL is provided (per CA configuration) in the CA signed certificate that was issued to Security Manager. This information consists of CRL location, enabled access methods, and how often the CRL is updated and published.

Note: A regular publication schedule for certificate revocation data is necessary to ensure an up-to-date and accurate CRL is made available to the clients that utilize the list.

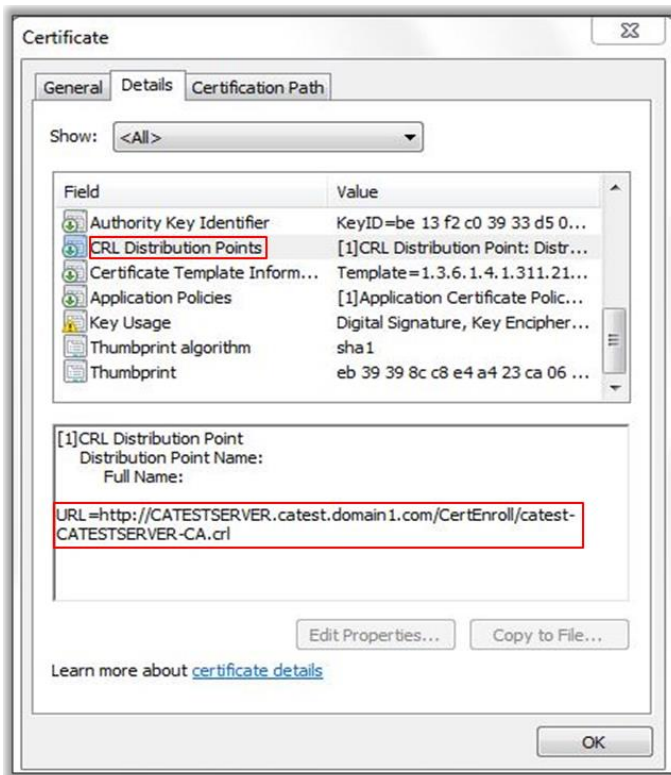
To validate the installed signed certificate, Security Manager uses the CRL information in the signed certificate to access the CRL during subsequent certificate assessments. More CRL knowledge and Security Manager use of CRLs during assessments is covered in the next section of this document.

Security Manager Assessment Behavior (CRL)

As mentioned earlier in this document, the checking of a CRL doesn't occur until after a CA signed certificate is initially installed on the device. Upon the next assessment, Security Manager will use the CDP information provided in the certificate to locate the CRL. If another assessment is performed prior to the next publishing of the CRL, Security Manager won't attempt CRL access. The CDP information was gleaned from the certificate when it was issued to Security Manager, then cached. These next steps will

demonstrate Security Manager assessment and remediation behavior after the device has acquired a CA signed identity certificate:

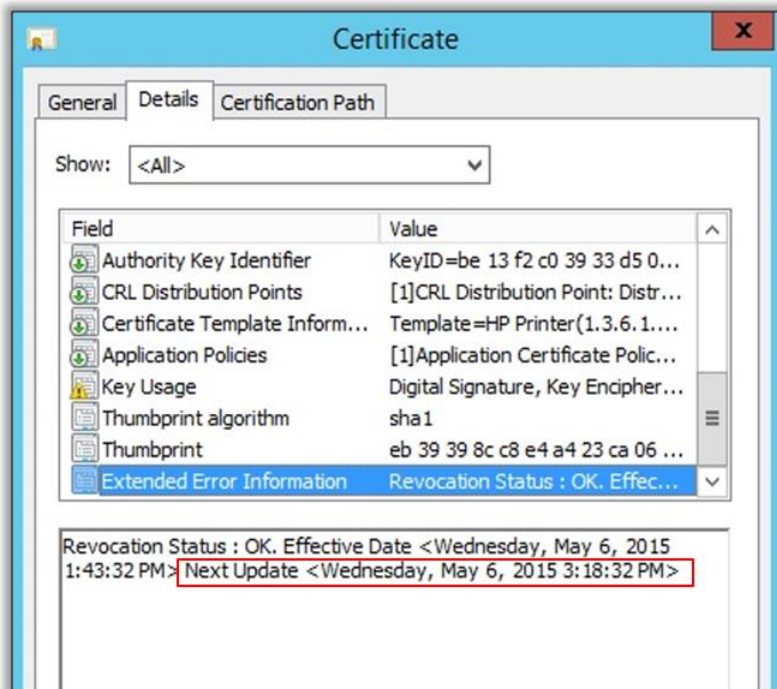
1. The following image shows a snapshot of the CDP information provided in the CA issued certificate.



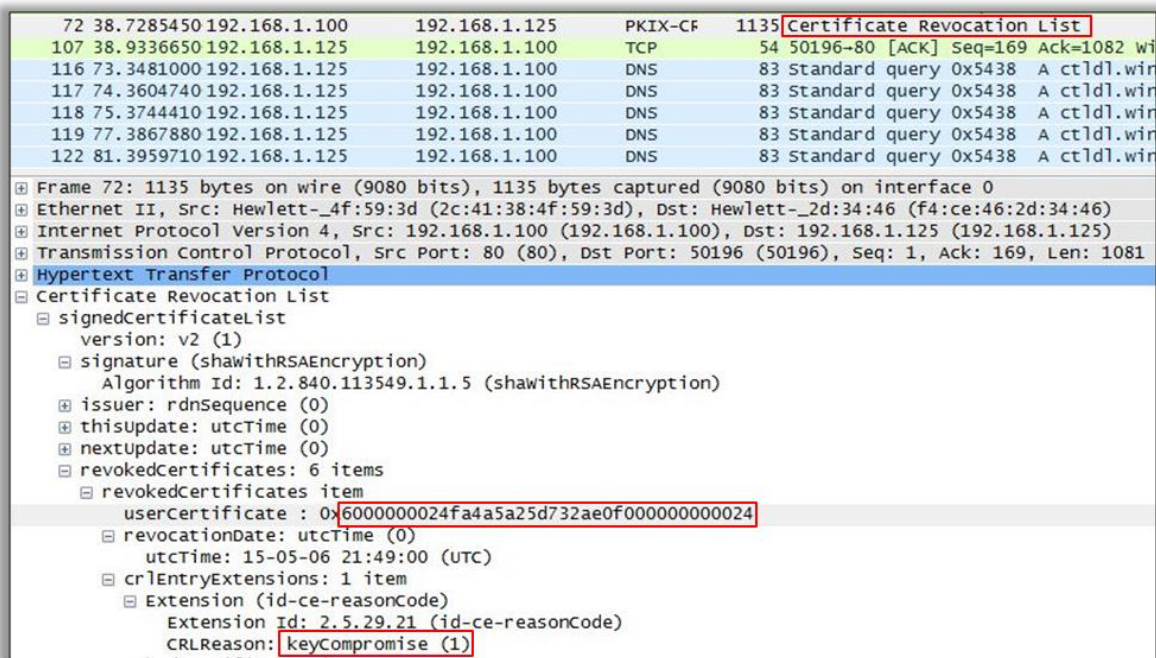
2. When the CA signed certificate was issued to Security Manager, the CDP information is collected from the certificate and a Security Manager attempt is made to access the CRL. The next image is a network capture showing the Security Manager server (192.168.1.125) requesting the CRL from the advertised location (192.168.1.100) via HTTP. After acknowledging the request, the CRL is provided to Security Manager. As long as the CA issued certificate is not in the CRL, the Security Manager "certificate revocation" assessment will pass.

615	119.718007	192.168.1.125	192.168.1.100	HTTP	222	GET /CertEnroll/catest-CATESTSERVER-CA.crl	HTTP/1.1
616	119.775754	192.168.1.100	192.168.1.125	TCP	60	80-50167 [ACK] Seq=1 Ack=169 win=65536 Len=0	
617	119.821487	192.168.1.100	192.168.1.125	PKIX-CF	1323	Certificate Revocation List	

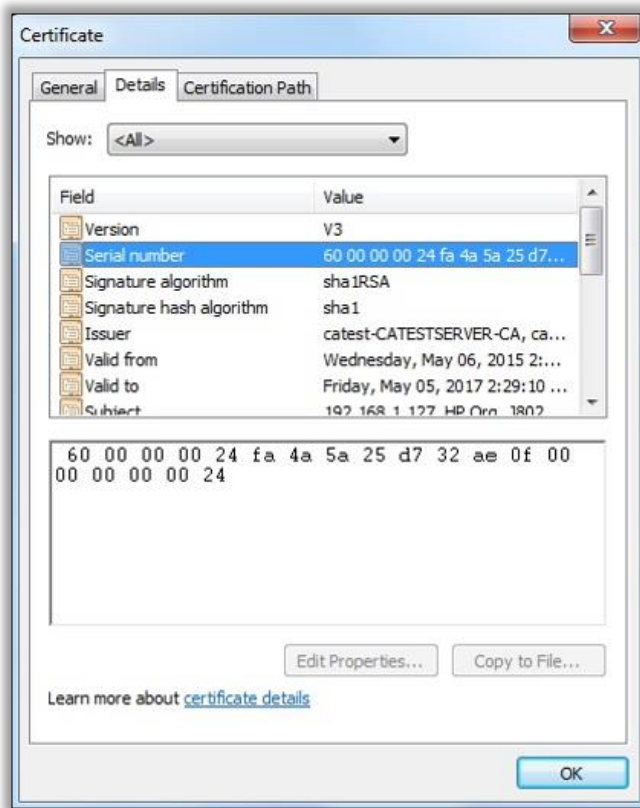
3. The certificate is then revoked. Even though the certificate has been revoked, the information hasn't been updated. The Revocation Status detail in the revoked certificate shows the next update of the CRL.



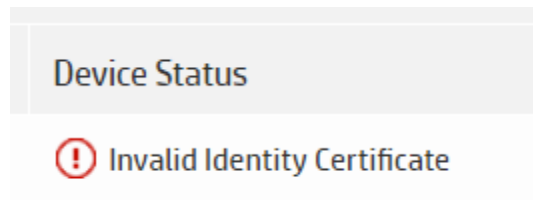
- If an assessment is performed before the next CRL update, Security Manager will not access the CRL to check for certificate revocation. If an assessment occurs after the next update of the CRL, Security Manager does access the CRL to check for revoked certificates. Continuing with this example, Security Manager accessed the CRL and was provided information about the revoked certificate. The next image shows a network capture that includes revoked certificate information. In the capture, you will see the certificate serial number and the reason for revocation. As mentioned earlier, the CRL is a collection of certificate serial numbers.



In the next image, you will see that the certificate serial number provided in the network packet matches the serial number of the installed certificate.

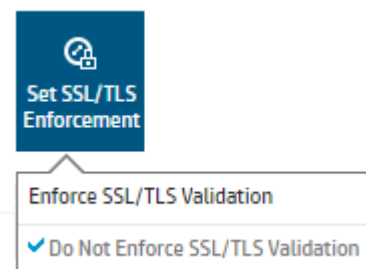


- Security Manager now possesses revocation knowledge of the certificate it installed on the device. If Security Manager attempts to access the device after gaining this knowledge, the connection to the device will be refused the time an assessment of the installed certificate occurs and the status will indicate Invalid Identity certificate.

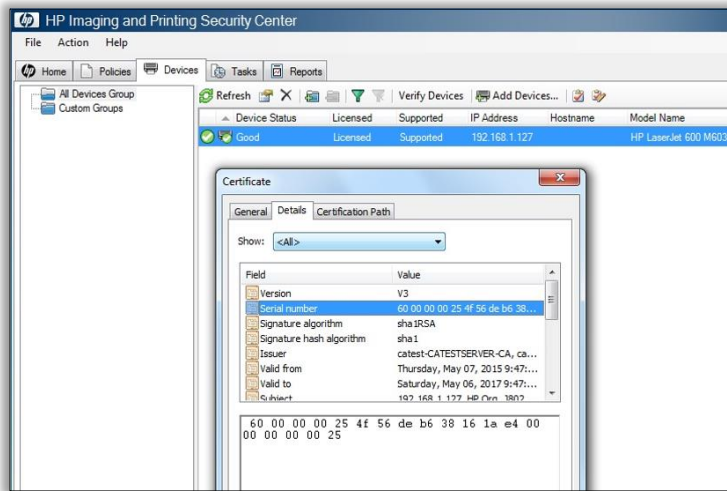


the
next

- The connection is refused because the certificate has been revoked. Security Manager backs off and attempts the remediation again with validating trust. This is essentially automating the task of selecting Do Not Enforce SSL/TLS Validation.



- Because the installed device identity certificate is no longer valid, Security Manager will replace it with a new CA signed certificate. The following image shows completion of this task and evidence of a new certificate based on the new serial number.

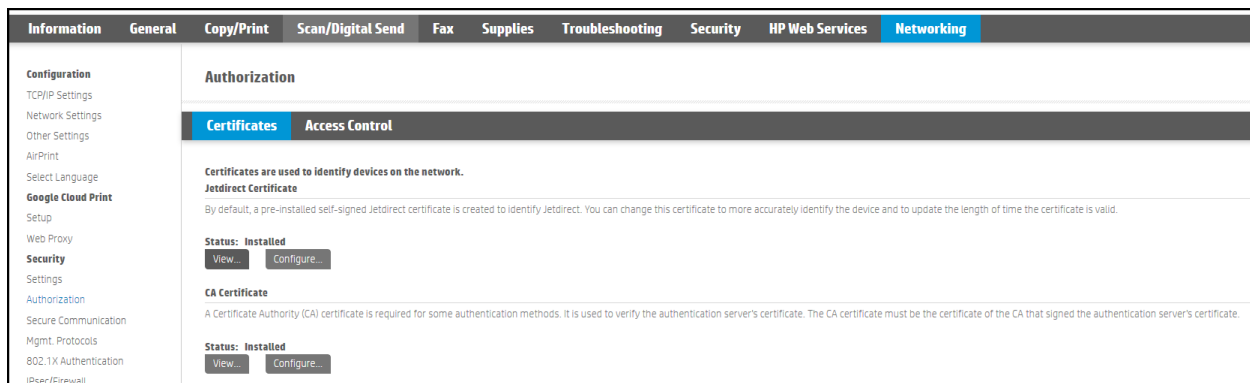


Using Security Manager to Manage CA Certificates

As mentioned previously, a CA certificate tells Jetdirect which identity certificates should be trusted (i.e. must be signed by that CA) when Jetdirect is receiving a certificate from another entity. Once a CA certificate is installed, any identity certificates signed by that certificate authority can be trusted.

Installing CA certificates is a much simpler process than installing identity certificates. A CA certificate is merely exported from the CA server itself, then imported into Security Manager to be installed on the fleet. Since the CA certificate is not unique per device, other tools such as HP Web Jetadmin could also install the CA certificate on the fleet. However, Security Manager expands the functionality by supporting multiple CA certificates per device.

The Jetdirect CA certificate has traditionally been located under the **Networking** tab in the same place as the identity certificate.



Devices also support other types of CA certificates under the **Security** tab. When the device connects securely to a server such as LDAP or SMTP, these CA certificates under the Security tab are used to authenticate the authenticity of the server so that data is not exchanged with an imposter.

Certificate Management

Certificates | Certificate Validation

Install Certificates

Choose File Choose File Certificate Password

Note: Used with a password-protected certificate

Issued To	Issued By	Expiration Date	Certificate Type	Email signing
<input checked="" type="radio"/> SysNameTest.dynamic.zlgo.nl	SysNameTest.dynamic.zlgo.nl	12 Mar, 2025 15:50:06	Identity certificate	<input checked="" type="checkbox"/>
<input type="radio"/> Baltimore CyberTrust Root	Baltimore CyberTrust Root	12 May, 2025 14:55:00	Certificate Authority (CA)	<input type="checkbox"/>
<input type="radio"/> COMODO RSA Certification Authority	COMODO RSA Certification Authority	18 Jan, 2038 14:59:59	Certificate Authority (CA)	<input type="checkbox"/>
<input type="radio"/> DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	9 Nov, 2031 15:00:00	Certificate Authority (CA)	<input type="checkbox"/>
<input type="radio"/> DigiCert Global Root CA	DigiCert Global Root CA	9 Nov, 2031 15:00:00	Certificate Authority (CA)	<input type="checkbox"/>
<input type="radio"/> DigiCert Global Root G2	DigiCert Global Root G2	15 Jan, 2038 03:00:00	Certificate Authority (CA)	<input type="checkbox"/>

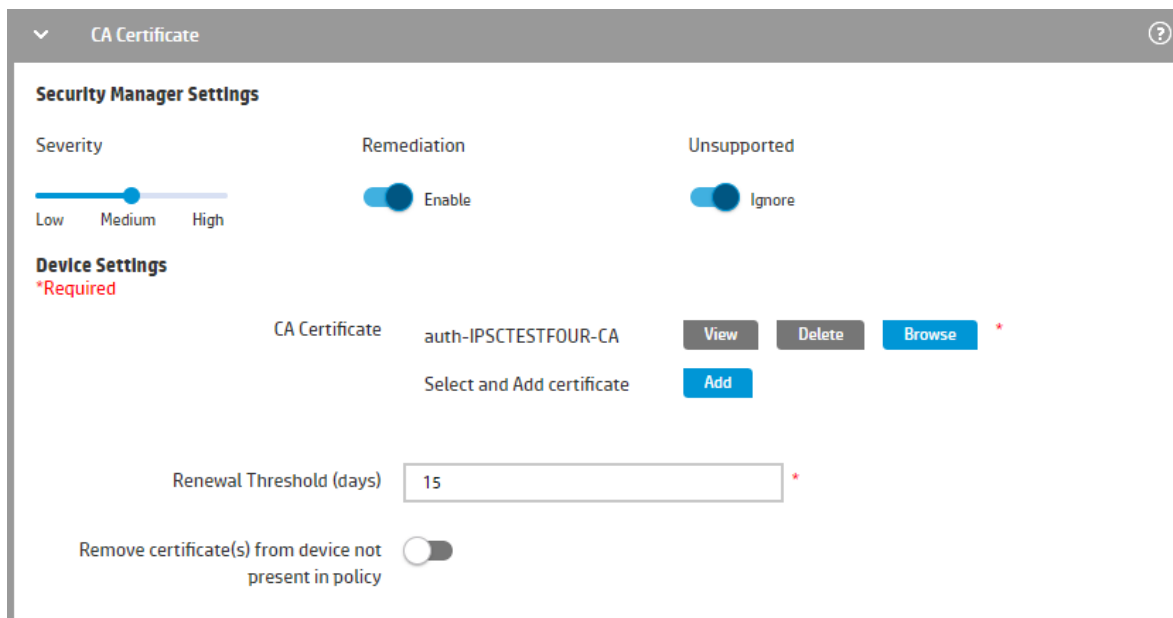
Newer HP devices such as the HP LaserJet M604/605/606, HP Color LaserJet MFP M577, HP Color LaserJet M552, and others began to unify the location of CA certificates previously located in these two separate places under EWS. Both the Jetdirect and device CA certificates have been combined to be located under the **Security** tab.

Authorization

Certificates | Access Control

Networking certificate management is now under the "Security" tab on the "Certificate Management" page.

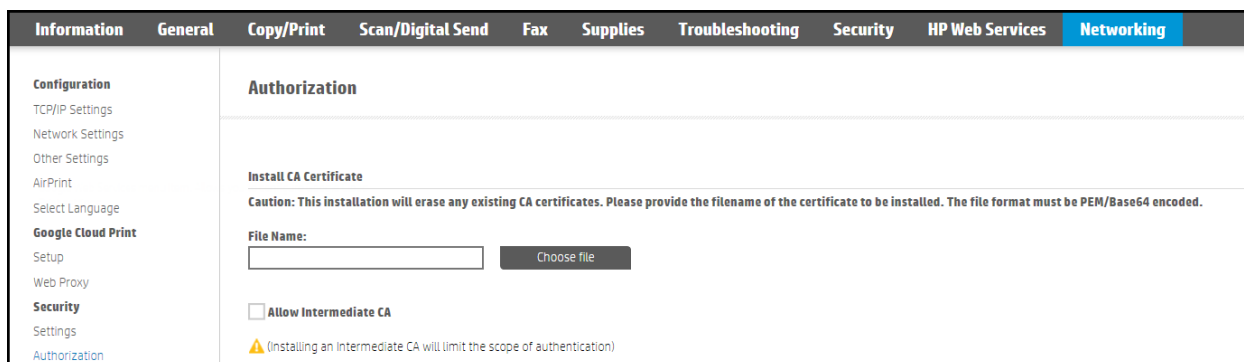
For devices that have unified these certificates into one location, Security Manager supports installing multiple CA certificates. Merely click the + symbol to create a new entry, browse to the location of the certificate and upload it.



NOTE: For devices that do not support this unification of Jetdirect and device CA certificates and still place the Jetdirect CA certificate on the **Networking** tab under EWS, the first certificate in the list in the policy will be installed under the **Networking** tab of the device, and all certificates will be placed under the Security tab.

Security Manager by default will perform an append operation meaning if the certificates in the policy are missing on the device, they will be installed, but existing certificates on the device not in the policy will remain untouched. A replace operation can be performed by checking the box titled **Remove certificates from device not present in policy**. If this box is checked, existing certificates on the device not in the policy will be removed.

For older devices where the certificates are managed under the Networking tab in EWS, a checkbox is present to allow installing intermediate CA certificates.



Security Manager reads the contents of the CA certificate and determines whether it is a root CA certificate or an intermediate CA certificate (compares Issued By and Issued To). Security Manager checks or unchecks the box accordingly depending upon the type of CA certificate when installing on a device.

Troubleshooting Certificate Remediations

All troubleshooting information is now combined in one document: [HP Security Manager - Troubleshooting Issues \(white paper\)](#). The chapter Certificate Installation Failures describes all certificate troubleshooting steps and the beginning of the troubleshooting whitepaper explains how debug logging can be enabled.

Summary

It should be easy to see why there is such a desire for an easier and less time-consuming technique to install Jetdirect (identity) certificates on a fleet of devices rather than using EWS to install certificates one by one. Fortunately, HP Security Manager has added just such a feature to install and manage certificates on a fleet of devices easily and effortlessly.

Appendix A

This Appendix covers information specific to Symantec and OpenTrust Certificate Authorities.

Symantec Certificate Authority

When Symantec is chosen as the Certificate Authority in the identity certificate policy item, some fields are disabled while others are enabled.

The screenshot shows the 'Identity Certificate' configuration window. Under 'Security Manager Settings', there are three sections: 'Severity' with a slider set to 'Medium', 'Remediation' with 'Enable' selected, and 'Unsupported' with 'Ignore' selected. Under 'Device Settings', there are several fields: 'Certificate Signing Request (CSR) Source' set to 'Best Possible', 'Certificate Authority' set to 'Symantec', and several empty fields for 'Organization (O)', 'Organizational Unit (OU)', 'City (L)', 'State (ST)', and 'Country (C)' (set to 'No Value'). There are also fields for 'Symantec Certificate SubjectName' and 'Symantec Certificate Profile OID', both marked as required with a red asterisk. At the bottom, there are 'Include Subject Alternative Name' (set to 'Enable') and 'Domain Name' (disabled) fields.

The **Certificate Profile OID** field is enabled as the certificates will be issued against a certificate profile in the Symantec CA. You can create multiple certificate profiles, and every certificate profile will have a unique OID.

Certificate Profile OID: (required)

The **Certificate Profile OID** field is mandatory. If empty, an error is seen.

Symantec certificate profile will not support Key length values of 1024 and 8192.

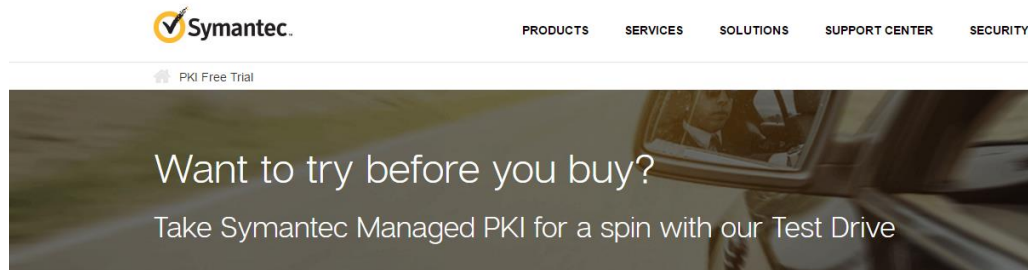
- If the CSR Source is set to Device and the Certificate Authority is set to Symantec, the only available Key Length value is 2048.

- If the CSR Source is set to Security Manager or Best Possible and the Certificate Authority is set to Symantec, available Key Length values are 2048 and 4096.

Setting Up the Symantec PKI Service

Registration

User can click a URL for registration that appears as such:



You can explore the full features of the market leading enterprise PKI. Try it and you will see why we are the most trusted name in security.

Symantec Managed PKI Service offers:

- › Simplified, all inclusive cloud service model including global validation
- › A single account to manage multiple CAs
- › Automated certificate lifecycle management
- › User-friendly certificate enrollment and renewal
- › Pre-provisioned support for multiple applications including VPN, web authentication, WIFI authentication, Adobe CDS, Secure email, and X.509 devices.

There is no obligation - just quick, easy and free access to the Symantec Managed PKI Service online.

Establishing secure connection...

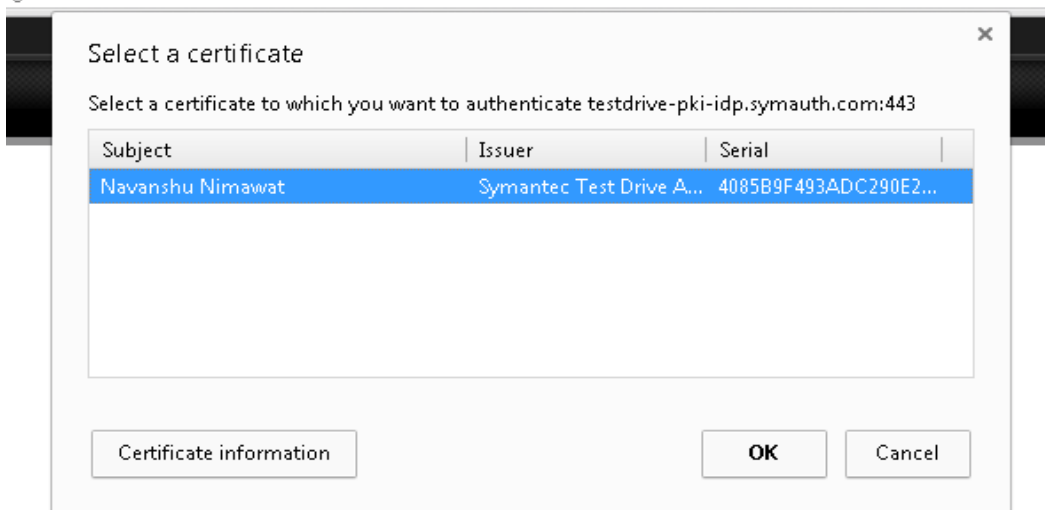
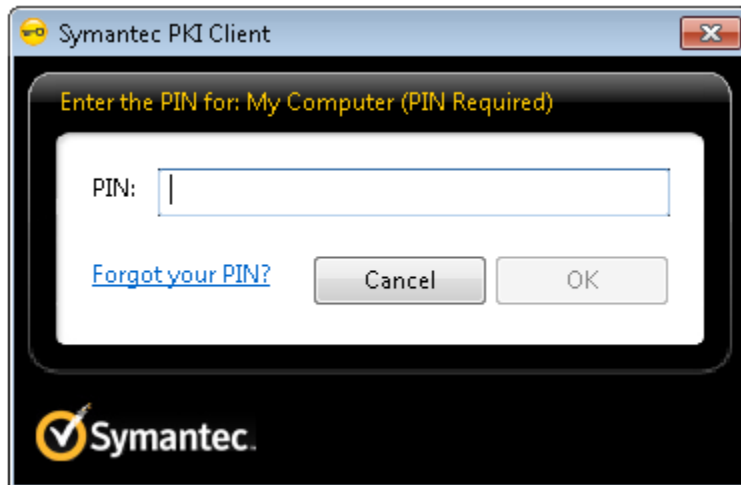
The image shows a registration form titled "Register for Symantec™ Managed PKI Service Test Drive". The form is set against a dark background with a yellow border. At the top left of the form is the Symantec logo and the text "MANAGED PKI SERVICE TEST DRIVE". Below the title, it says "Enter your information to begin the enrollment process." and provides a link to the "Symantec™ Managed PKI Test Drive FAQ". A note indicates that asterisks denote required fields. The form is divided into several sections: "Type of account" with radio buttons for "Standard test drive" (selected) and "Manufacturing test drive"; "Contact information" with input fields for "First name", "Last name", "Email address", and a dropdown for "Title"; and "Organization information" with an input field for "Company/Organization".

Installation

User will be prompted to install a certificate in browser and PKI client application. User is also required to set a PIN. For logging in, certificate in browser and PIN needs to be entered in the PKI client application

Login

Enter PIN in the PKI client application and select certificate.



Symantec Managed PKI Dashboard

After user logs in using PIN and certificate, Symantec dashboard is visible.



Registration Authority Certificate

After user is logged in, a registration authority certificate is required which will be used for authentication when Security Manager is communicating with Symantec web services to enroll for the certificate.

The screenshot shows the Symantec PKI Manager interface with a navigation menu overlay. The menu items are:

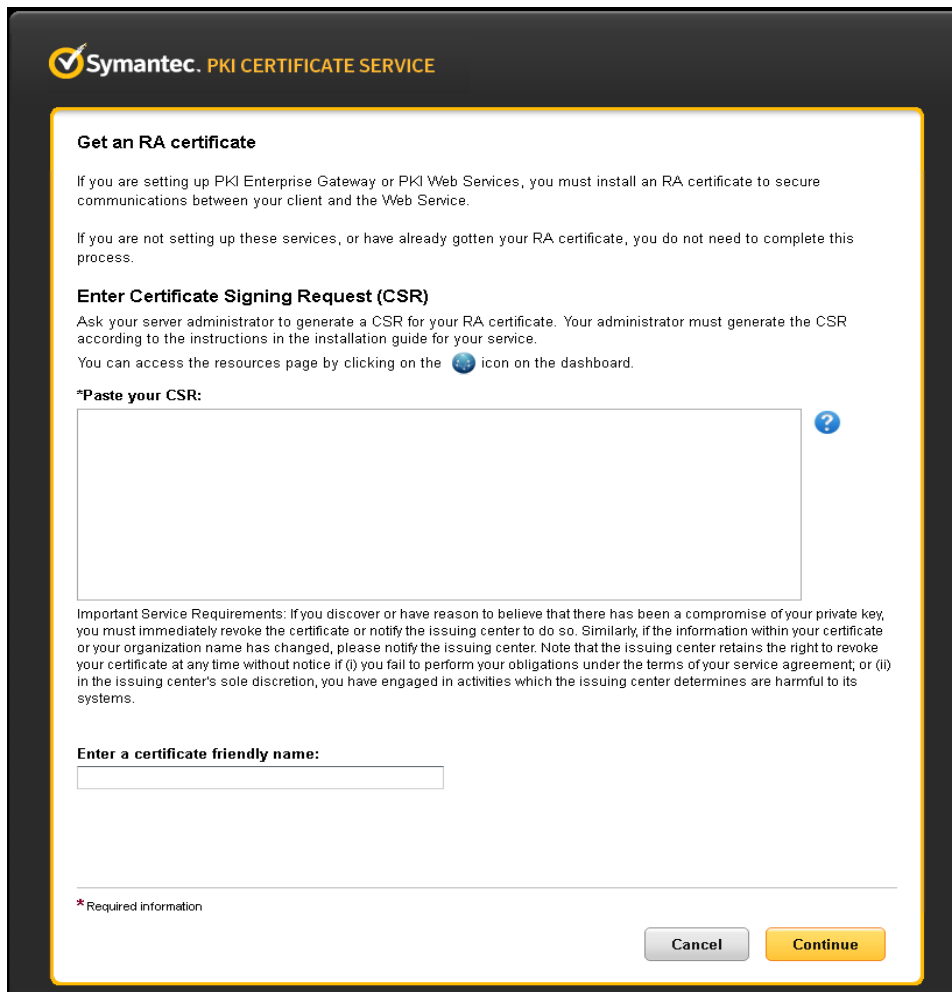
- Users and certificates**
 - Manage users
 - Manage certificates
 - Manage certificate profiles
 - Manage authorized user lists
- Reporting**
 - View recent reports
 - Schedule a report
 - View audit trails
- Your account**
 - Manage account and sub-accounts
 - Manage administrators
 - Manage CAs
 - Manage PKI Enterprise Gateways
 - Get an RA certificate** (highlighted with a red circle)
 - Get a signing authority certificate

The background shows a timeline from 12:00 on 27 Aug to 12:00 on 28 Aug. The bottom toolbar contains icons for a gauge, certificates, users, a gear, and a play button.

CSR for RA Certificate

Symantec recommends JAVA key tool to generate the private key and CSR for the RA certificate. When complete, the user has to paste the CSR to receive the RA certificate.

After user clicks on **Continue**, a download link for certificate is generated.



The screenshot shows a web interface for Symantec's PKI Certificate Service. At the top left is the Symantec logo and the text "Symantec. PKI CERTIFICATE SERVICE". The main heading is "Get an RA certificate". Below this, there are two paragraphs of text explaining the requirements for setting up PKI services. The next section is "Enter Certificate Signing Request (CSR)", which includes instructions for generating a CSR and a link to resources. A large text area is provided for pasting the CSR, with a question mark icon to its right. Below the text area is a section titled "Important Service Requirements" with detailed text. Underneath is a field for "Enter a certificate friendly name:". At the bottom left, there is a note "*Required information". At the bottom right, there are two buttons: "Cancel" and "Continue".

Symantec. PKI CERTIFICATE SERVICE


Get an RA certificate

If you are setting up PKI Enterprise Gateway or PKI Web Services, you must install an RA certificate to secure communications between your client and the Web Service.

If you are not setting up these services, or have already gotten your RA certificate, you do not need to complete this process.

Enter Certificate Signing Request (CSR)

Ask your server administrator to generate a CSR for your RA certificate. Your administrator must generate the CSR according to the instructions in the installation guide for your service.

You can access the resources page by clicking on the  icon on the dashboard.

***Paste your CSR:**

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify the issuing center to do so. Similarly, if the information within your certificate or your organization name has changed, please notify the issuing center. Note that the issuing center retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the terms of your service agreement, or (ii) in the issuing center's sole discretion, you have engaged in activities which the issuing center determines are harmful to its systems.

Enter a certificate friendly name:

*Required information

Windows Certificate Store

Next the user needs to install the Symantec root, intermediate and RA certificate (with private key) in the Windows certificate store of the system where Security Manager is installed.

Now the user can create certificate profiles and install certificates via Security manager on the fleet.

OpenTrust Certificate Authority

The screenshot shows the 'Identity Certificate' configuration window. It is divided into two main sections: 'Security Manager Settings' and 'Device Settings'.
Security Manager Settings:
- **Severity:** A slider is positioned at the 'Low' end, with 'Medium' and 'High' also visible.
- **Remediation:** A toggle switch is turned to 'Enable'.
- **Unsupported:** A toggle switch is turned to 'Ignore'.
Device Settings:
- ***Required:** A red asterisk indicates that the following fields are mandatory.
- **Certificate Signing Request (CSR) Source:** A dropdown menu is set to 'Best Possible'.
- **Certificate Authority:** A dropdown menu is set to 'OpenTrust'.
- **Organization (O):** An empty text input field.
- **Organizational Unit (OU):** An empty text input field.
- **City (L):** An empty text input field.
- **State (ST):** An empty text input field.
- **Country (C):** A dropdown menu is set to 'No Value'.
- **OpenTrust Certificate SubjectName:** An empty text input field with a red asterisk.
- **OpenTrust Profile Name:** An empty text input field with a red asterisk.
- **OpenTrust Endpoint:** An empty text input field with a red asterisk.
- **OpenTrust Contact Email:** An empty text input field with a red asterisk.
- **OpenTrust Zone:** An empty text input field with a red asterisk.

Installing the root and client certificates

To work with OpenTrust PKI, a user must have a valid profile created in OpenTrust PKI. Upon successful profile creation, a user should also have a valid root and client authentication certificate and the password to connect to OpenTrust PKI.

The first step is to add the client authentication certificate into the certificate store of the machine where Security Manager is installed. Add the certificate for the computer account to the Personal certificate store. Import the client certificate and enter the password in the Certificate Import Wizard. Make sure the "Mark this key as exportable" checkbox is checked

After the successful import of certificate right click on the newly imported certificate. Select "All Tasks -> Manage Private Keys". Add the permission as "NETWORK SERVICE" and click OK.

Next, the OpenTrust Root CA certificate needs to be added into the Trusted Root Certificate store. This completes the setup of client authentication certificate into the certificate store for connecting to OpenTrust PKI.

Creating the Security Manager Policy

Select Certificate Authority as “OpenTrust” from the drop down. Provide details for the following OpenTrust specific parameters:

- Certificate Subject Name
- Profile Name
- Endpoint
- Contact Email
- Zone

OpenTrust Certificate SubjectName	<input type="text" value="Subject Name of the Client Certificate"/>	*
OpenTrust Profile Name	<input type="text" value="SimpleAuthenticationDecentralized"/>	*
OpenTrust Endpoint	<input type="text" value="https://pki-demo.idnomic.net/RA/connector.cgi"/>	*
OpenTrust Contact Email	<input type="text" value="admin@hp.com"/>	*
OpenTrust Zone	<input type="text" value="hp"/>	*

Appendix A

HP Security Manager Support information

For more information about HP Security Manager, refer to the guides and whitepapers available at HP.com. To view them, go to the HP JetAdvantage Security Manager Support page and click **Manuals**.

The following list of guides, topics, and whitepapers are examples of support information available:

- Installation and Setup Guide
- User Guide
- Certificate Management (white paper)
- Credential Management (white paper)
- Device Discovery, Determining Device Details, and Exporting Devices
- Instant-On Security and Auto-Group Remediation (white paper)
- Manage devices with FutureSmart 4.5 Firmware
- Release Notes with Ports (white paper)
- Securing the HP Security Manager (white paper)
- Sizing and Performance (white paper)
- Supported Devices (white paper)
- Troubleshooting Issues (white paper)
- Using Microsoft® SQL Server (white paper)
- Using licenses and troubleshooting licensing issues (white paper)
- Policy Editor Settings including supported devices feature table (white paper)
- Automatic Email notification for remediation tasks and policy changes (white paper)
- Reporting, Email Alert Subscriptions, Remediation Summary, Auditing & Syslog Functionality (white paper)

hp.com/go/support

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

© **Copyright 2021 HP Development Company, L.P.** The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

c04677863ENW, Rev.10, August 2021

