whitepaper

How to Utilize the Networking Infrastructure to Protect HP Printing and Imaging Devices

Table of Contents:

Overview

As network printers and Multi-Function Printers (MFPs) grow in capability, they begin to resemble networked PCs in their ability to send and receive data. It would be wise for a company to view these networking devices like publicly available PCs with access to their network for sending and receiving data. Many security conscious customers use Web Jetadmin and the extensive security capabilities of HP's printing and imaging devices to "lock them down" from unauthorized use. While a formidable approach, there is even more that can be done with a little coordination from three common teams found at most customer sites: the Printer Administrators, the IT Information Security Team, and the Network Infrastructure Team. The purpose of this tutorial is to go through a step by step analysis of how to configure the HP printing and imaging devices and the networking infrastructure for additional security protections above and beyond simple device "lock downs".

Threat Analysis

How many businesses would allow a PC to be publicly available in a hallway or an easily accessed cubical where anyone using it was not required to login and had access to their internal network for the sending and receiving of data? Security conscious customers would consider this a mistake, but that is exactly the situation that they find themselves in with networked MFPs. MFPs are often readily available in a customer's environment with scan to email setup.

In many cases, HP networked printers and MFPs (hereafter: HP Printing and Imaging Devices – 'HP PIDs') are plug-n-play. Simply attach them to the network and run the CD that comes with the device and the user is up and running. These users often do not even need to know anything about networking or IP addresses. Such ease of use comes at a cost – by default, HP PIDs trust the network, the users, and the people who claim to be administrators. This default trust can be the cause of accidental configurations that cause down time as well as more malicious attacks.

In general, attacks on HP PIDs are internal threats (e.g., threats coming from other compromised machines, such as a Web Server, or launched by a trusted employee). While many attacks against network printers can be simply running the printer out of paper or changing the display, other networking attacks can be very disruptive (e.g., loss of an IP address) and potentially detrimental to a customer's business (e.g., long down times impacting productivity). However, another type of threat is often even more disruptive but overlooked. For example, a maintenance crew that works overnight in a customer environment may be able to scan confidential documents and send them to a competitor without being traced using the customer's own MFPs!

The good news is that HP has all the tools to make its PIDs some of the most secure devices on your network. In addition, there are opportunities to explore regarding the actual networking infrastructure and how it can be used to enhance the security of these devices. This whitepaper is a tutorial on how to do just that. Although tailored to the large enterprise environments, this whitepaper can also help small to medium businesses use the network to help "lock down" their devices too.

Towards Additional Security

One of the tough parts about use the networking infrastructure to further secure HP PIDs is that often there are three different groups that have to coordinate to do it right. These groups include Networking Infrastructure, IT Information Security, and Printer/MFP (PID) Administration. In many customer environments, these teams often work together for many things, but often do not work together in regards to the printing and imaging infrastructure.

The IT Information Security team will be responsible for issuing HP PIDs Digital Certificates. HP Jetdirect products can support Digital Certificates as credentials to prove their identity. Digital Certificates are a much more effective way to determine identity and in many cases are used in conjunction with passwords. By properly identifying end-nodes, effective management of the network infrastructure parameters associated with those end-nodes can be performed by the infrastructure. The HP ProCurve switch line calls this Identity Driven Management (IDM).

The Networking Infrastructure team will be responsible for putting PIDs on their own Virtual LAN (VLAN). A VLAN is its own broadcast domain and is usually configured with its own IP subnetwork. VLANs help the network support access control. In many cases, VLANs are often group based (e.g., a Lab VLAN, a Marketing VLAN), but HP PIDs are often managed by site or by building or by floor. What we will do is place those HP PIDs on their own Printing and Imaging (PID) VLAN. In addition, we'll create Printing and Imaging Management (PIM) VLANs which will help manage and control these PIDs

Since each VLAN is really an IP subnet, we can now use Access Controls to control traffic to and from VLANs. The HP ProCurve networking line calls this "Control to the Edge". This behavior allows decisions to be made sooner rather than later regarding networking traffic. With IDM, network access controls can be put into place automatically once the device has been identified, making the maintenance of these controls very easy.

How are all these things used in combination? The IT Information Security team does the initial setup of the Public Key Infrastructure to allow Digital Certificates to be issued to HP PIDs. A PID Administrator configures the PID with the Digital Certificate and other important security settings. Using 802.1X technology, this Digital Certificate is presented to the Networking Infrastructure which automatically determines the VLAN and the appropriate access control methods.

Example Deployment

Let's look at a logical VLAN view of an example configuration. Refer to Figure 1 – Logical VLANs

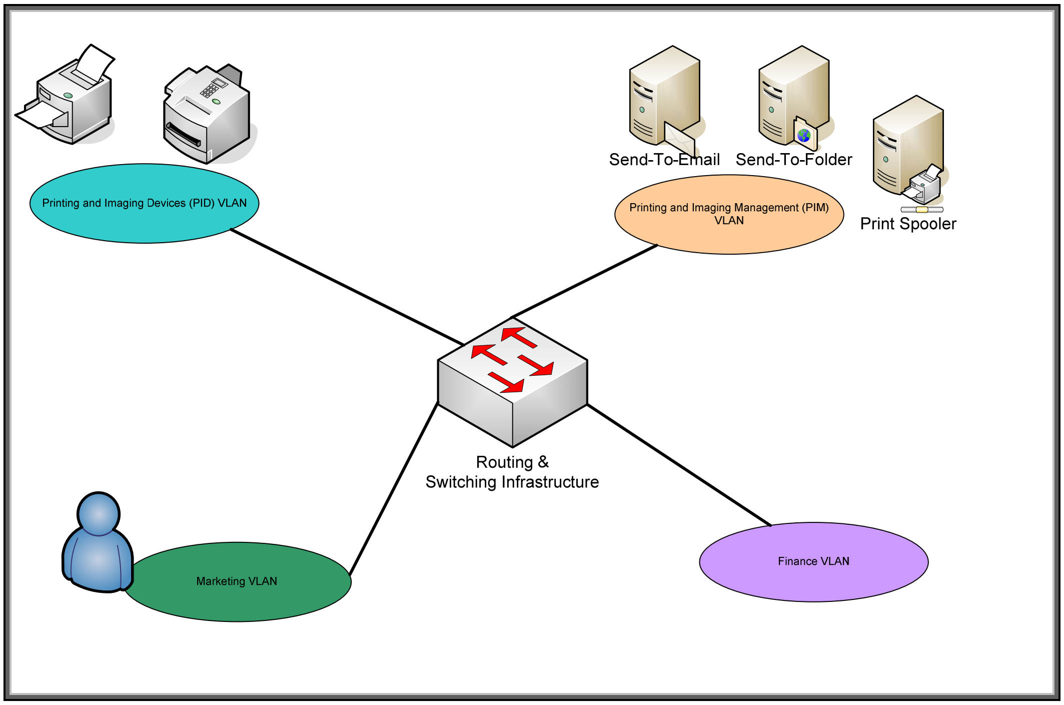


Figure 1 - Logical VLANs

The PID VLAN is for the actual devices. No matter where these devices are placed physically, they will automatically be placed in the VLAN associated with printing and imaging devices. This process is done through IDM. The PID Administration team will have machines set up in the PIM VLAN. These machines will run services that may include some of the following: Web Jetadmin, Scan to Email, Scan to Folder, Digital Sending Software, Syslog, and Windows Print Spooler/Servers. We can see that there will be a lot of communication between the PID VLAN and the PIM VLAN.

Since each VLAN is an IP subnet, routing must be done between VLANs. Because routing is done, we can use network access controls to limit traffic to and from these VLANs. For instance, currently we see no reason for the PID VLAN to communicate to any VLAN except the PIM VLAN. This type of restriction can be associated with the VLAN or with the identity of the device. In our example, the identity of the device is causing a VLAN to be automatically assigned and access controls to be put into place to restrict the traffic flow – the PID VLAN can only communicate with the PIM VLAN. Consequently, the PIM VLAN is the only VLAN that can communicate with the PID VLAN. Therefore, we have used our networking infrastructure to force the Marketing and Finance VLANs to go through the PIM VLAN in order to contact the PID VLAN. In most cases, these users will be connecting to printer shares published in Directory Services. These printer shares will reside on computers physically located in the PIM VLAN.

So far we have been discussing VLANs from a logical perspective. Let's take a look at what happens from a physical deployment. Refer to Figure 2 – Physical VLANs.

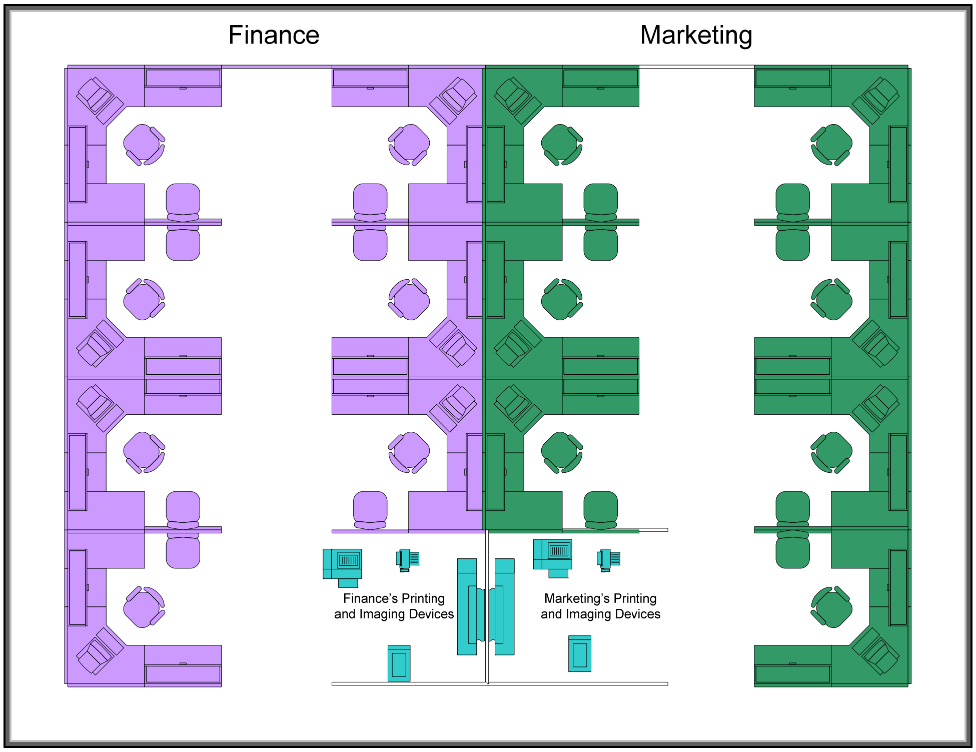

Finance
Marketing
Finance's Printing and Imaging Devices
Marketing's Printing and Imaging Devices

Figure 2 - Physical VLANs

There are three VLANs in Figure 2 – one for printing and imaging, one for Marketing, and one for Finance. The color coding in the diagram is based upon the VLAN. Each user's VLAN is automatically determined by their Identity and is not fixed by their cubical location. For instance, should some employees leave the Finance department and move to other areas of the company and the Marketing department happens to expand, the new layout may be like Figure 3:

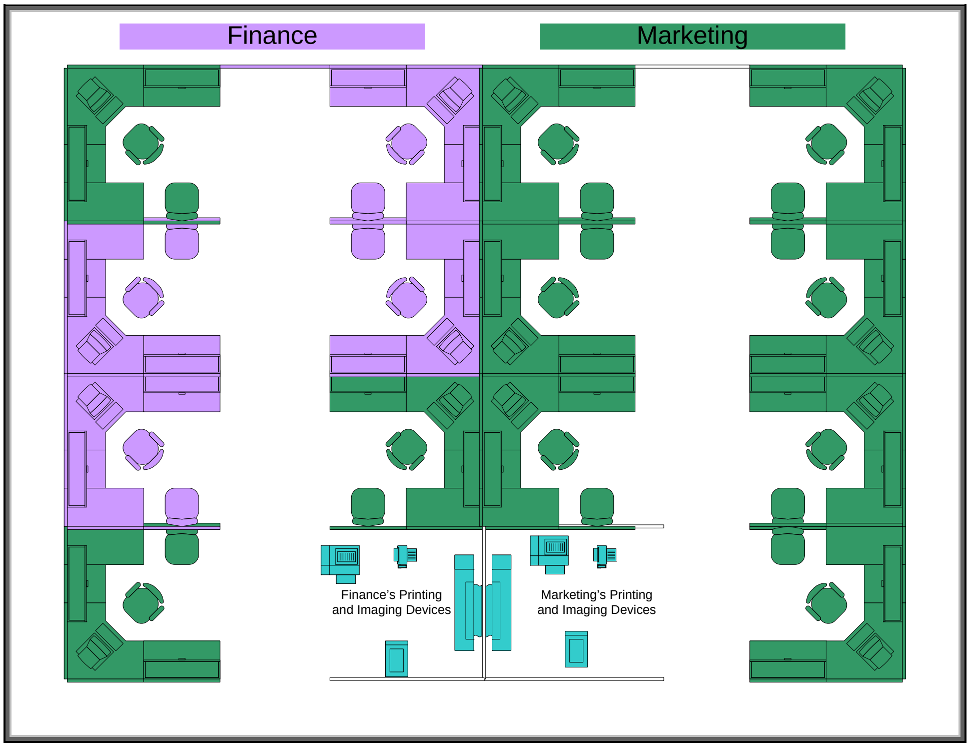


Figure 3 - Dynamic Physical VLANs

In Figure 3, the users are a part of Identity Driven Management – wherever they go in the network, their VLAN configuration follows. This behavior allows tremendous flexibility and minimizes administration headaches for fixed configuration (e.g., Cubical #1 is always a part of the Marketing VLAN and a service request must be issued to change it).

The PID Administration team will then assign printer shares to groups defined in Directory Services. As an example, a PID in Building One by Pole L2 is "owned" by the Marketing department. The PID Administration team has setup printer shares that can only be connected to if the user is part of the appropriate group in Directory Services. In order to use the printer "owned" by Marketing, the user would need to be part of the Marketing Group because of access restrictions on the printer share. Although a user in Marketing that is sitting next to PIDs whose consumables are billed to Finance may not appreciate having to walk a little bit further to get their printouts, the key point is that access to the printer is determined by the Identity of the user and the access restriction of the printer share in the PIM VLAN. The same holds true for PIDs. They can be moved anywhere in the building and they are still a part of the PID VLAN.

With imaging devices, which act as clients that need to talk to servers, the PID VLAN will need to talk to things like DNS servers, Key Distribution Centers (Kerberos), secure LDAP servers, among others. These types of servers we will call Infrastructure Servers and not surprisingly, we'll put them it its own VLAN – the Infrastructure Servers VLAN. The PID VLAN will be able to communicate with the Infrastructure Servers VLAN and the PID VLAN will be able to communicate with the PIM VLAN. Refer to Figure 4 – Infrastructure Servers VLAN.

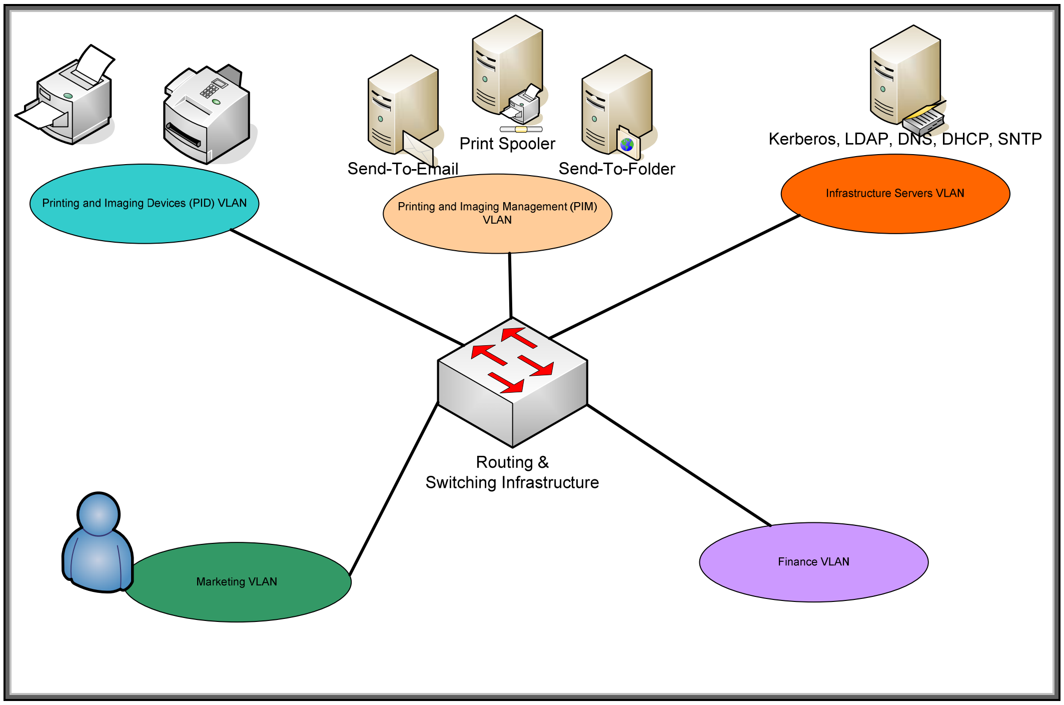

Send-To-Email
Print Spooler
Send-To-Folder
Kerberos, LDAP, DNS, DHCP, SNTP
Printing and Imaging Devices (PID) VLAN
Printing and Imaging Management (PIM) VLAN
Infrastructure Servers VLAN
Routing & Switching Infrastructure
Marketing VLAN
Finance VLAN

Figure 4 - Infrastructure Servers VLAN

You may think there is not much else we can do. However, we can do even more to secure our printing and imaging devices. Assigning PIDs to private VLANs so that the PIDs can only see router ports in the VLAN is a next logical step. This step further isolates traffic to a PID and the Router as opposed to allowing PIDs to communicate with each other, which is often unnecessary. A further step is to restrict communication between the PID VLAN and the PIM VLAN to utilize IPsec. Because there are some chicken-egg scenarios with IPsec and the Infrastructure Servers VLAN, we won't require IPsec there, but we will limit the protocols that can communicate between them to only those necessary.

As we can see, utilizing the powerful capabilities of today's infrastructure devices, especially HP ProCurve switches, we can further protect valuable printing and imaging devices. Let's go into more detail about what needs to be done.

Step 1: Domain Name System and Static IP Addresses

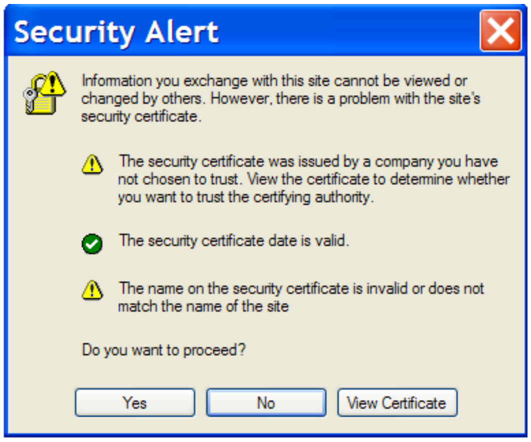
One of the most important things we can do for PIDs is to develop a consistent naming scheme for them and to assign static IP addresses to them. These names can then be entered into the Domain Name System, or DNS. Once a name has been entered into DNS, we can then use that name when we create digital certificates and provide more security.

For our environment, static IP addresses are actually a better solution than DHCP. The reason is that DHCP is rarely deployed with authentication of the DHCP server. Without proper authentication, rogue DHCP servers can often alter the configuration of DHCP clients. In addition, we really want to start treating our PIDs as servers and not as clients. IPv6 has similar security issues with Stateless Automatic Address Configuration. We'll assume that we will manually set an IPv6 address too. Once we have static IP addresses assigned and a name associated with them entered into DNS, we can use this name in the digital certificate. To create digital certificates (also called "security certificate"), we'll need a Public Key Infrastructure (PKI).

Note: For more information about DNS and name resolution, see the whitepaper "Practical IPv6 Deployment for Printing and Imaging Devices".

Step 2: Public Key Infrastructure

Have you ever seen a warning dialog shown in Figure 5 when using https:// (e.g., going to any secure web site, such as a login or shopping cart) in a web browser?



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

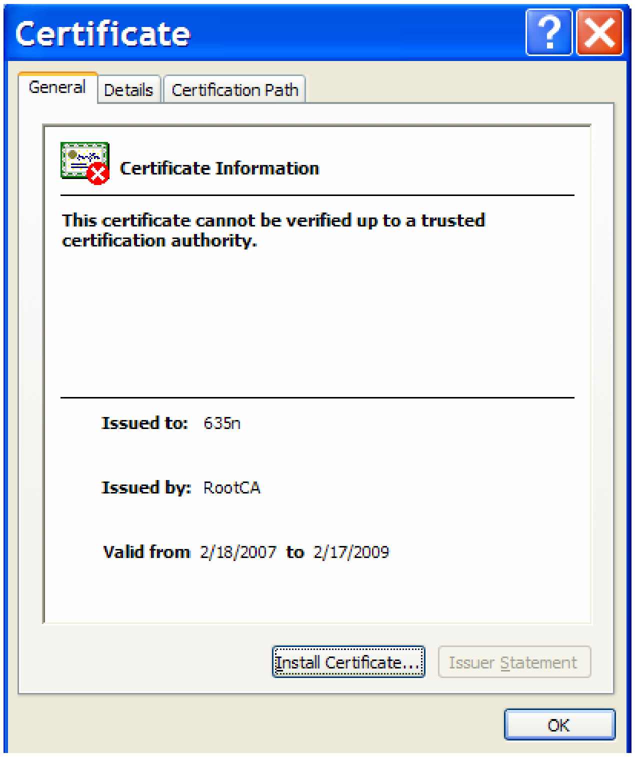
✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Figure 5 – Security Alert

This dialog is entitled "Security Alert" and it talks about something called a "security certificate". What is a security certificate? Well, a security certificate is there to help identify the web site as one that can be trusted. However, the Security Alert 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. There are two warning icons associated with this dialog. The help text by the first warning icon prompts us to view the certificate. Let's click on "View Certificate".



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: 635n

Issued by: RootCA

Valid from 2/18/2007 to 2/17/2009

Figure 6 – Certificate Details

There is a red X on the certificate, indicative of a security problem. In addition, there is a very specific error message: “This certificate cannot be verified up to a trusted certification authority.” Here we see that the “Issued By” is entitled “RootCA”.   What the message is trying to say is that “RootCA”, who issued the certificate “635n”, is not trusted.

A useful analogy is to think of the certificate issuer like the California Department of Motor Vehicles (DMV). Each state in the United States has a DMV run by the state’s government. The DMV issues driver’s licenses which grant the privilege to drive in a given state. A person that goes to the DMV to get a driver’s license must pass a series of tests that helps the DMV determine if they are fit to drive on the state’s roads. The state’s Highway Patrol, a group which enforces the rules of the road, recognizes the validity of the DMV to issue driver’s licenses. Therefore, if one violates one of the rules of the road and is pulled over by a Highway Patrol officer, showing a driver’s license issued by the DMV is a requirement. The Highway Patrol will not recognize a driver’s license issued by an institution other than the DMV as being valid. In short, the DMV is a trusted third party that issues “certificates” (driver’s licenses) to individuals. These “certificates”, issued by the DMV, are trusted by the Highway Patrol.

The Security Alert dialog is troubling because it is indicative of a trust problem. In the terms of our analogy, it would be like a driver, who has been pulled over by the Highway Patrol, handing the officer a driver’s license that the driver’s mother wrote for him indicating that her son had been granted the privilege to drive in the state. While a note from mom may be trusted by her sister, it isn’t trusted by the Highway Patrol.

In essence, a digital certificate, one used by computers, binds an identity to a key and needs to be issued by a trusted third party. What is a key? A key is a secret that is used in cryptographic algorithms. There are public keys and private keys used for asymmetric cryptography and symmetric keys used for symmetric cryptography. Let’s look at symmetric cryptography first.

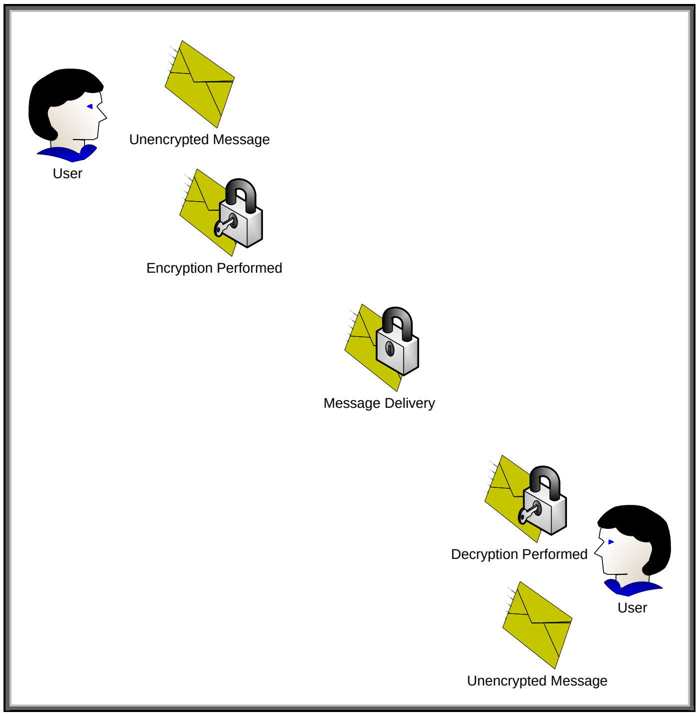


Figure 7 – Symmetric Cryptography

In Figure 7, the confidentiality provided to the message is done via a single key. Because the same key is used for encryption and decryption, this process is known as symmetric cryptography. Symmetric cryptography commonly has two attributes associated with it:

- It performs well – it is fast and easy to implement
- It has a key distribution problem – how do you get the symmetric key to everyone that needs it in a secure way?

Asymmetric cryptography is also available and functions very different than symmetric cryptography. It has two keys – one Public and one Private. The private key is not shared with anyone. The Public key is like a public telephone number. You can share it with everyone.

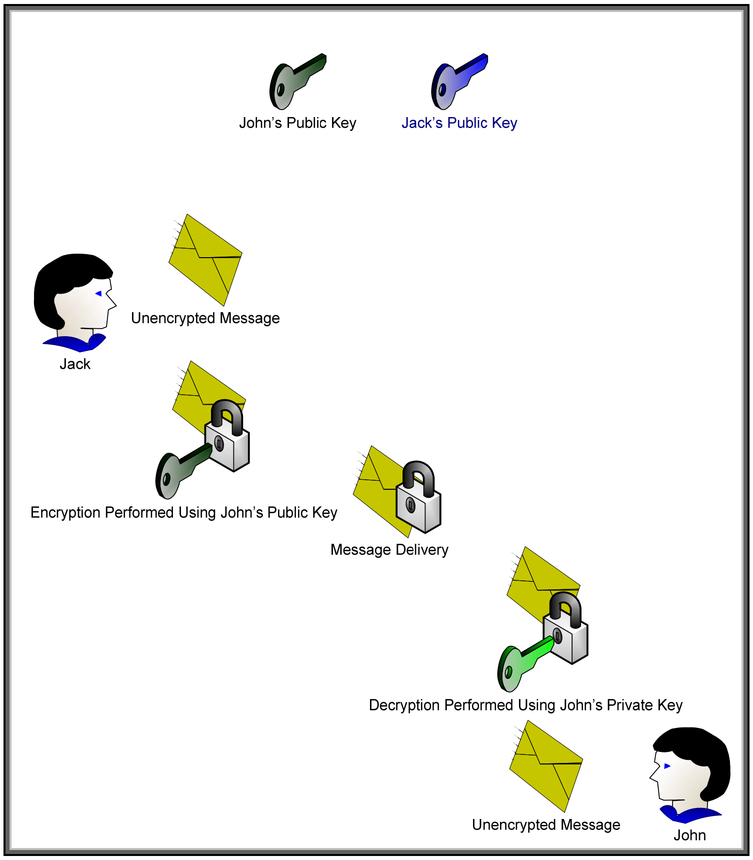


Figure 8 – Asymmetric Cryptography

In Figure 8, we can see the difference between asymmetric and symmetric cryptography. One key can be used for encryption and then the corresponding key can be used for decryption. It appears that asymmetric cryptography has solved the key distribution issue; however there are two new attributes usually associated with asymmetric cryptography

- It is slow
- It has a trust problem. How do I know that this is John's public key and not someone pretending to be John?

To solve the first problem, asymmetric cryptography is usually used to securely distribute symmetric keys and sign hash codes. In short, what is actually being encrypted and decrypted is usually much smaller than actual messages. This has the nice benefit of solving the key distribution issue with symmetrical cryptography. So, in essence, symmetric keys are sent securely using asymmetric cryptography and the actual messages themselves are protected using symmetric cryptography. Cool! We get the flexibility of asymmetric cryptography and the speed of symmetric cryptography. Now we only have to solve the trust problem.

In order to solve the trust problem, five things will need to be discussed:

- A certificate authority – a trusted third party that creates digital certificates from certificate requests
- A certificate request – a public key associated with identity information that will serve as that basic building block for a digital certificate that the certificate authority will create and sign.
- A digital certificate – a public key associated with identity information that is digitally signed by the certificate authority.
- A digital signature – the hash of the digital certificate encrypted by the private key of the certificate authority.
- A hash – also known as a message digest. A hash is the output of a one way function that attempts to ensure the integrity of the message (i.e., that the message has not been altered). It is usually combined with authentication information to ensure that the message originator can be authenticated and that the integrity of the message has not been disrupted. You can think of a hash like an advanced checksum or an advanced cyclic redundancy check (CRC).

Let's cover hashes and digital signatures first. We'll assume that Jack wants to send John a message. Jack wants to make sure that John knows the message came from him and that the message was not altered in transit. However, Jack doesn't care about confidentiality – in other words, the actual message can be sent "in the clear" – but does care about authentication and integrity. We can accomplish this through hashes and digital signatures.

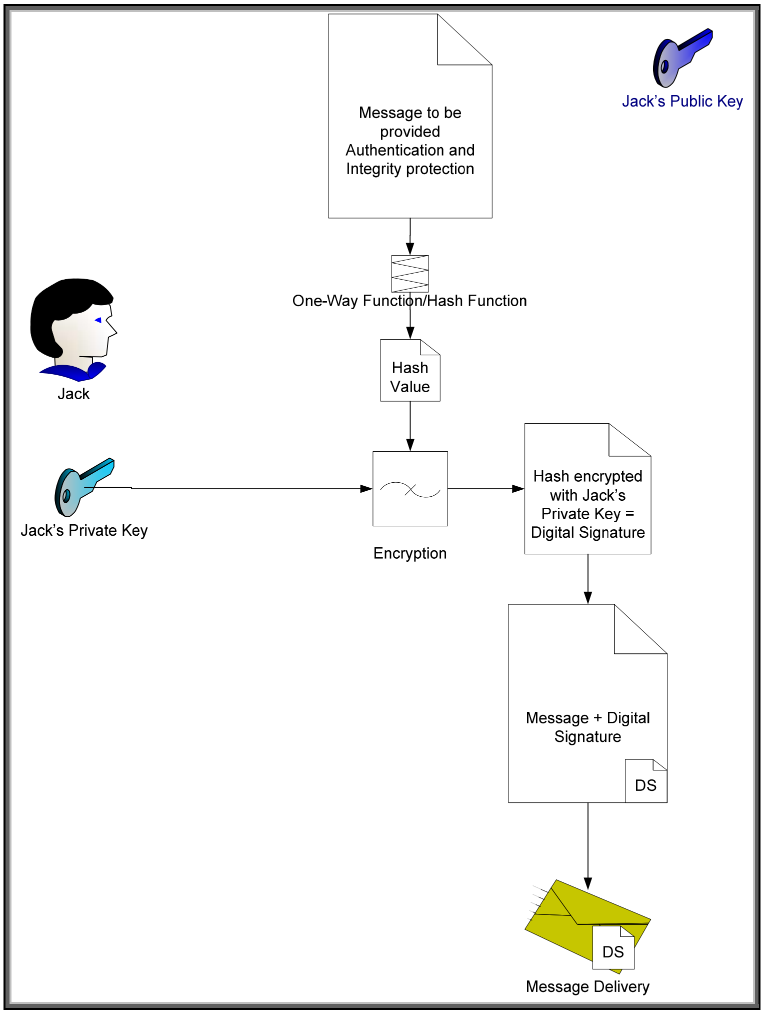

Message to be provided Authentication and Integrity protection
Jack's Public Key
One-Way Function/Hash Function
Jack
Hash Value
Jack's Private Key
Encryption
Hash encrypted with Jack's Private Key = Digital Signature
Message + Digital Signature
DS
DS
Message Delivery

Figure 9 – Digital Signature

In Figure 9, Jack has sent John a message with a digital signature. Let's see how John would validate this message to make sure it came from Jack and was not altered. Refer to Figure 10.

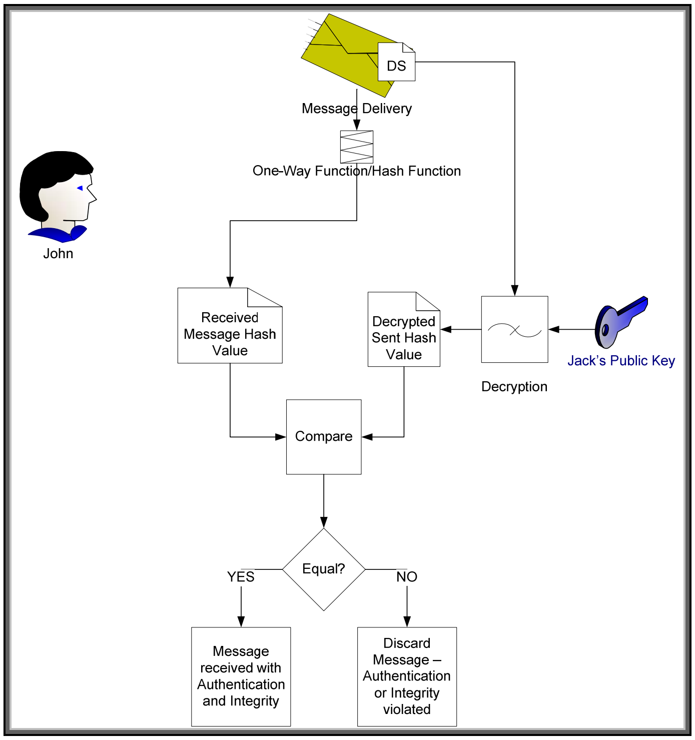

DS
Message Delivery
One-Way Function/Hash Function
John
Received Message Hash Value
Decrypted Sent Hash Value
Jack's Public Key
Decryption
Compare
Equal?
YES
NO
Message received with Authentication and Integrity
Discard Message – Authentication or Integrity violated

Figure 10 – Digital Signature Verification

Here we see how John uses Jack's public key to verify the message. Jack's public key is the only key that can decrypt the digital signature and obtain the hash value of the message that Jack calculated before sending the message. Because the hash was encrypted with Jack's private key, which no one should know but Jack, John can be sure that Jack was the one that sent it.

We still have a problem – How does John know that Jack's public key really belongs to the person that he knows as "Jack"? There are many people in the world named "Jack" – how does John know it isn't one of them? We still need a trusted third party to provide Jack's public key in a format John can trust and we probably need Jack to provide a little more identity information too. Here is where the Certificate Authority comes into play. Refer to Figure 11 – Certificate Authority.

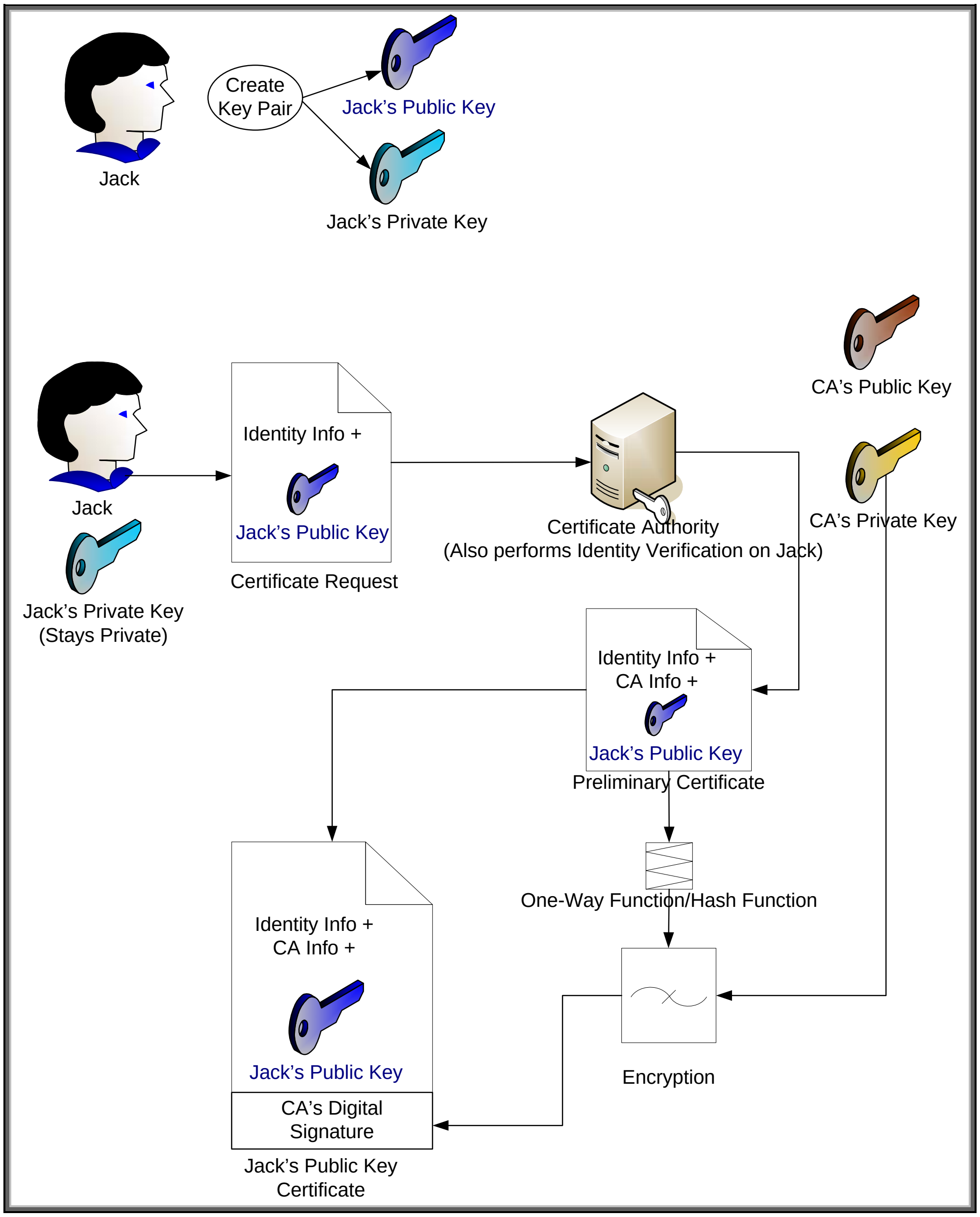


Figure 11 – Certificate Authority

Jack goes through a key pair generation process and creates a public and private key pair. The private key is kept secret. The public key is associated with some identity information and is given to a Certificate Authority. The certificate authority generates a certificate, usually specific to a purpose such as email, and signs the certificate with its digital signature. Assuming there is a place where these digital certificates are publicly available, as long as Jack and John can agree to trust a specific certificate authority, they'll be fine trusting certificates signed by that authority. Refer to Figure 12.

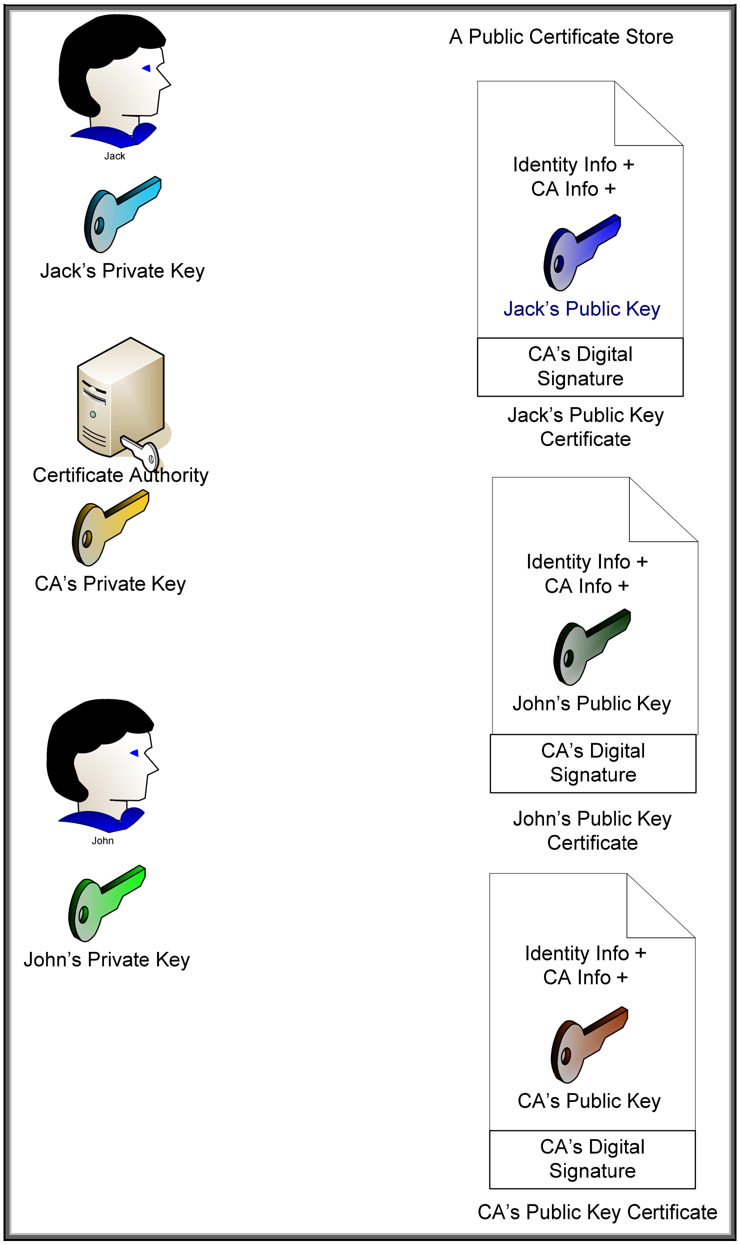


Figure 12 – Public Key Certificates

Here we can see that everyone's public key certificate is, well – um, public. The important thing to note is that the certificate authority also has a public key certificate that identifies itself. This certificate is signed with its own private key and is a "self-signed" certificate. There is no "higher" level of trust than the top level certificate authority. Therefore, John and Jack must choose a particular certificate authority that they both trust. In most cases, there is a hierarchy of certificate authorities at customer sites. This forms what is known as a certificate chain and there is a top level CA or Root CA where the ultimate trust resides.

Also, we should take care to point out that there is usually a difference between Internet trust using certificates and Intranet trust using certificates. Internet trust will involve well-known certificate authorities like Verisign and Entrust. However, Intranet models usually revolve around Microsoft's certificate authority that comes with Windows 2003 server. Each company establishes their own Public Key Infrastructure (PKI) that includes an entire policy around certificates.

Now that we have covered some basics around certificates, we can talk specifically about Jetdirect. Jetdirect is an embedded system and as a result, has limited storage space for certificates. Jetdirect can store one Identity certificate and one CA 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.

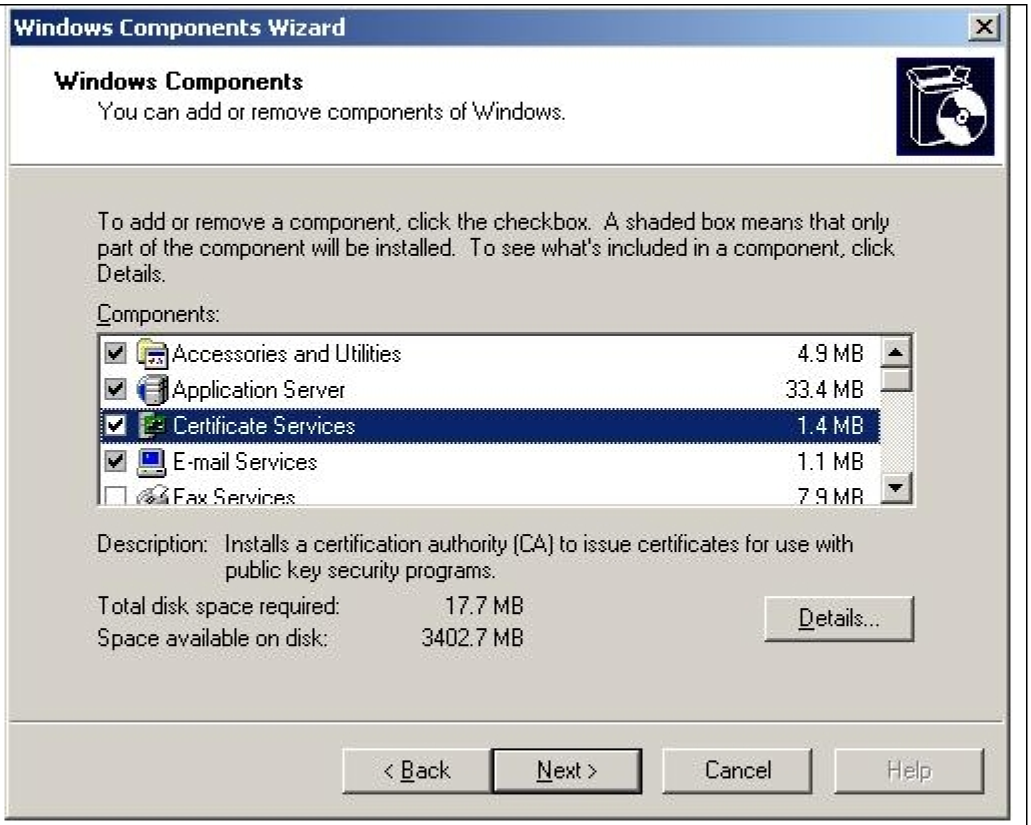
Since Jetdirect only has one Identity certificate that can be configured, it must be capable of being used in a variety of situations. Jetdirect can act as a client or a server, depending on the protocol being used. For instance, if a web browser is using HTTPS to communicate to Jetdirect, Jetdirect will return its Identity certificate as part of the SSL/TLS negotiation process, which will identify Jetdirect as a server. In other cases, like EAP-TLS, Jetdirect will send its Identity certificate for client authentication.

By default, Jetdirect will create a “self-signed” certificate the first time it is powered on. This certificate is not secure because it has not been signed by a trusted 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.

PKI: Installing a Certificate Authority (CA)

NOTE: The following details around installing PKI servers are shown for example purposes and to be utilized in a test network. For production deployments, much more stringent care and consideration must be used and is usually the responsibility of a separate security team.

Using Windows 2003, we can simply go to the Control Panel and select “Add/Remove Programs” and then select Windows Components.

Select “Certificate Services”, then click Next.	

Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Accessories and Utilities	4.9 MB
☑	Application Server	33.4 MB
☑	Certificate Services	1.4 MB
☑	E-mail Services	1.1 MB
□	Fax Services	7.9 MB

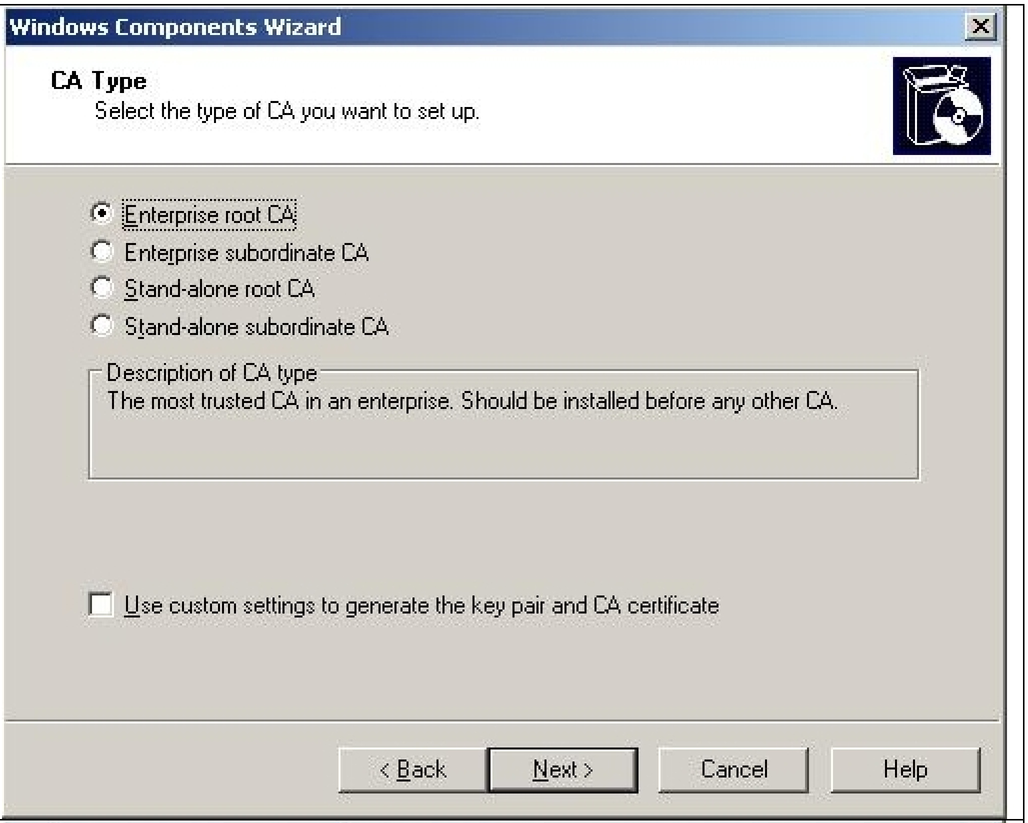
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 17.7 MB

Space available on disk: 3402.7 MB

In this example, we are installing an Enterprise Root CA. Click Next.

NOTE:
If you select a standalone CA, the certificate template functionality described below will not be available.



CA Type

Select the type of CA you want to set up.

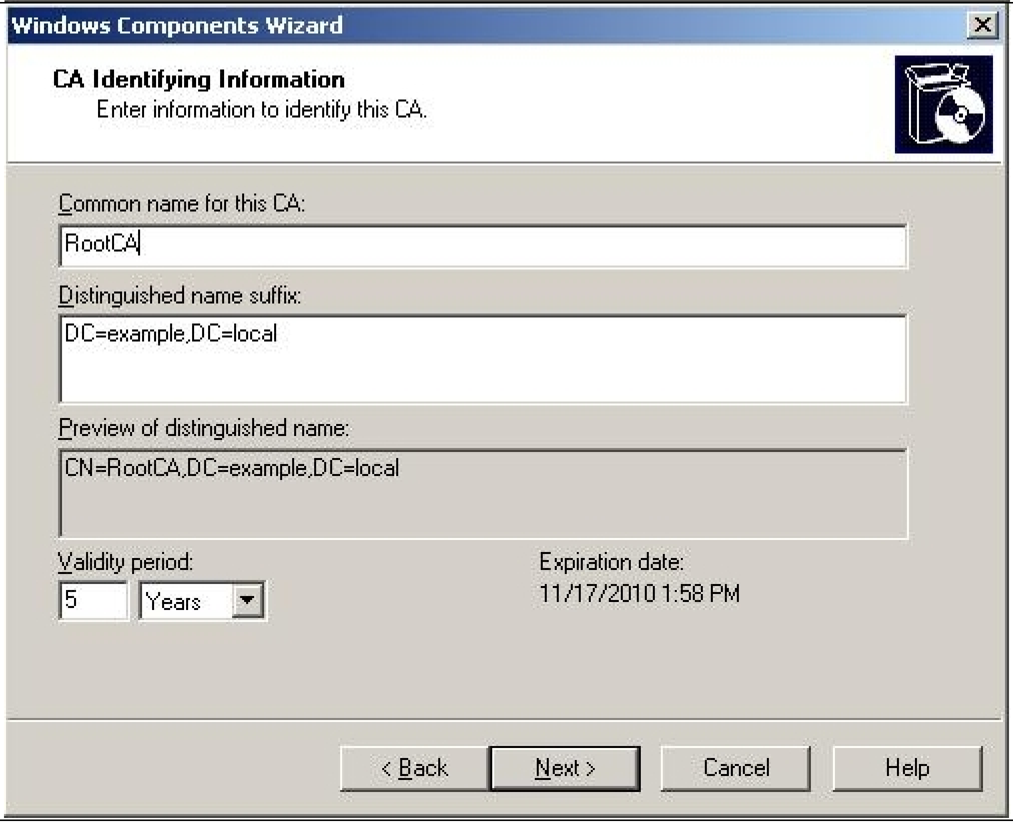
● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

☐ Use custom settings to generate the key pair and CA certificate

Here is our CA identity information. Click Next and complete the installation.



CA Identifying Information

Enter information to identify this CA.

Common name for this CA: RootCA

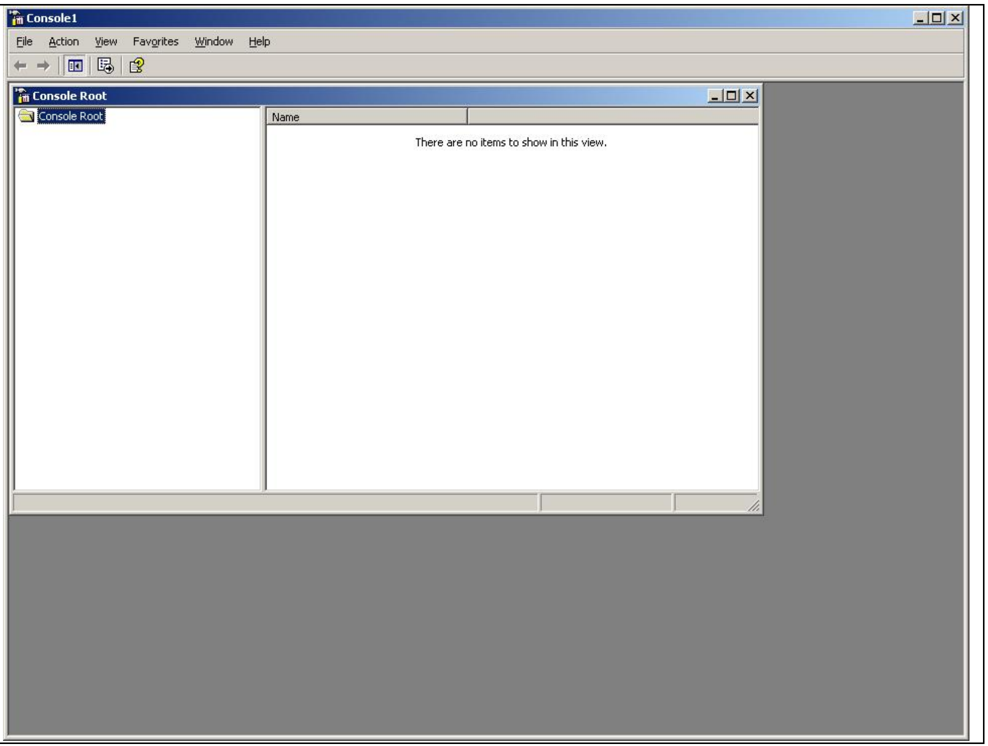
Distinguished name suffix: DC=example,DC=local

Preview of distinguished name: CN=RootCA,DC=example,DC=local

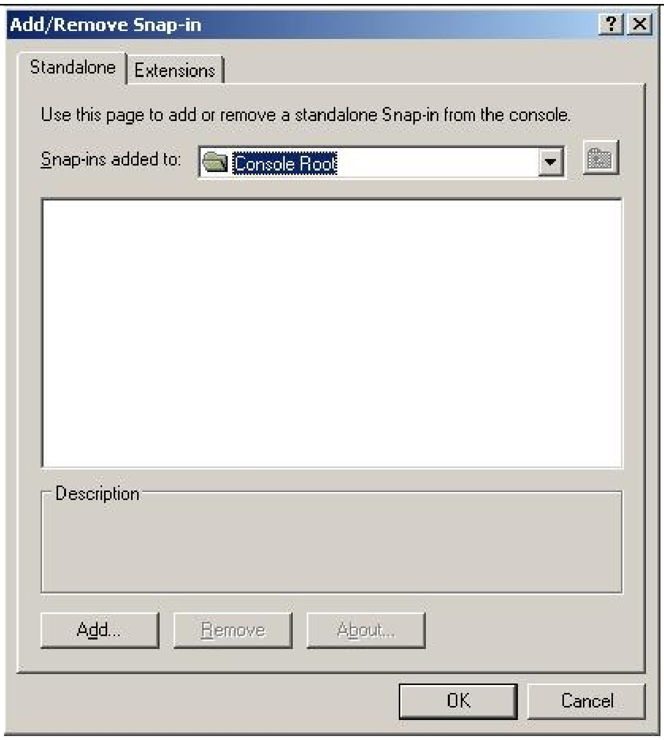
Validity period: 5 Years

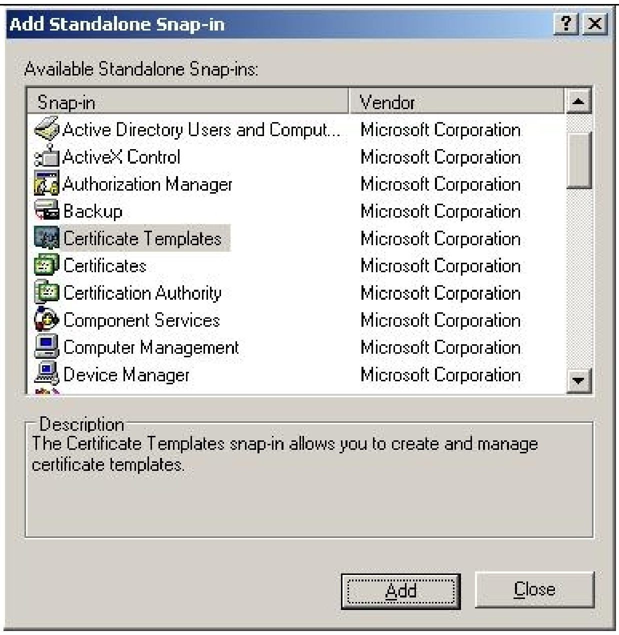
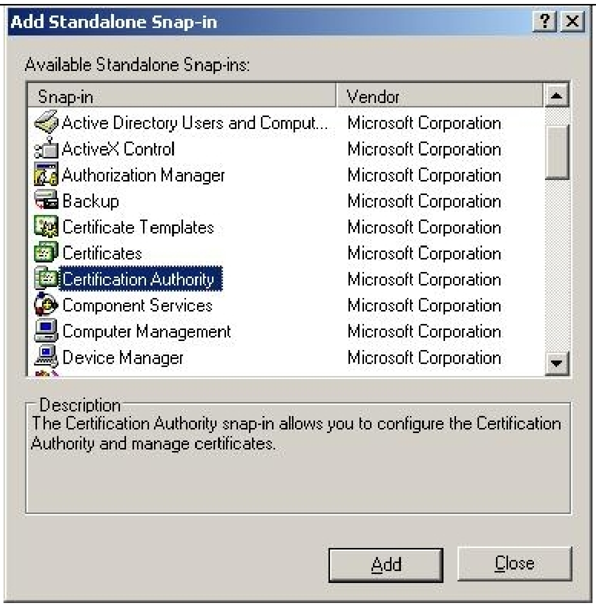
Expiration date: 11/17/2010 1:58 PM

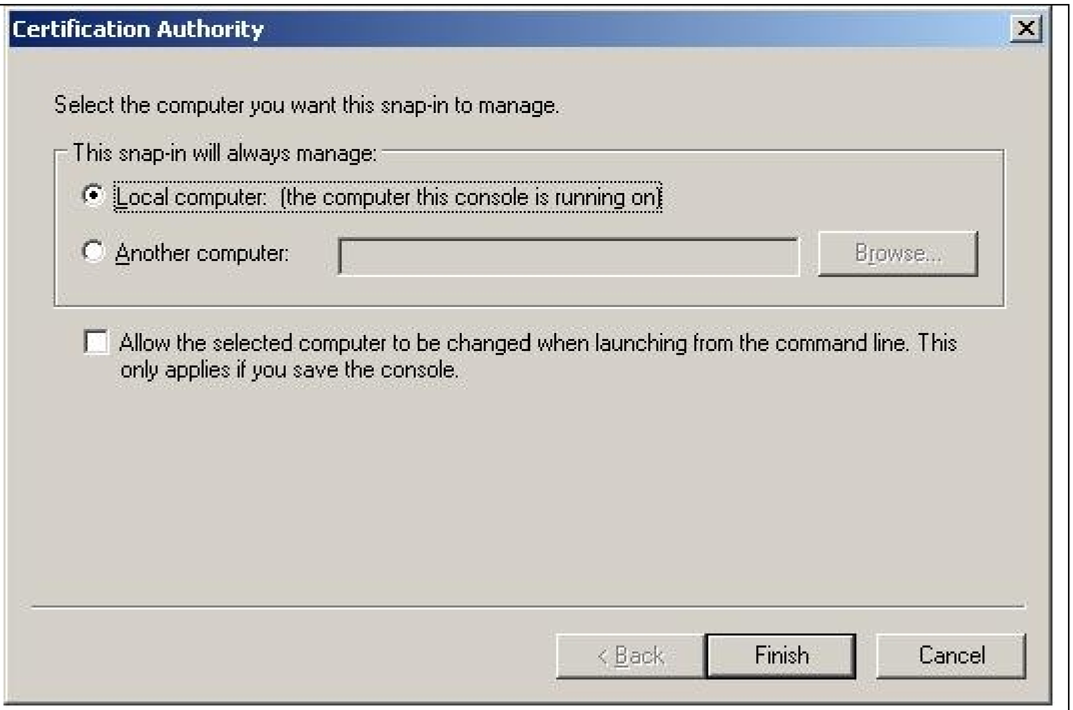
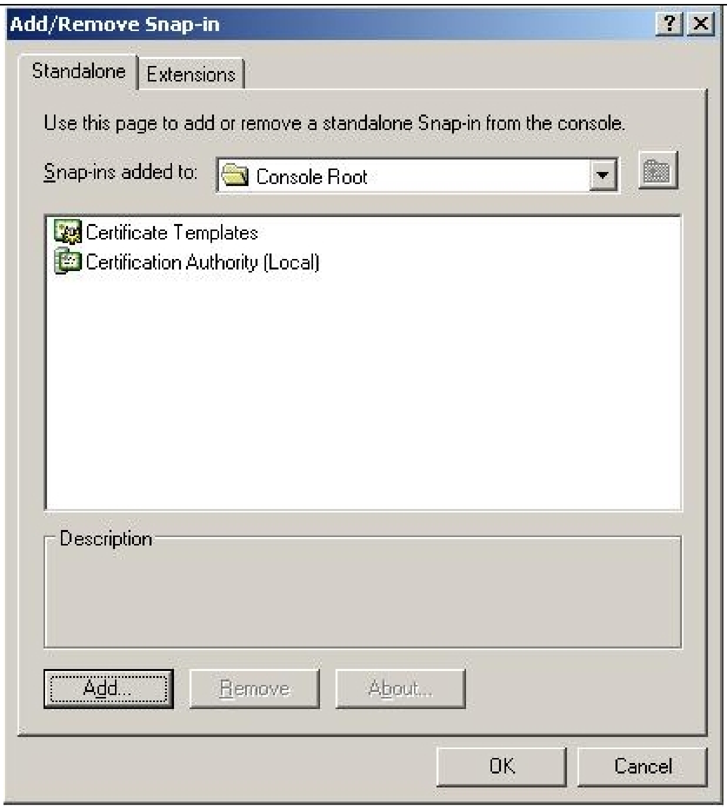
Once the installation has completed, we can go to Start -> Run -> mmc

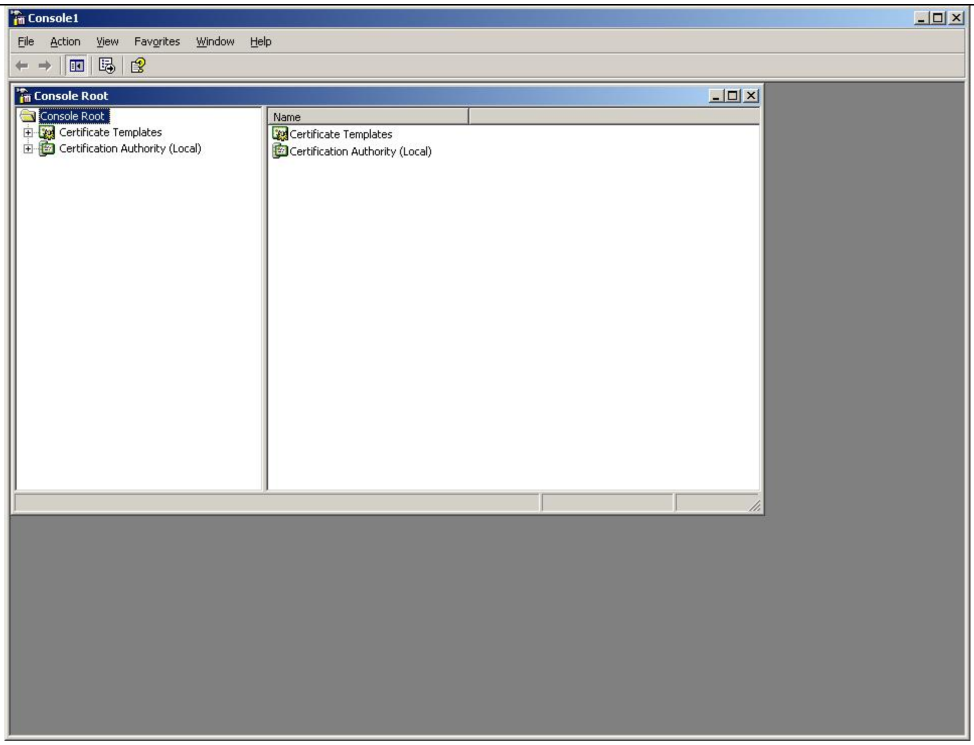
The Microsoft Management Console is a framework that allows various "Snap-Ins" to be loaded. Each "Snap-In" manages a specific service. For example, there is a "Snap-In" to manage the Certificate Authority (or Certification Authority as Microsoft sometimes calls it).	 Console1 File Action View Favorites Window Help Console Root Console Root Name There are no items to show in this view.

At this point, we want to load in separate Snap-Ins into the Microsoft Management Console (MMC). Snap-Ins are modules that provide specific management functionality to the MMC. Go to the File menu and select "Add/Remove Snap-In".

Click Add.	 Add/Remove Snap-in Standalone Extensions Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Description Add... Remove About... OK Cancel
Select Certificate Templates, then press "Add".	

	 Add Standalone Snap-in Available Standalone Snap-ins: Snap-in: Vendor Active Directory Users and Comput...: Microsoft Corporation ActiveX Control: Microsoft Corporation Authorization Manager: Microsoft Corporation Backup: Microsoft Corporation Certificate Templates: Microsoft Corporation Certificates: Microsoft Corporation Certification Authority: Microsoft Corporation Component Services: Microsoft Corporation Computer Management: Microsoft Corporation Device Manager: Microsoft Corporation Description The Certificate Templates snap-in allows you to create and manage certificate templates. Add Close
Select Certification Authority, then press "Add". Then press Close.	 Add Standalone Snap-in Available Standalone Snap-ins: Snap-in: Vendor Active Directory Users and Comput...: Microsoft Corporation ActiveX Control: Microsoft Corporation Authorization Manager: Microsoft Corporation Backup: Microsoft Corporation Certificate Templates: Microsoft Corporation Certificates: Microsoft Corporation Certification Authority: Microsoft Corporation Component Services: Microsoft Corporation Computer Management: Microsoft Corporation Device Manager: Microsoft Corporation Description The Certification Authority snap-in allows you to configure the Certification Authority and manage certificates. Add Close

Select “Local Computer”. Then click Finish.	 Certification Authority Select the computer you want this snap-in to manage. This snap-in will always manage: ● Local computer: (the computer this console is running on) ○ Another computer: Browse... □ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. < Back Finish Cancel
Select OK.	 Add/Remove Snap-in Standalone Extensions Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Certificate Templates Certification Authority (Local) Description Add... Remove About... OK Cancel

Done.	

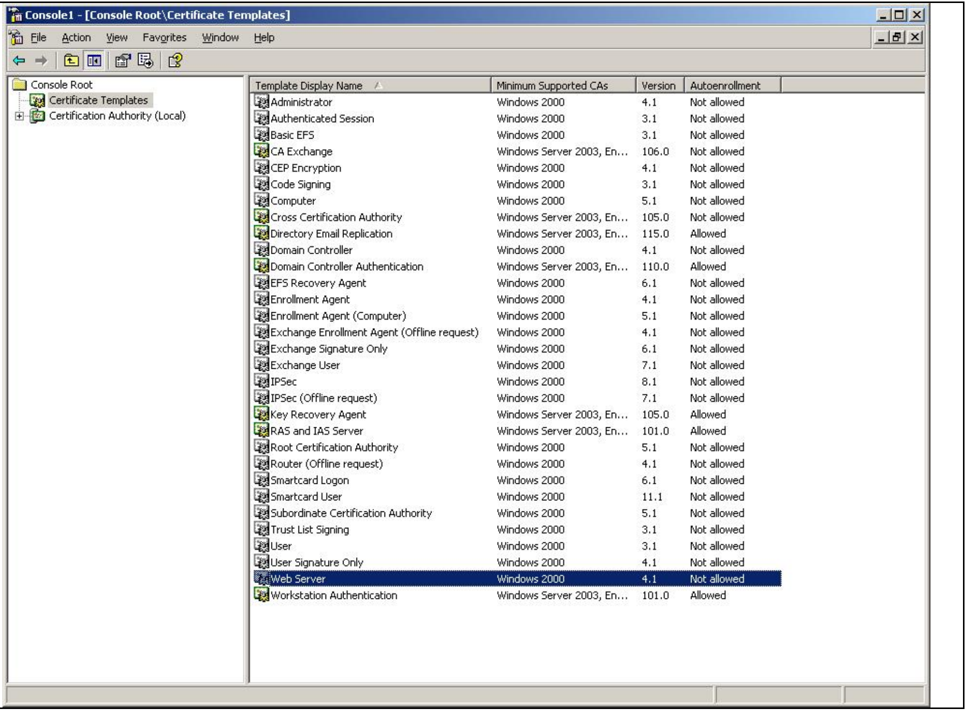
Console1
File Action View Favorites Window Help
Console Root
Console Root
Certificate Templates
Certification Authority (Local)
Name
Certificate Templates
Certification Authority (Local)

PKI: Creating a Certificate Template

The Certificate Authority needs to have a template from which certificates can be created for services. The Microsoft CA has some predefined templates to help the administrator. Microsoft also allows you to create new templates. We will illustrate a process of creating a certificate template specifically for an HP Jetdirect print server.
Note: The certificate template functionality described below is only available for Windows 2003 Enterprise Edition and Windows 2003 Datacenter Edition.

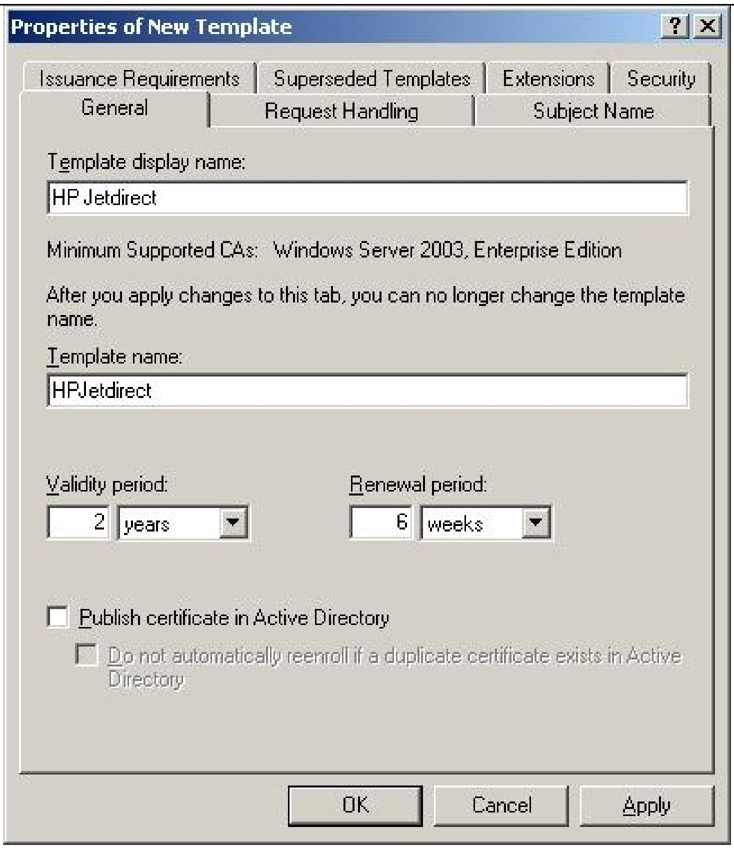
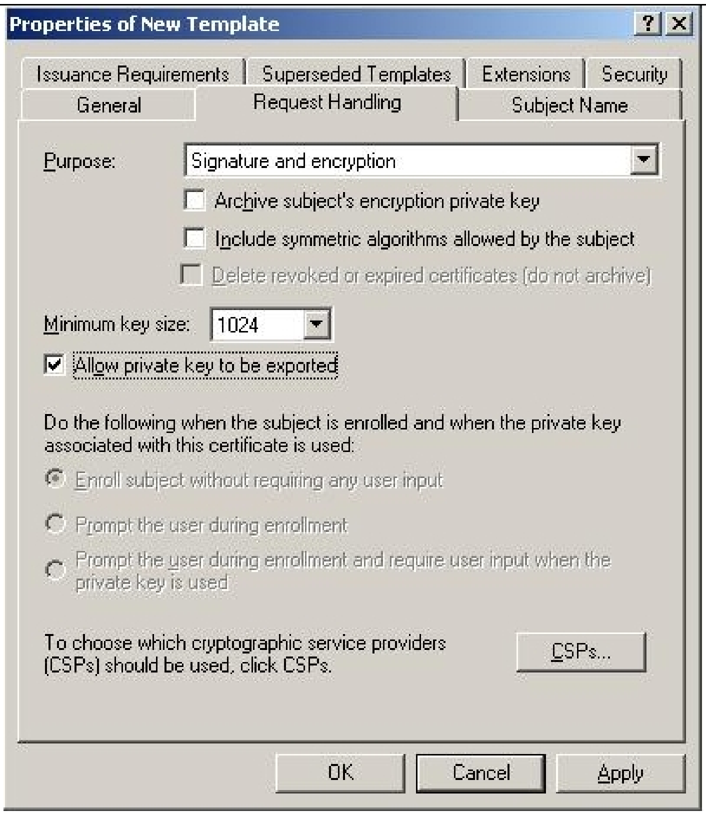
Select Certificate Templates.

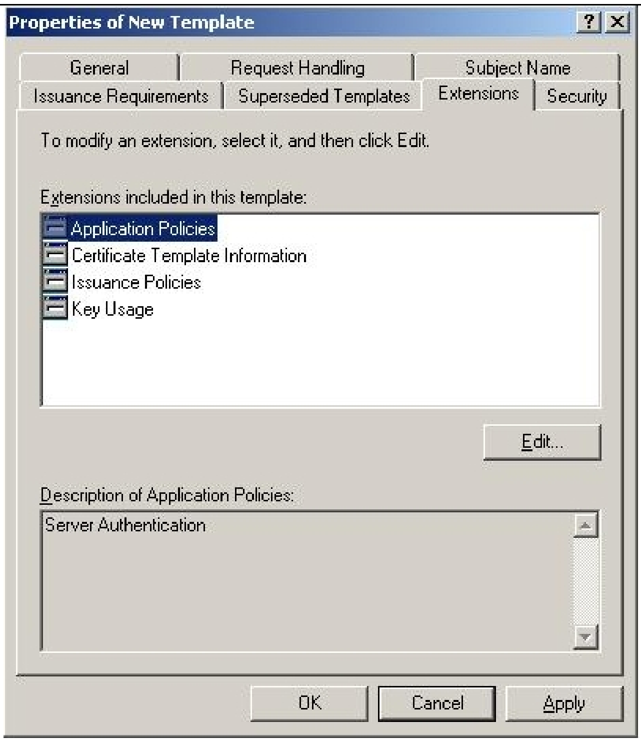
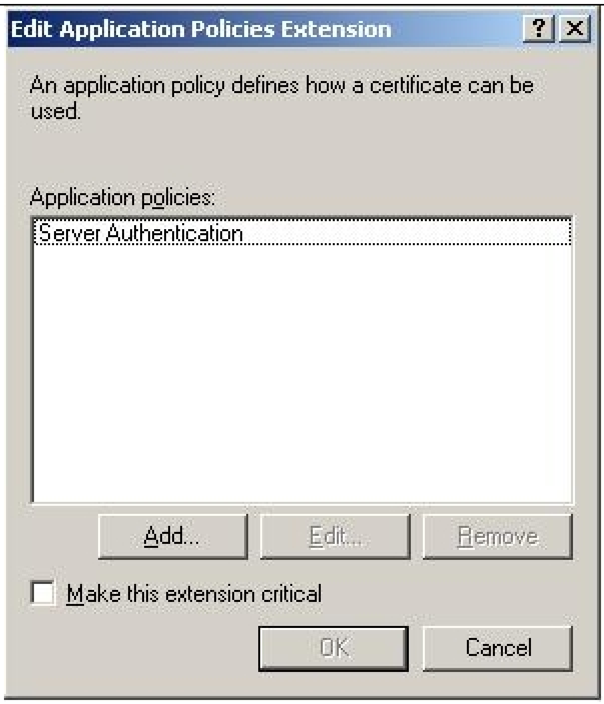
Highlight the "Web Server" template. Right click and copy the certificate template, and name it "HP Jetdirect". Now right click on "HP Jetdirect" and select properties.

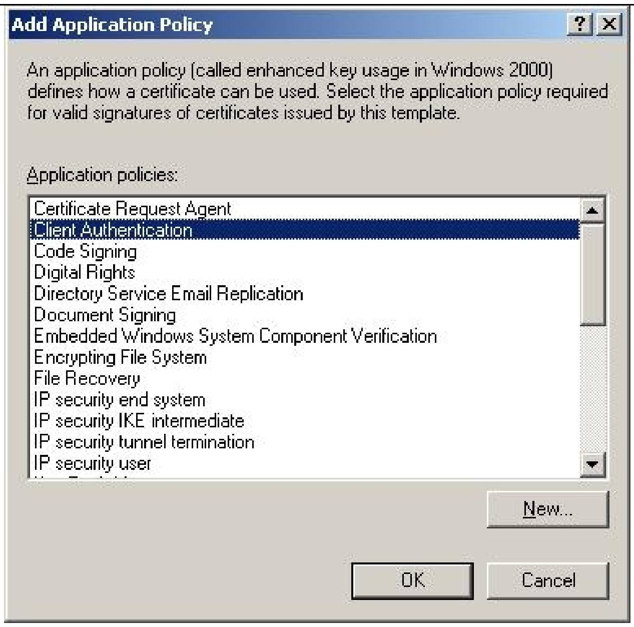
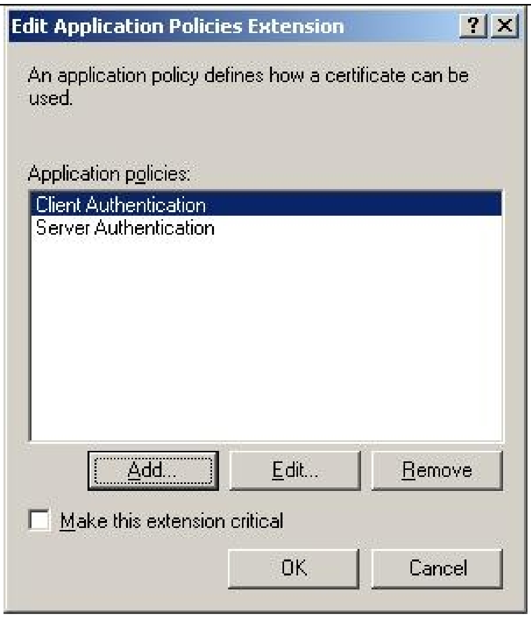


Console1 - [Console Root\Certificate Templates]

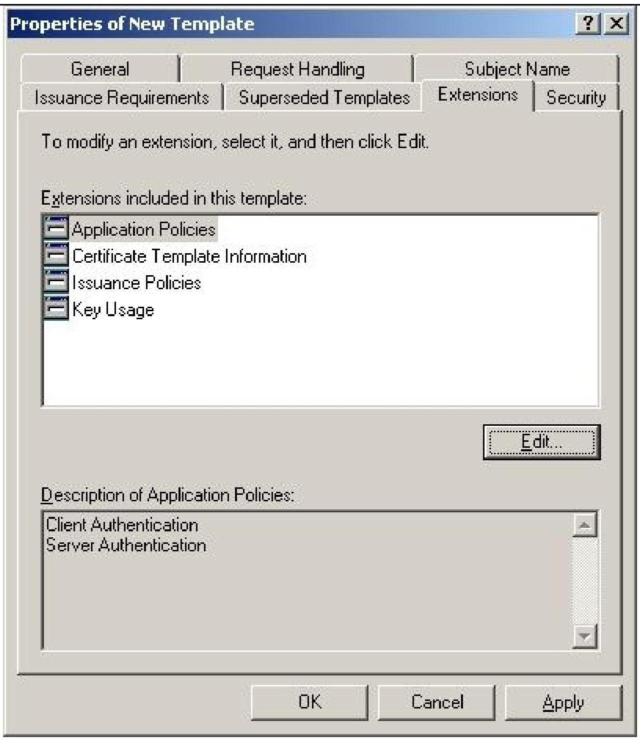
Template Display Name	Minimum Supported CAs	Version	Autoenrollment
Administrator	Windows 2000	4.1	Not allowed
Authenticated Session	Windows 2000	3.1	Not allowed
Basic EFS	Windows 2000	3.1	Not allowed
CA Exchange	Windows Server 2003, En...	106.0	Not allowed
CEP Encryption	Windows 2000	4.1	Not allowed
Code Signing	Windows 2000	3.1	Not allowed
Computer	Windows 2000	5.1	Not allowed
Cross Certification Authority	Windows Server 2003, En...	105.0	Not allowed
Directory Email Replication	Windows Server 2003, En...	115.0	Allowed
Domain Controller	Windows 2000	4.1	Not allowed
Domain Controller Authentication	Windows Server 2003, En...	110.0	Allowed
EFS Recovery Agent	Windows 2000	6.1	Not allowed
Enrollment Agent	Windows 2000	4.1	Not allowed
Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed
Exchange Signature Only	Windows 2000	6.1	Not allowed
Exchange User	Windows 2000	7.1	Not allowed
IPSec	Windows 2000	8.1	Not allowed
IPSec (Offline request)	Windows 2000	7.1	Not allowed
Key Recovery Agent	Windows Server 2003, En...	105.0	Allowed
RAS and IAS Server	Windows Server 2003, En...	101.0	Allowed
Root Certification Authority	Windows 2000	5.1	Not allowed
Router (Offline request)	Windows 2000	4.1	Not allowed
Smartcard Logon	Windows 2000	6.1	Not allowed
Smartcard User	Windows 2000	11.1	Not allowed
Subordinate Certification Authority	Windows 2000	5.1	Not allowed
Trust List Signing	Windows 2000	3.1	Not allowed
User	Windows 2000	3.1	Not allowed
User Signature Only	Windows 2000	4.1	Not allowed
Web Server	Windows 2000	4.1	Not allowed
Workstation Authentication	Windows Server 2003, En...	101.0	Allowed

Provide the names you would like the certificate template to have.	 Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name OK Cancel Apply Template display name: HP Jetdirect Minimum Supported CAs: Windows Server 2003, Enterprise Edition After you apply changes to this tab, you can no longer change the template name. Template name: HPJetdirect Validity period: 2 years Renewal period: 6 weeks □ Publish certificate in Active Directory □ Do not automatically reenroll if a duplicate certificate exists in Active Directory
Select the "Allow private key to be exported" checkbox in the Request Handling tab.	 Properties of New Template ? × Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name CSPs... OK Cancel Apply Purpose: Signature and encryption □ Archive subject's encryption private key □ Include symmetric algorithms allowed by the subject □ Delete revoked or expired certificates (do not archive) Minimum key size: 1024 ☑ Allow private key to be exported Do the following when the subject is enrolled and when the private key associated with this certificate is used: ● Enroll subject without requiring any user input ○ Prompt the user during enrollment ○ Prompt the user during enrollment and require user input when the private key is used To choose which cryptographic service providers (CSPs) should be used, click CSPs.

Select the Application Policies extension in the Extensions tab. Click Edit.	 Properties of New Template To modify an extension, select it, and then click Edit. Extensions included in this template: Application Policies Certificate Template Information Issuance Policies Key Usage Description of Application Policies: Server Authentication General Request Handling Subject Name Issuance Requirements Superseded Templates Extensions Security Edit... OK Cancel Apply
Click Add…	 Edit Application Policies Extension An application policy defines how a certificate can be used. Application policies: Server Authentication □ Make this extension critical

Select Client Authentication, then click OK.	 Add Application Policy An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template. Application policies: Certificate Request Agent Client Authentication Code Signing Digital Rights Directory Service Email Replication Document Signing Embedded Windows System Component Verification Encrypting File System File Recovery IP security end system IP security IKE intermediate IP security tunnel termination IP security user
Click OK.	 Edit Application Policies Extension An application policy defines how a certificate can be used. Application policies: Client Authentication Server Authentication □ Make this extension critical

Click OK.



To modify an extension, select it, and then click Edit.

Extensions included in this template:

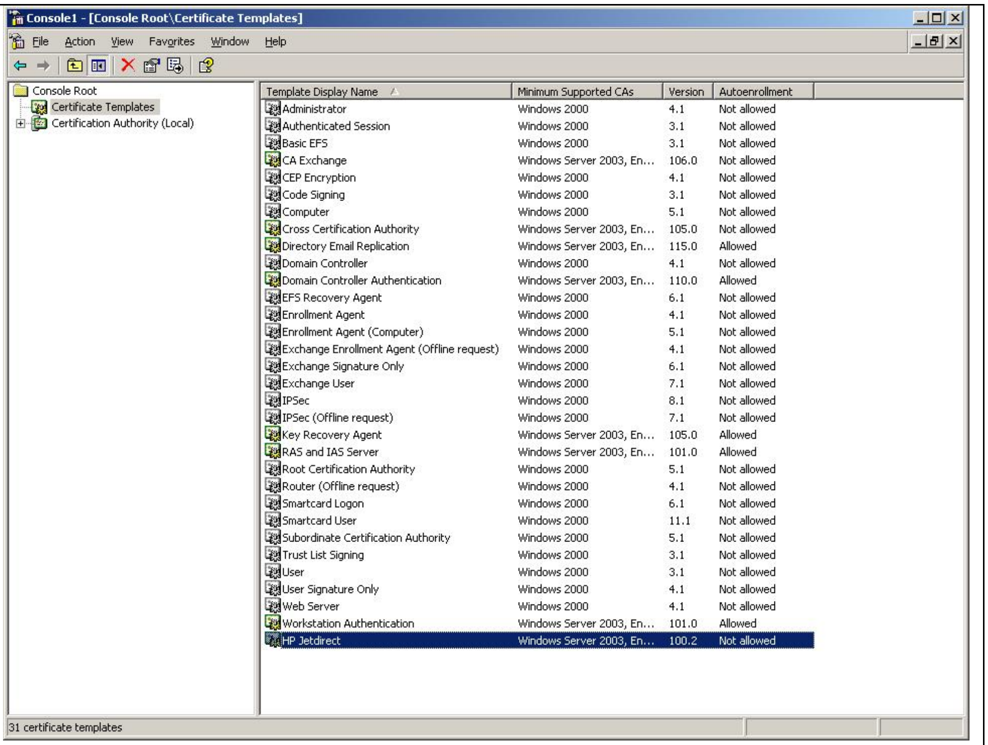
- Application Policies
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication
Server Authentication

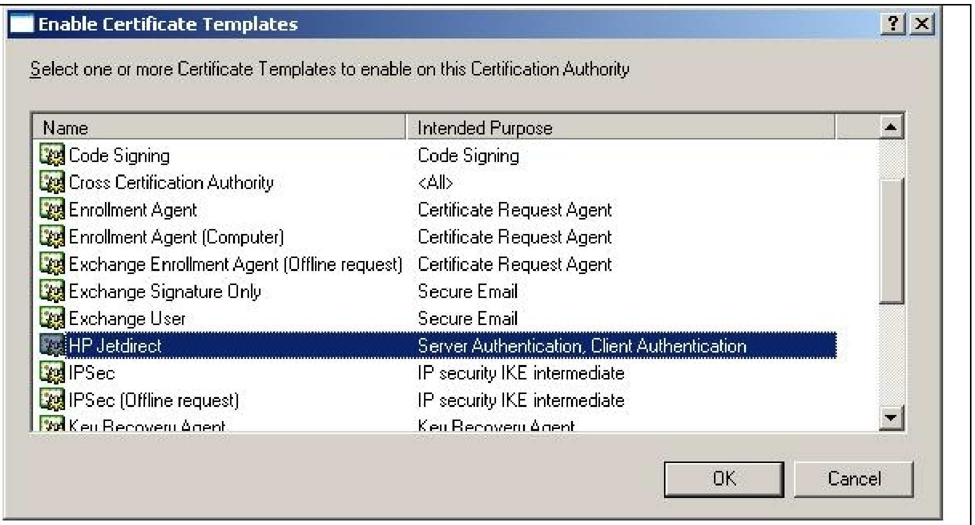
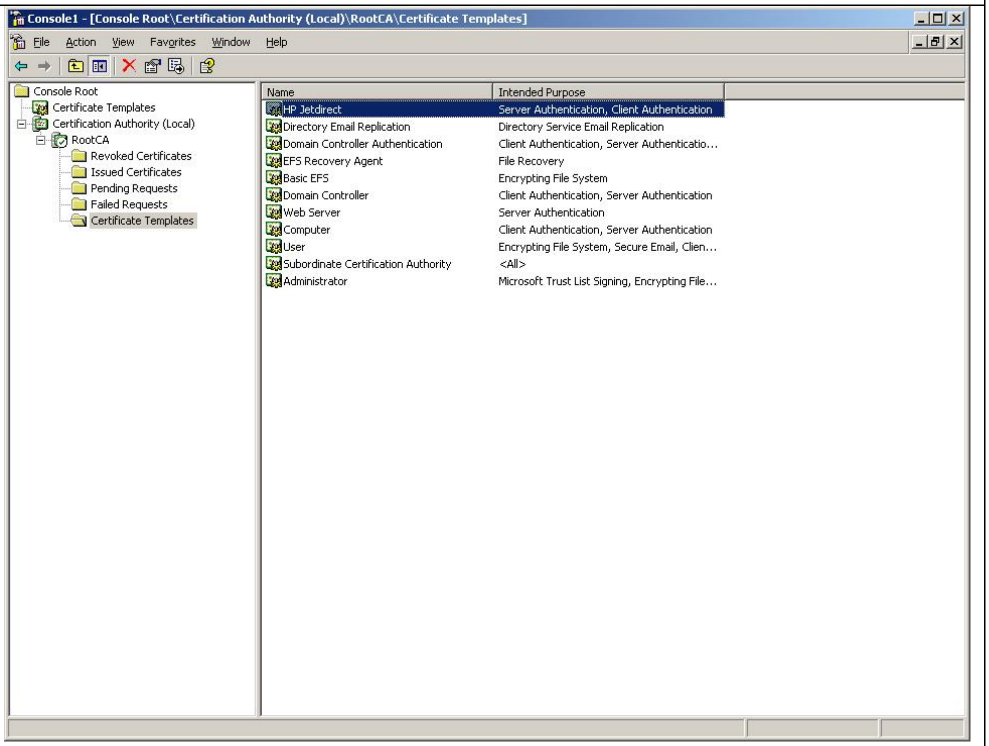
Now we have created a new certificate template, we need to enable it to be used by the Certification Authority.

Select the HP Jetdirect certificate template, Right click and select "Enable"


Console1 - [Console Root\Certificate Templates]
File
Action
View
Favorites
Window
Help
Console Root
Certificate Templates
Certification Authority (Local)

Template Display Name	Minimum Supported CAs	Version	Autoenrollment
Administrator	Windows 2000	4.1	Not allowed
Authenticated Session	Windows 2000	3.1	Not allowed
Basic EFS	Windows 2000	3.1	Not allowed
CA Exchange	Windows Server 2003, En...	106.0	Not allowed
CEP Encryption	Windows 2000	4.1	Not allowed
Code Signing	Windows 2000	3.1	Not allowed
Computer	Windows 2000	5.1	Not allowed
Cross Certification Authority	Windows Server 2003, En...	105.0	Not allowed
Directory Email Replication	Windows Server 2003, En...	115.0	Allowed
Domain Controller	Windows 2000	4.1	Not allowed
Domain Controller Authentication	Windows Server 2003, En...	110.0	Allowed
EFS Recovery Agent	Windows 2000	6.1	Not allowed
Enrollment Agent	Windows 2000	4.1	Not allowed
Enrollment Agent (Computer)	Windows 2000	5.1	Not allowed
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1	Not allowed
Exchange Signature Only	Windows 2000	6.1	Not allowed
Exchange User	Windows 2000	7.1	Not allowed
IPSec	Windows 2000	8.1	Not allowed
IPSec (Offline request)	Windows 2000	7.1	Not allowed
Key Recovery Agent	Windows Server 2003, En...	105.0	Allowed
RAS and IAS Server	Windows Server 2003, En...	101.0	Allowed
Root Certification Authority	Windows 2000	5.1	Not allowed
Router (Offline request)	Windows 2000	4.1	Not allowed
Smartcard Logon	Windows 2000	6.1	Not allowed
Smartcard User	Windows 2000	11.1	Not allowed
Subordinate Certification Authority	Windows 2000	5.1	Not allowed
Trust List Signing	Windows 2000	3.1	Not allowed
User	Windows 2000	3.1	Not allowed
User Signature Only	Windows 2000	4.1	Not allowed
Web Server	Windows 2000	4.1	Not allowed
Workstation Authentication	Windows Server 2003, En...	101.0	Allowed
HP Jetdirect	Windows Server 2003, En...	100.2	Not allowed

31 certificate templates

Select HP Jetdirect and click OK.	
View the Certificate Templates folder in the Certification Authority snap-in MMC, and make sure that the HP Jetdirect template is present. Done.	

Select one or more Certificate Templates to enable on this Certification Authority

Name	Intended Purpose
Code Signing	Code Signing
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
HP Jetdirect	Server Authentication, Client Authentication
IPSec	IP security IKE intermediate
IPSec (Offline request)	IP security IKE intermediate
Key Recovery Agent	Key Recovery Agent

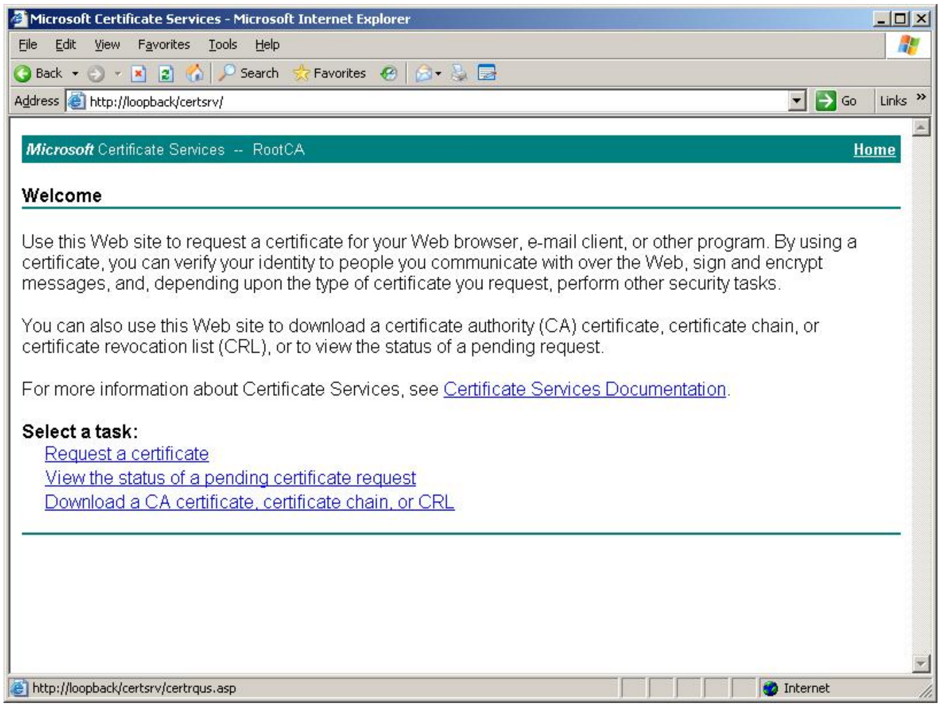
Name	Intended Purpose
HP Jetdirect	Server Authentication, Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

PKI: Issuing a Certificate

Now that we have the Certification Authority installed, we can use the CA's web server interface to issue a certificate for Jetdirect and to copy the public certificate of the CA to a file for Jetdirect to use.

Bring up the web server for the CA.

Using the URL for the certsrv, we get to the web interface of the Certification Authority. Since we want to create a certificate for Jetdirect, click the "Request a certificate" link.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://loopback/certsrv/
Go Links
Microsoft Certificate Services -- RootCA
Home
http://loopback/certsrv/certrqus.asp
Internet

Welcome

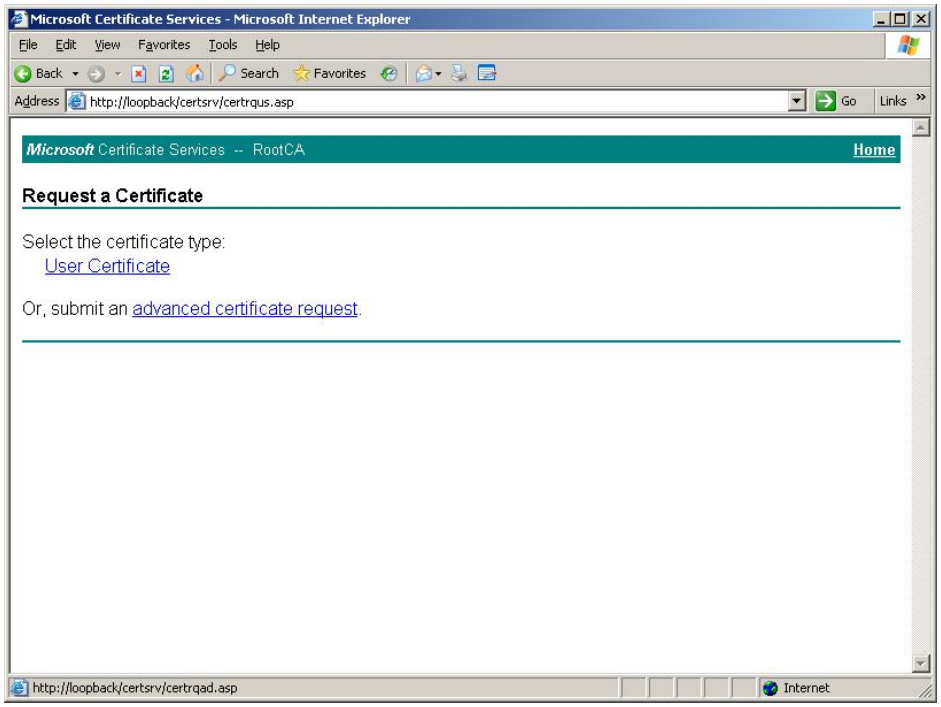
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

Click "advanced certificate request"

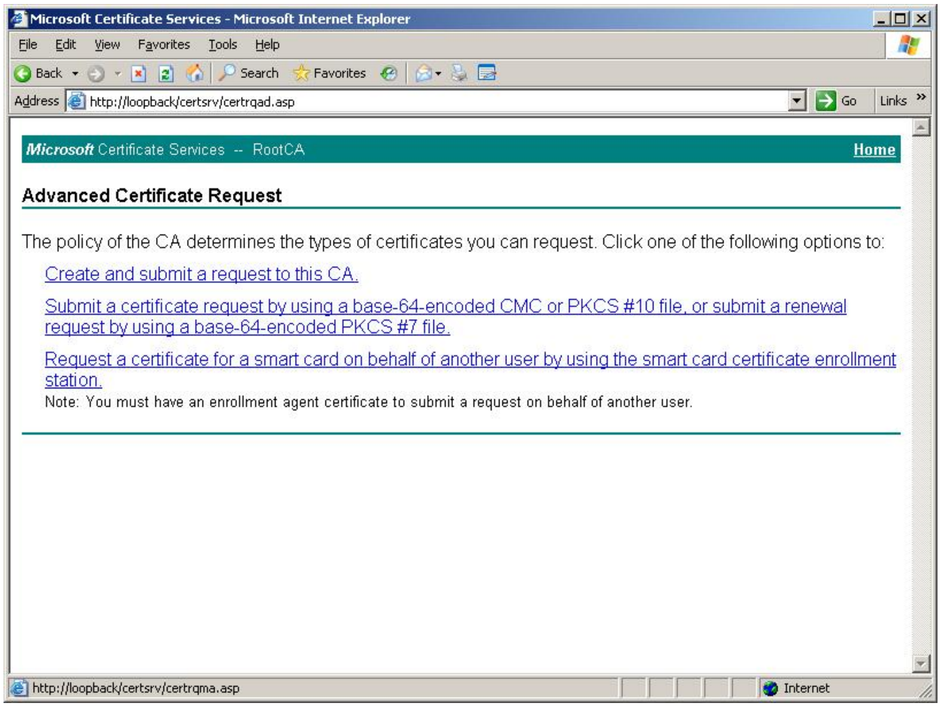

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://loopback/certsrv/certrqus.asp
Go Links
Microsoft Certificate Services -- RootCA
Home
http://loopback/certsrv/certrqad.asp
Internet

Request a Certificate

Select the certificate type:
- User Certificate

Or, submit an advanced certificate request.

Click “Create and submit a request to this CA”.



http://loopback/certsrv/certrqad.asp

Microsoft Certificate Services -- RootCA

Home

Advanced Certificate Request

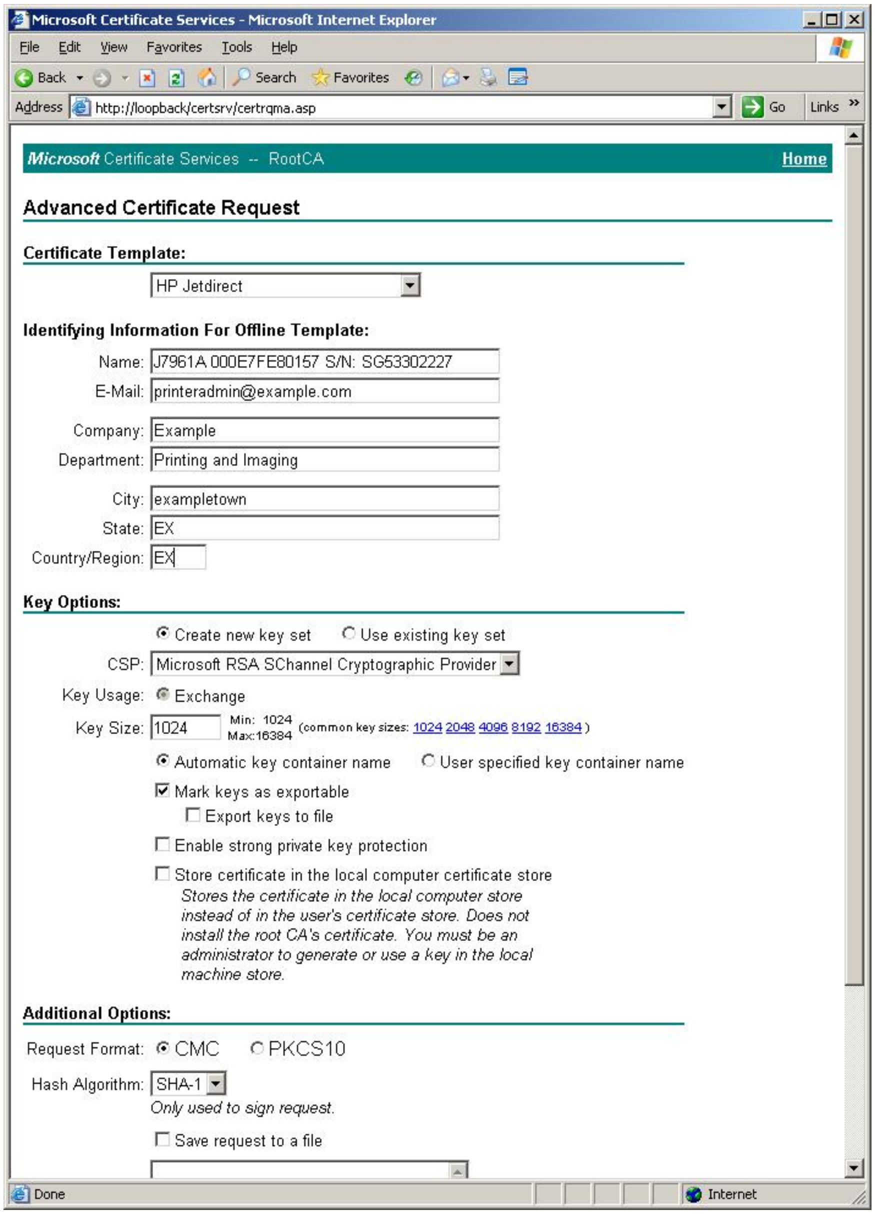
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- Create and submit a request to this CA.
- Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

http://loopback/certsrv/certrqma.asp

Be sure to select the Certificate Template "HP Jetdirect" and to check the checkbox entitled "Mark keys as exportable". Although this example doesn't show the DNS name, we would generally use the DNS name for the "Name" field.



Microsoft Certificate Services - Microsoft Internet Explorer

Address http://loopback/certsrv/certrqma.asp

Microsoft Certificate Services -- RootCA

Advanced Certificate Request

Certificate Template:

HP Jetdirect

Identifying Information For Offline Template:

Name:	J7961A 000E7FE80157 S/N: SG53302227
E-Mail:	printeradmin@example.com
Company:	Example
Department:	Printing and Imaging
City:	exampletown
State:	EX
Country/Region:	EX

Key Options:

● Create new key set ○ Use existing key set

CSP: Microsoft RSA SChannel Cryptographic Provider

Key Usage: ● Exchange

Key Size: 1024 Min: 1024 Max:16384 (common key sizes: 1024 2048 4096 8192 16384)

● Automatic key container name ○ User specified key container name

☑ Mark keys as exportable

□ Export keys to file

□ Enable strong private key protection

□ Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

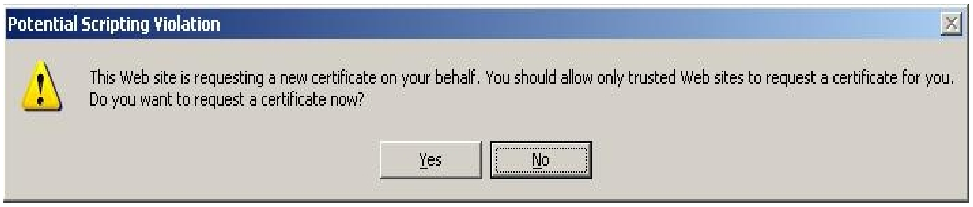
Request Format: ● CMC ○ PKCS10

Hash Algorithm: SHA-1

Only used to sign request.

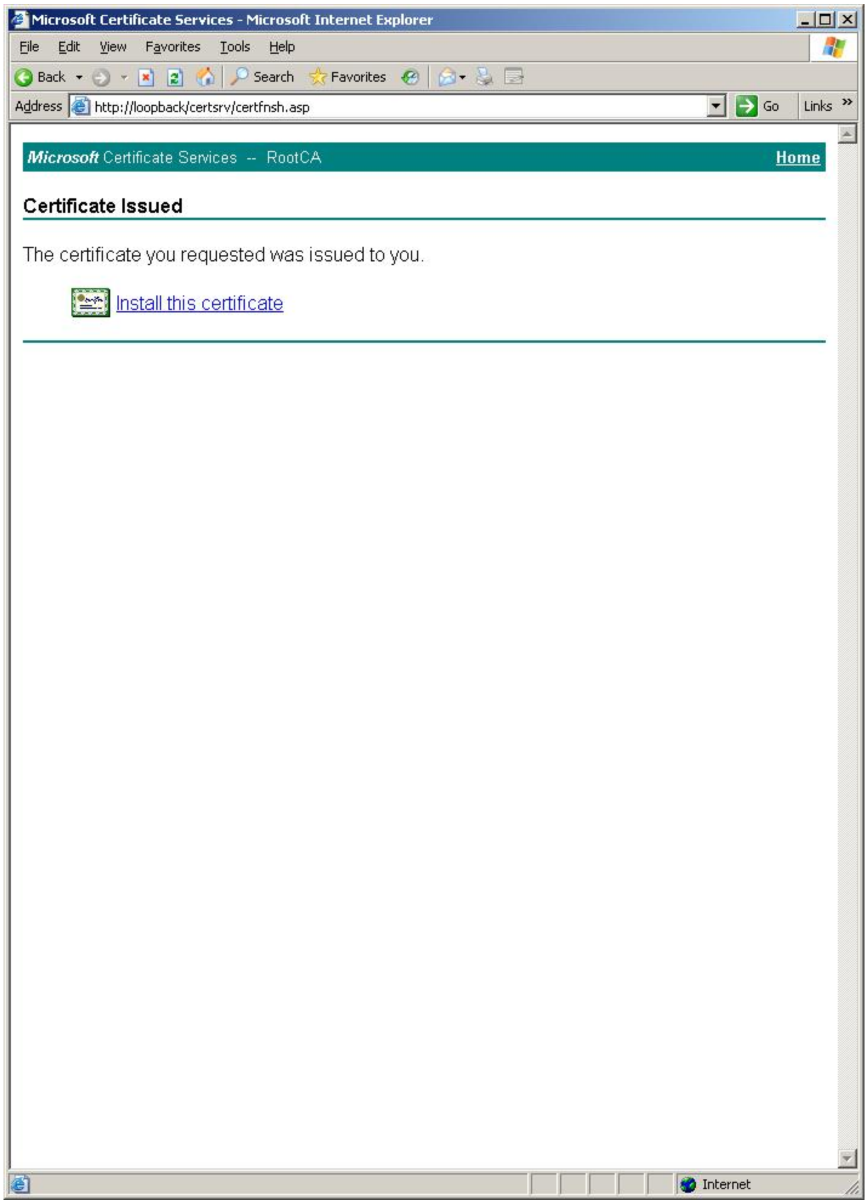
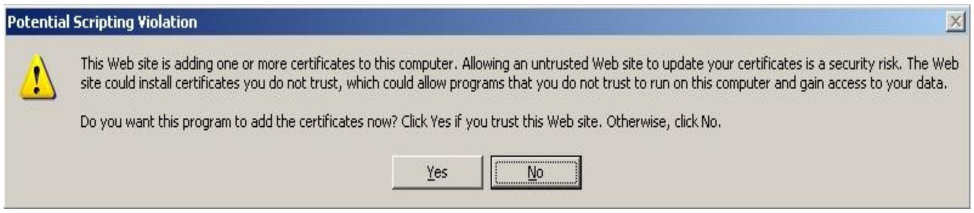
□ Save request to a file

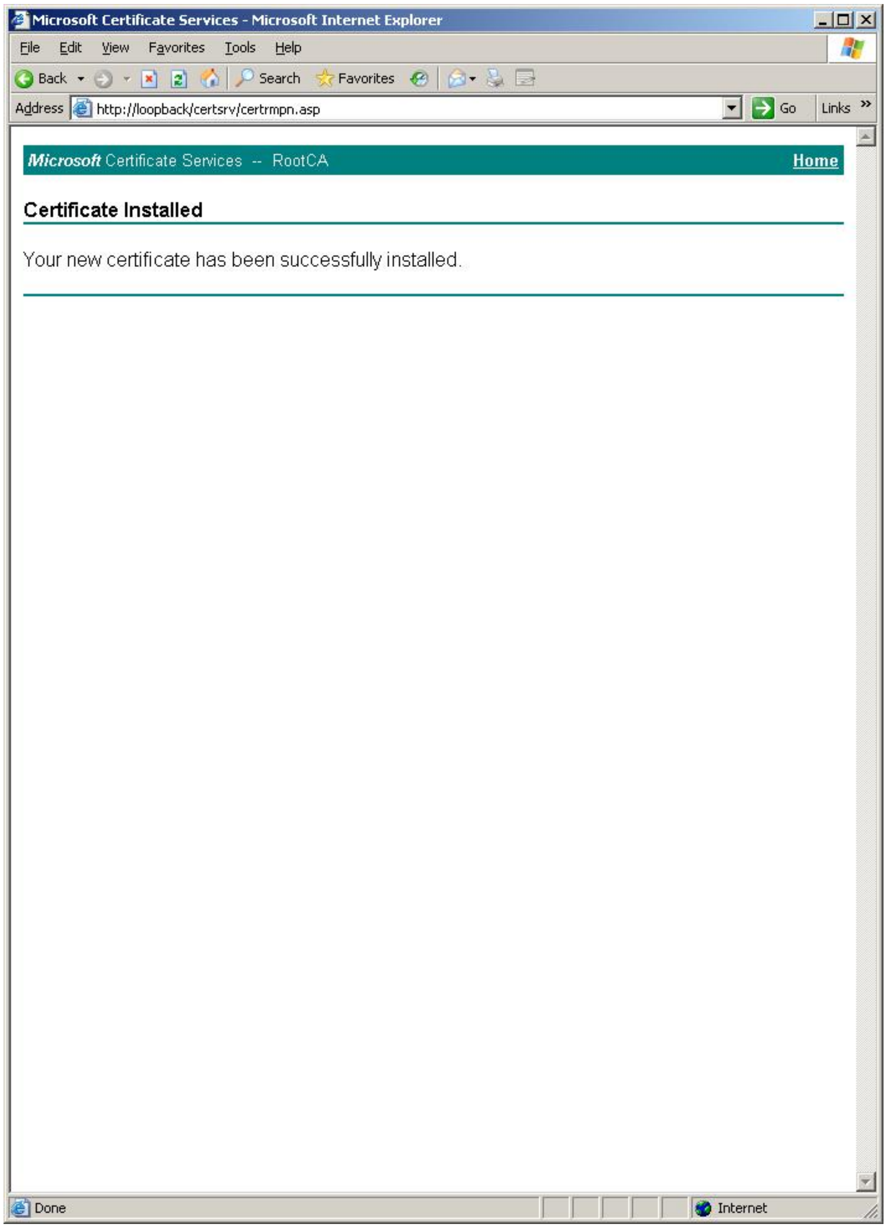
Click Yes.



Potential Scripting Violation

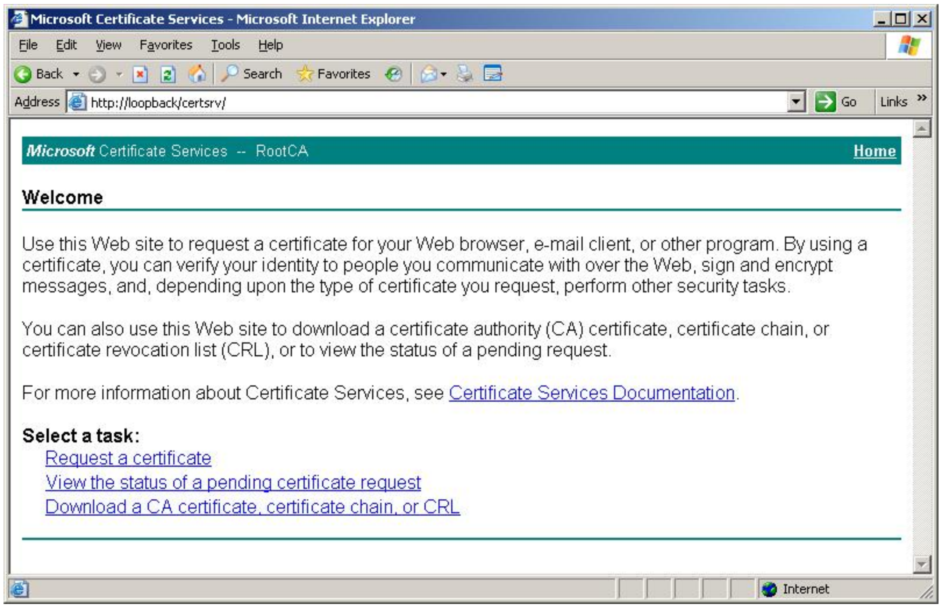
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

Click "Install this certificate" to install it on your local computer. We will export it and then delete it from this computer later.	 Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address Go Links Home Internet http://loopback/certsrv/certfnsh.asp Microsoft Certificate Services -- RootCA Certificate Issued The certificate you requested was issued to you. Install this certificate
Click Yes.	 Potential Scripting Violation This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

Done.	 Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address http://loopback/certsrv/certrmpn.asp Go Links Microsoft Certificate Services -- RootCA Home **Certificate Installed** Your new certificate has been successfully installed.

Up to this point, we have loaded the Jetdirect certificate in the local certificate store of the computer running the web browser. Later, we will go back and export this certificate so that we can import it into Jetdirect. For now, we need to download the CA certificate for Jetdirect.

From the main web interface, click "Download a CA certificate…"


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://loopback/certsrv/
Go Links
Internet

Microsoft Certificate Services -- RootCA **Home**

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

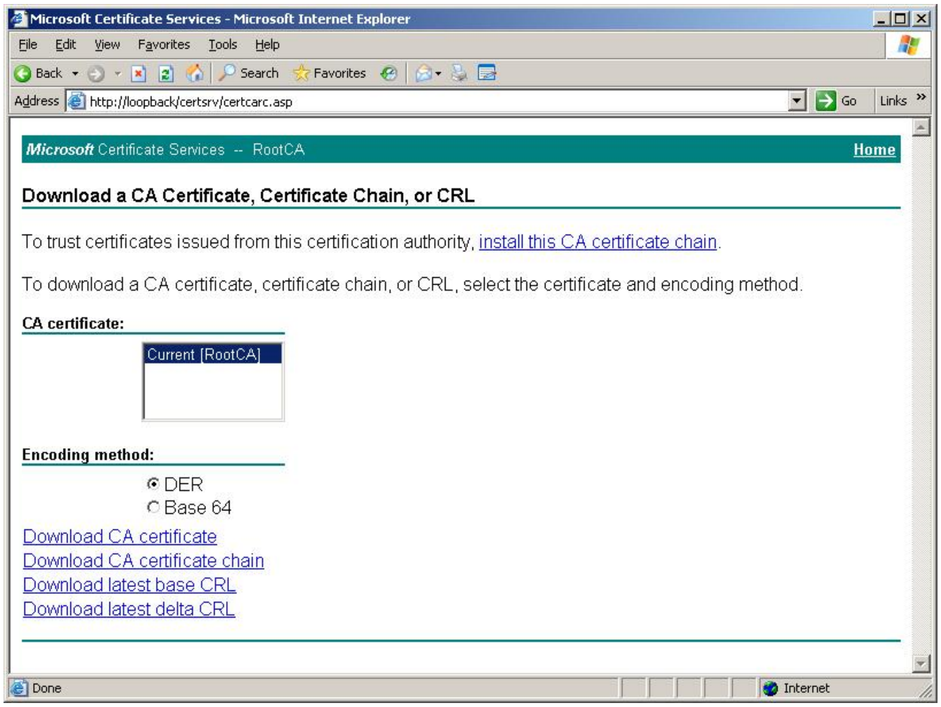
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Select "Current [RootCA]", then DER (or Base 64 if you are using an older Jetdirect product), then click "Download CA certificate",


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://loopback/certsrv/certcarc.asp
Go Links
Done
Internet

Microsoft Certificate Services -- RootCA **Home**

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

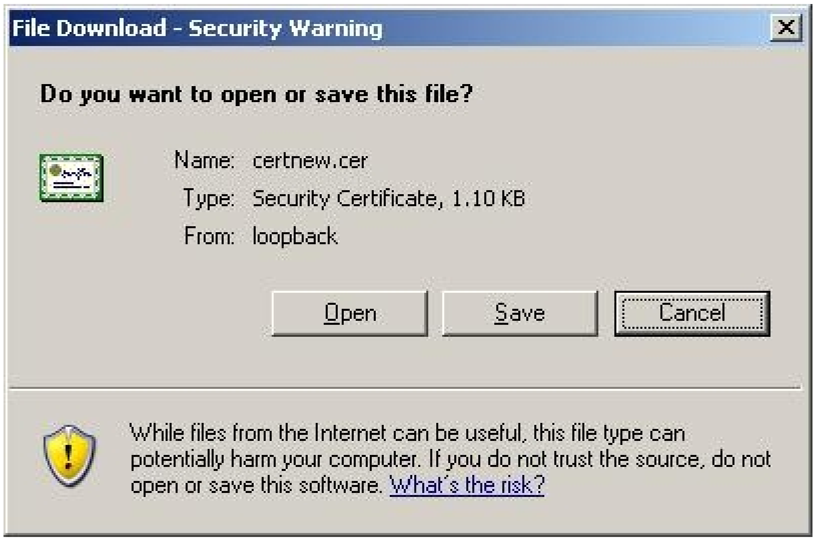
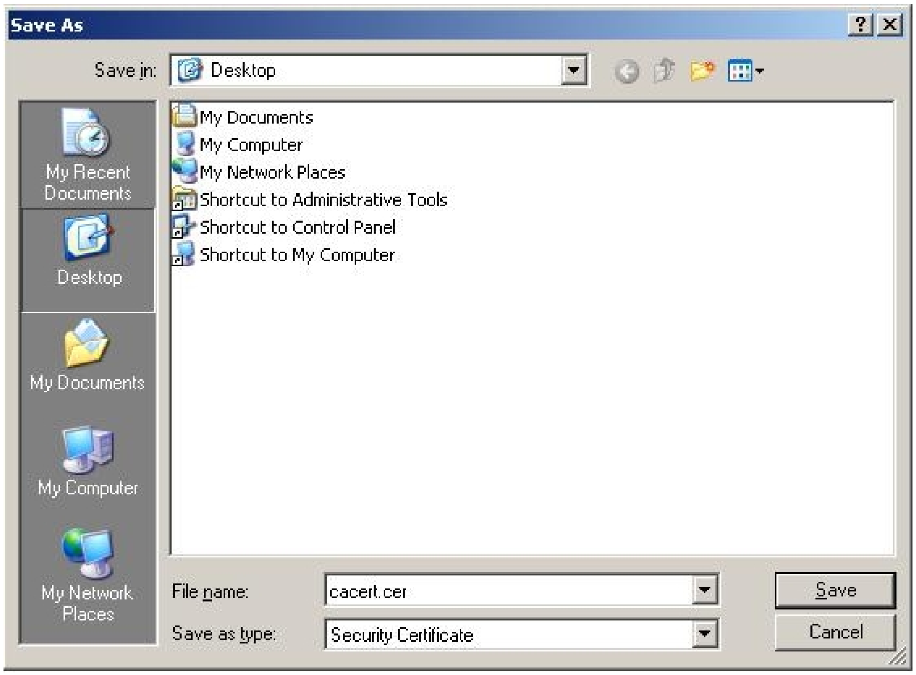
CA certificate:

Current [RootCA]

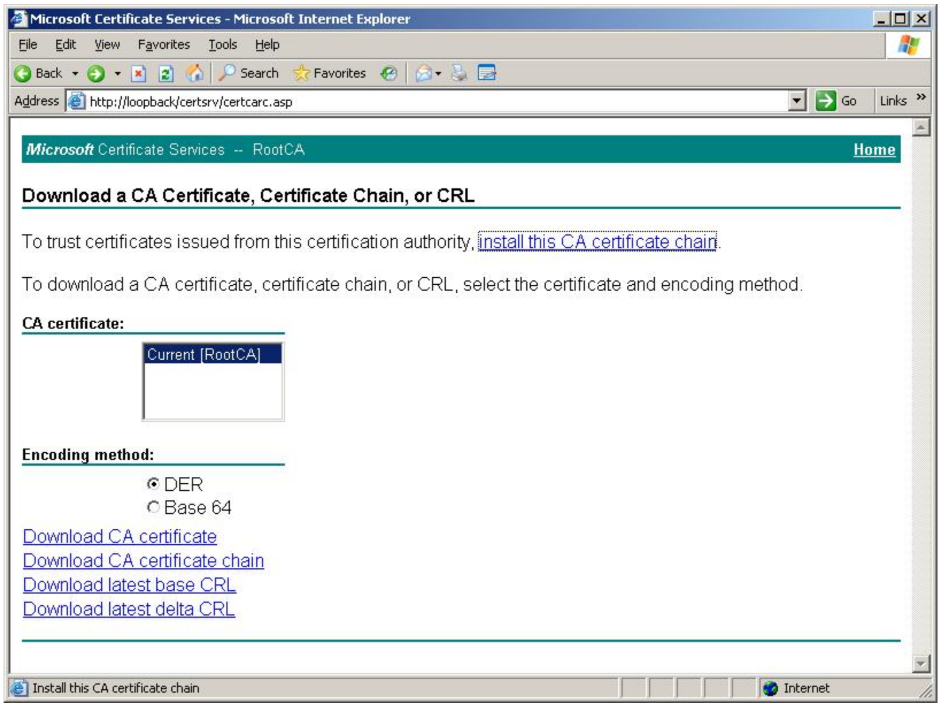
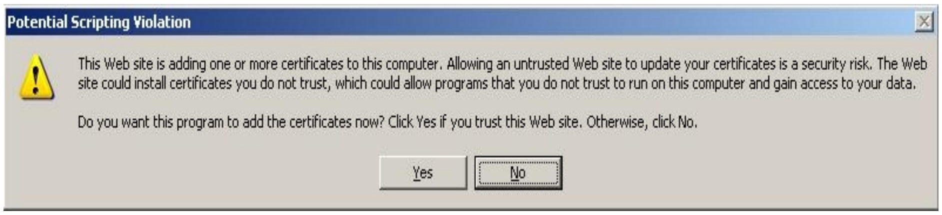
Encoding method:

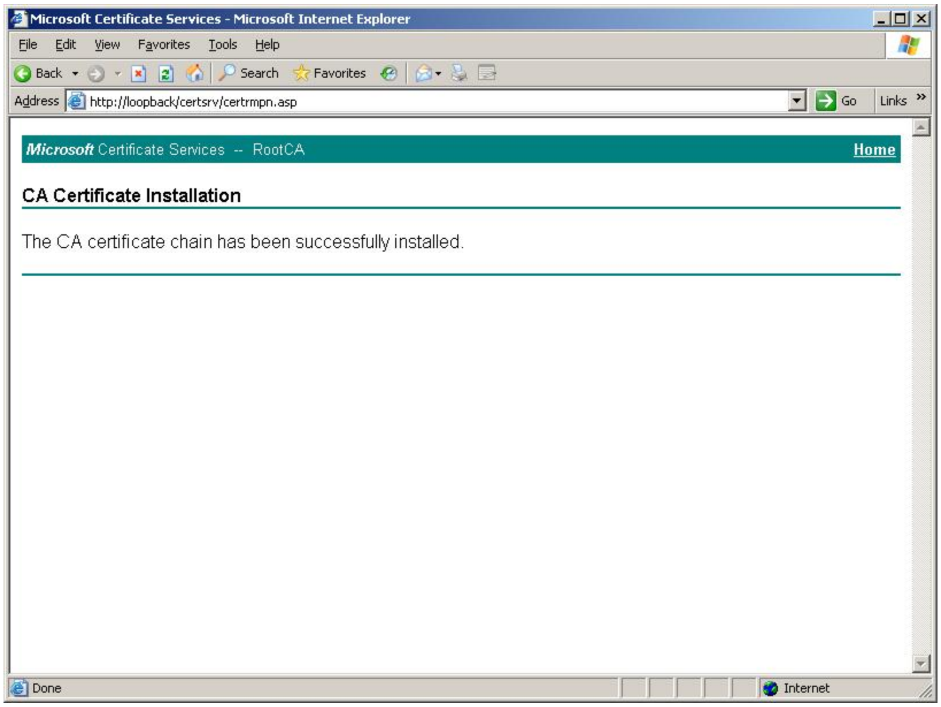
● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

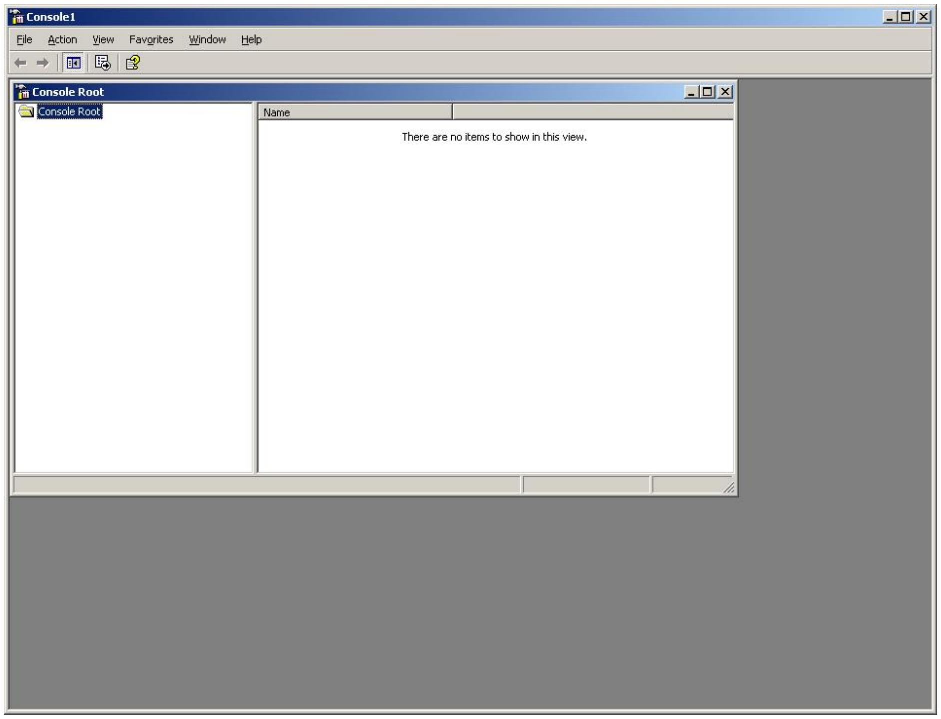
Click Save.	 File Download - Security Warning Do you want to open or save this file? Name: certnew.cer Type: Security Certificate, 1.10 KB From: loopback While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?
Name the file "cacert.cer"	 Save As Save in: Desktop My Documents My Computer My Network Places Shortcut to Administrative Tools Shortcut to Control Panel Shortcut to My Computer My Recent Documents Desktop My Documents My Computer My Network Places File name: cacert.cer Save as type: Security Certificate

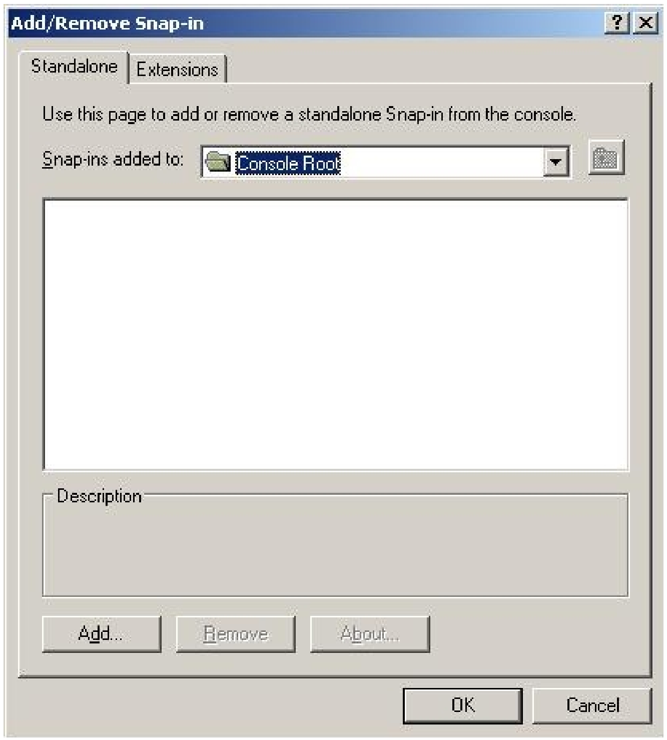
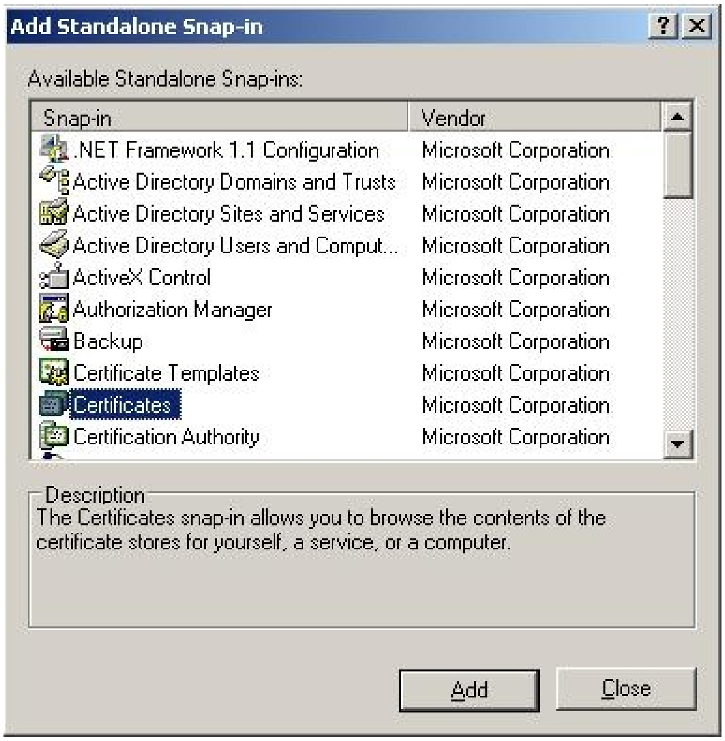
We also want to install the CA certificate chain on the local computer. This will allow the browser to recognize certificates issued by the CA as trusted.

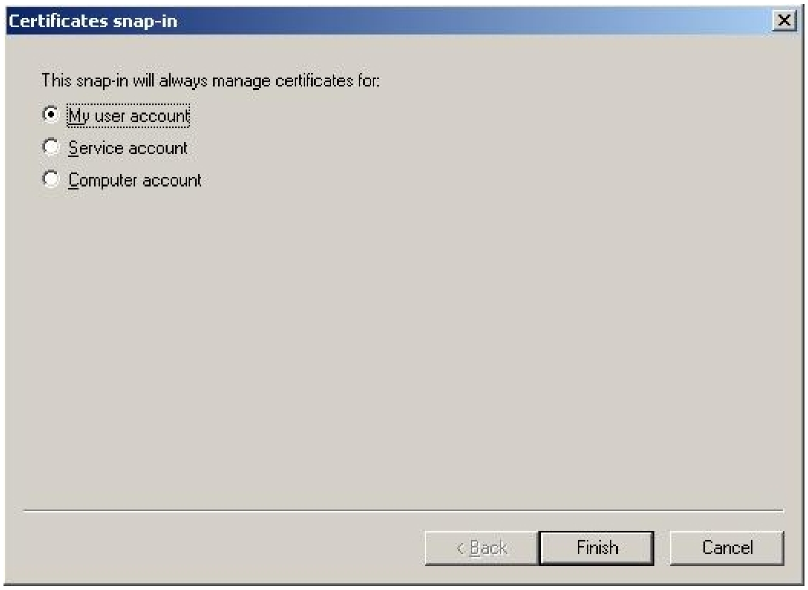
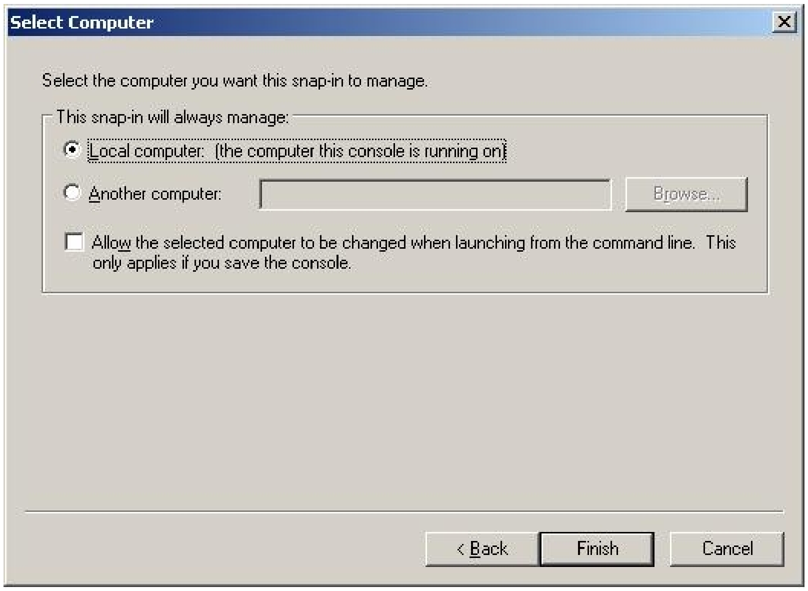
Click "Install this CA certificate chain".	 Microsoft Certificate Services - Microsoft Internet Explorer Address http://loopback/certsrv/certcarc.asp *Microsoft* Certificate Services -- RootCA Home **Download a CA Certificate, Certificate Chain, or CRL** To trust certificates issued from this certification authority, install this CA certificate chain. To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method. **CA certificate:** Current [RootCA] **Encoding method:** ● DER ○ Base 64 Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL Install this CA certificate chain Internet
Click Yes.	 Potential Scripting Violation This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data. Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No. Yes No

Done	 Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address Go Links http://loopback/certsrv/certrmpn.asp *Microsoft* Certificate Services -- RootCA Home **CA Certificate Installation** The CA certificate chain has been successfully installed. Done Internet

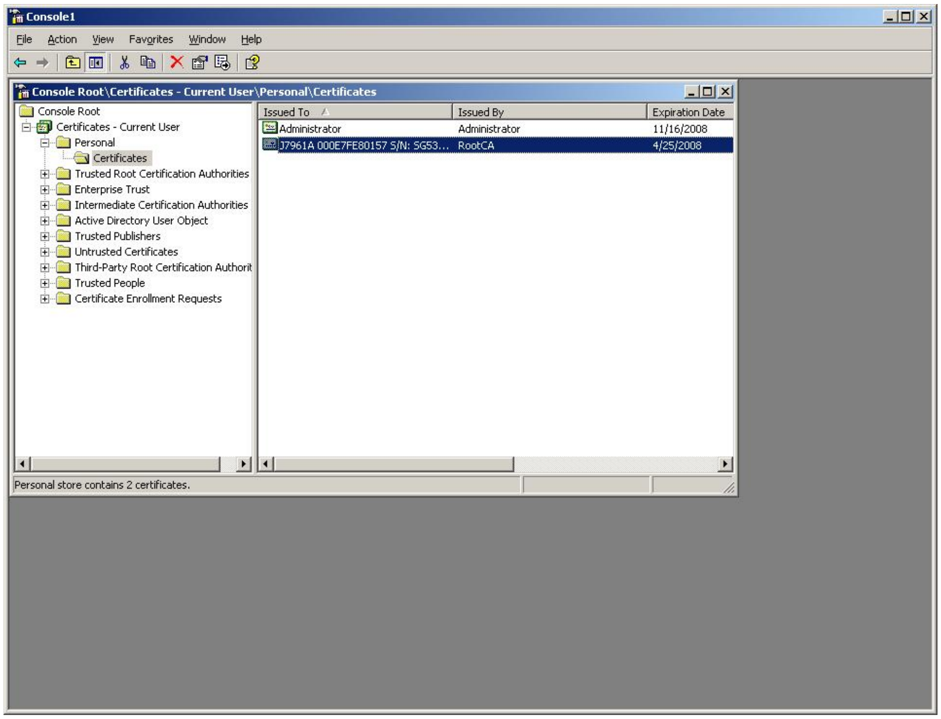
At this point, we want to export the certificate so that it can be loaded with its private key into Jetdirect. We need to bring up MMC again and load the Certificates snap-in.

Go to the File Menu and select Add/Remove Snap-In.	 Console1 File Action View Favorites Window Help Console Root Console Root Name There are no items to show in this view.

Click “Add…”	 Use this page to add or remove a standalone Snap-in from the console. Snap-ins added to: Console Root Add/Remove Snap-in Standalone Extensions Description Add... Remove About... OK Cancel
Click “Certificates”	 Available Standalone Snap-ins: Snap-in Vendor .NET Framework 1.1 Configuration Microsoft Corporation Active Directory Domains and Trusts Microsoft Corporation Active Directory Sites and Services Microsoft Corporation Active Directory Users and Comput... Microsoft Corporation ActiveX Control Microsoft Corporation Authorization Manager Microsoft Corporation Backup Microsoft Corporation Certificate Templates Microsoft Corporation Certificates Microsoft Corporation Certification Authority Microsoft Corporation Description The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Click “My user account”	 Certificates snap-in This snap-in will always manage certificates for: ● My user account ○ Service account ○ Computer account < Back · Finish · Cancel
Click “Local Computer”	 Select Computer Select the computer you want this snap-in to manage. This snap-in will always manage: ● Local computer: (the computer this console is running on) ○ Another computer: Browse... □ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console. < Back · Finish · Cancel

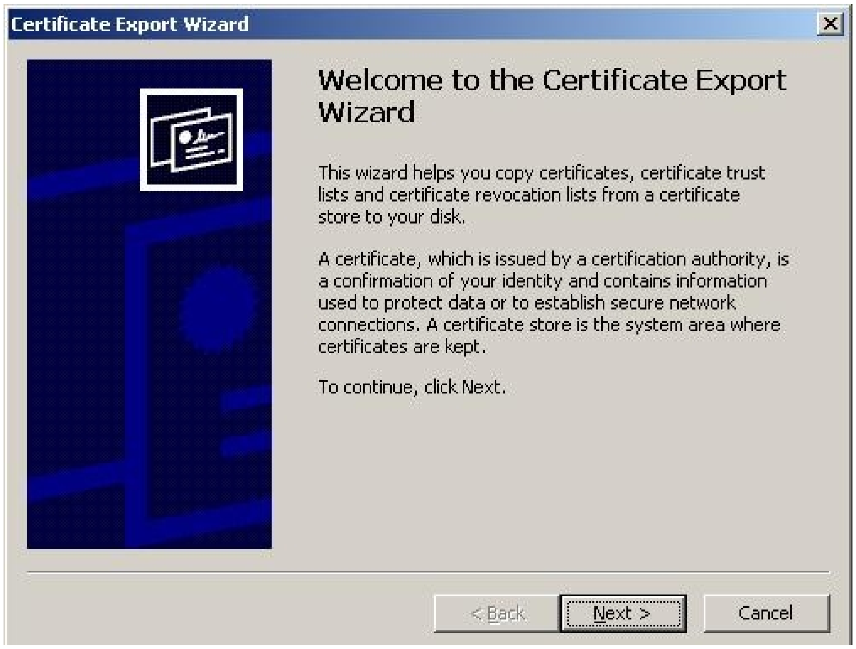
Select the folder “Certificates” under “Personal”. Highlight the Jetdirect certificate issued. Right Click and select “Export…”


Console1
File
Action
View
Favorites
Window
Help
Console Root\Certificates - Current User\Personal\Certificates
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorit
Trusted People
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date
Administrator	Administrator	11/16/2008
J7961A 000E7FE80157 S/N: SG53…	RootCA	4/25/2008

Personal store contains 2 certificates.

The “Certificate Export Wizard” launches – Press “Next”



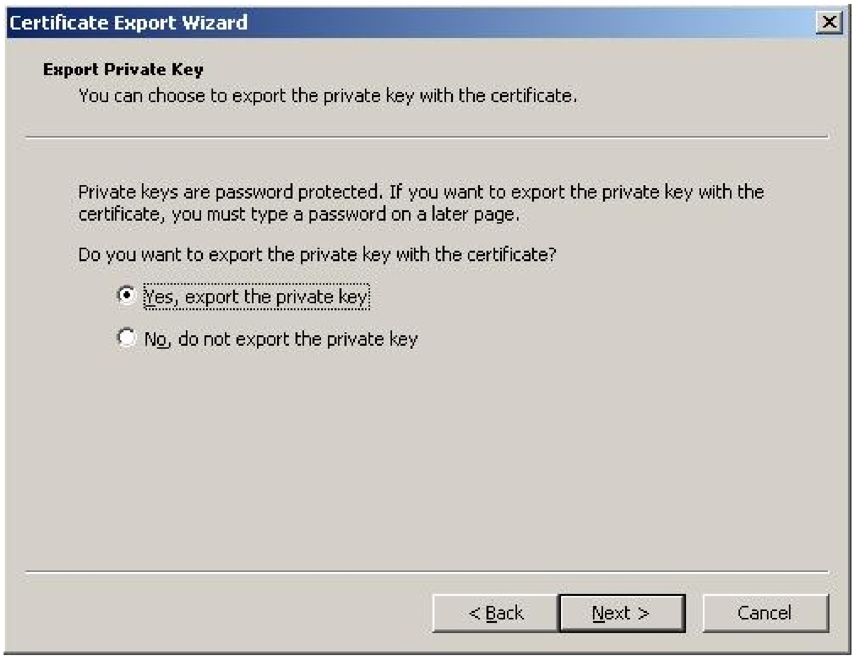
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Since we are going to import this certificate into Jetdirect, we need to export the private key as well. Select "Yes, export the private key" and then click "Next".



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

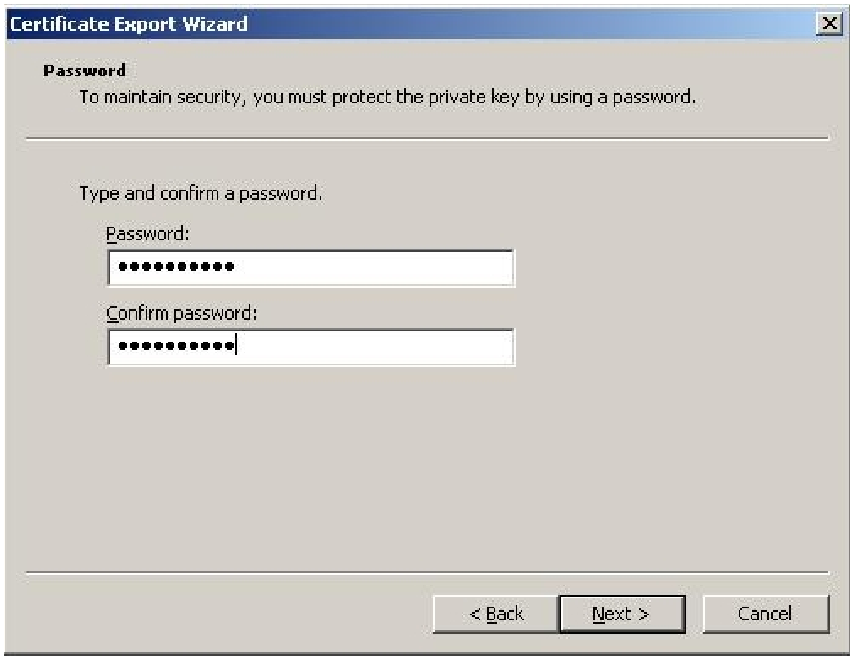
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

NOTE: In most cases, when exporting a certificate, you will not want to export the private key. The private key is best kept on the machine that generated it and never moved. This functionality is usually done by generating a Certificate Signing Request (CSR) on Jetdirect. The CSR process on Jetdirect creates a public and private key pair and includes the public key with the CSR while the private key is stored in flash and never exposed external to the Jetdirect device. The CSR is then sent to the Certificate Authority which issues a certificate based upon the information in the request. This certificate would be simply "installed" in Jetdirect and not "imported". Unfortunately, the Enterprise CA modifies the certificate in a way that is not compatible with Jetdirect's CSR and this resulted in Jetdirect refusing to accept the certificate during its installation. Jetdirect has since addressed this problem starting with version V.36.11. Using V.36.11 and later, certificates issued from the Enterprise CAs using a Jetdirect CSR file are accepted. As this process is more secure and preferred, we will cover it later in the whitepaper.

Type a password to protect the private key. Click "Next".



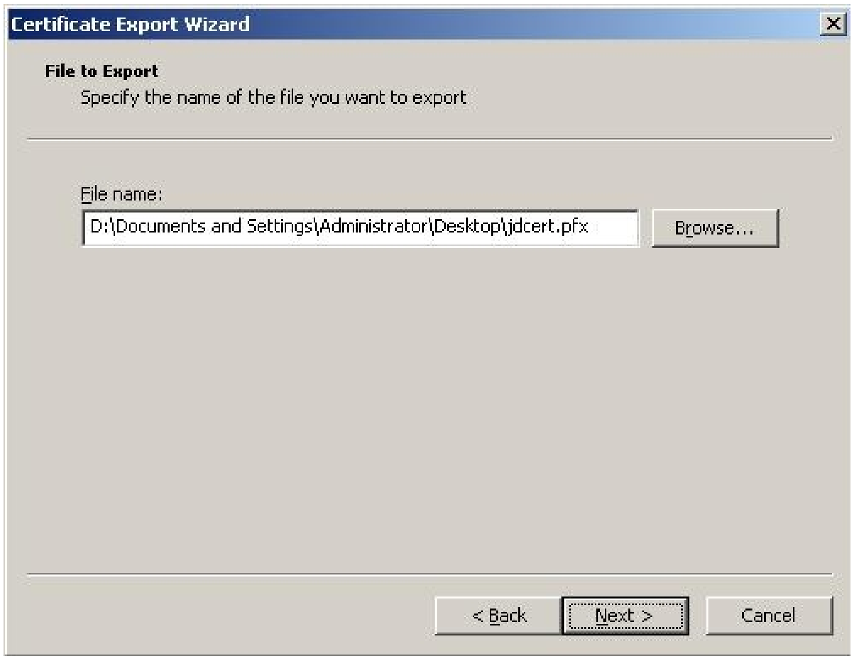
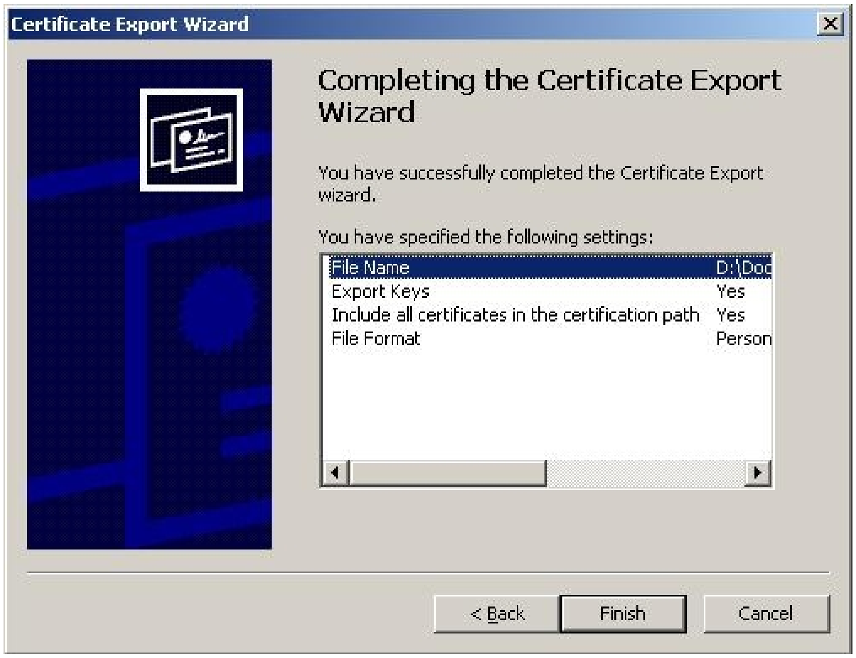
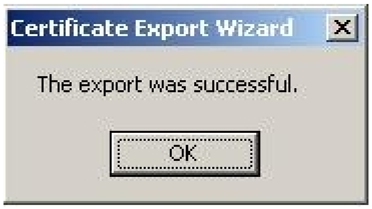
Certificate Export Wizard

Password
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ●●●●●●●●●●●

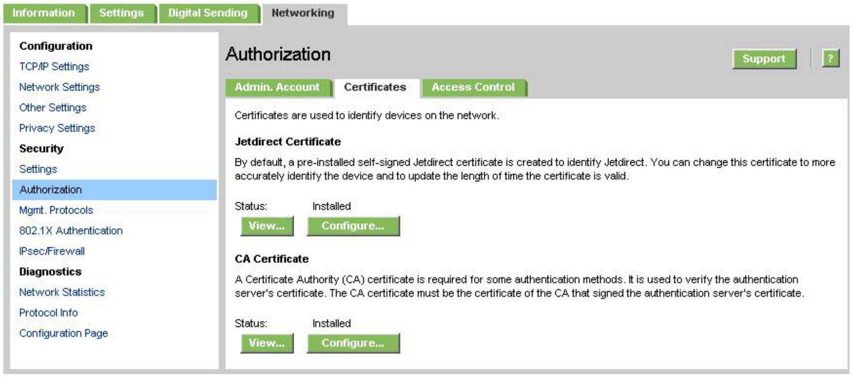
Confirm password: ●●●●●●●●●●●

Name the file “jdcert.pfx” and click “Next”	 Certificate Export Wizard **File to Export** Specify the name of the file you want to export File name: D:\Documents and Settings\Administrator\Desktop\jdcert.pfx
Click Finish	 Certificate Export Wizard Completing the Certificate Export Wizard You have successfully completed the Certificate Export wizard. You have specified the following settings: File Name D:\Doc Export Keys Yes Include all certificates in the certification path Yes File Format Person
Click Ok.	 Certificate Export Wizard The export was successful.

PKI: Creating a Jetdirect CSR and Installing the Certificate

Starting with Jetdirect firmware version V.36.11, certificates created from CSRs and issued by the Enterprise CA can be installed. This method is a more secure way (and preferred way) of installing a certificate. First, we need to create a CSR on Jetdirect.

Click on the "Networking" tab and go to "Authorization" and then "Certificates". Click "Configure" under the Jetdirect Certificate section.



Authorization

Certificates are used to identify devices on the network.

Jetdirect Certificate

By default, a pre-installed self-signed Jetdirect certificate is created to identify Jetdirect. You can change this certificate to more accurately identify the device and to update the length of time the certificate is valid.

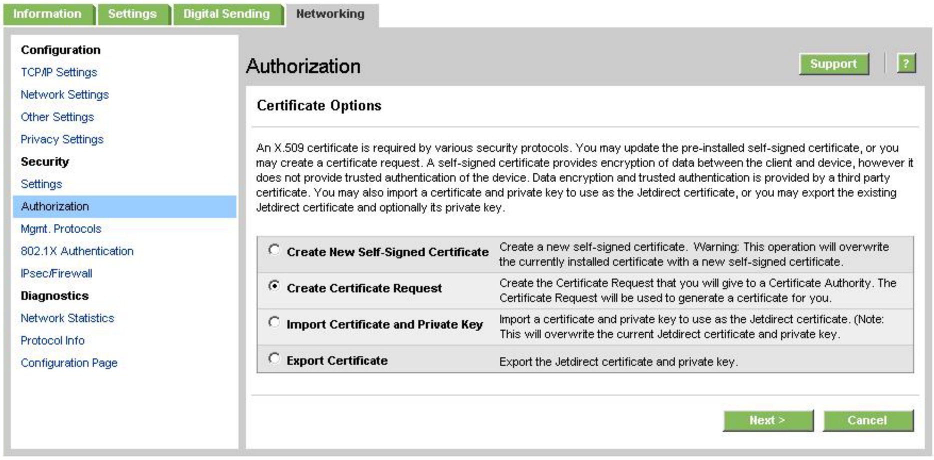
Status: Installed

CA Certificate

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

Status: Installed

Select "Create Certificate Request" and then click "Next".



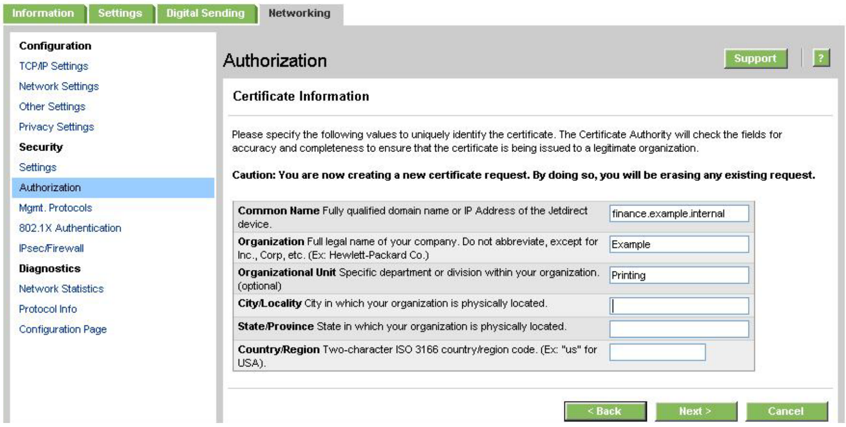
Authorization

Certificate Options

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

○ **Create New Self-Signed Certificate**	Create a new self-signed certificate. Warning: This operation will overwrite the currently installed certificate with a new self-signed certificate.
● **Create Certificate Request**	Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.
○ **Import Certificate and Private Key**	Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key.
○ **Export Certificate**	Export the Jetdirect certificate and private key.

Enter in the fields that describe the devices. Click "Next".



Authorization

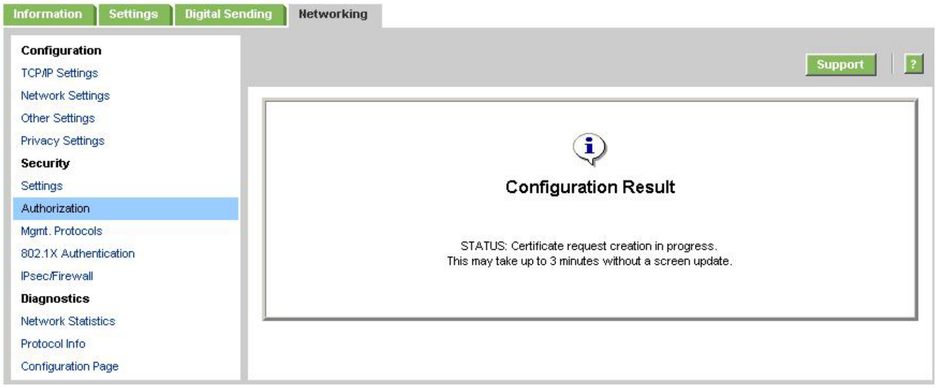
Certificate Information

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.	finance.example.internal
Organization Full legal name of your company. Do not abbreviate, except for Inc., Corp, etc. (Ex: Hewlett-Packard Co.)	Example
Organizational Unit Specific department or division within your organization. (optional)	Printing
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).	

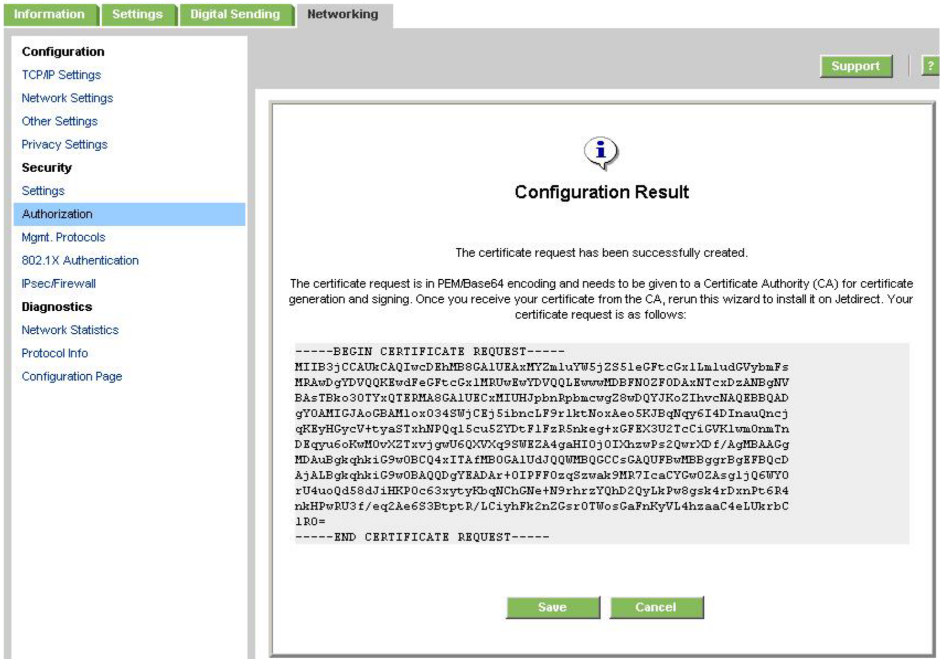
Jetdirect generates the public/private key pair, which can take a little while.



Configuration Result

STATUS: Certificate request creation in progress.
This may take up to 3 minutes without a screen update.

You can save the file, or you can simply copy the text starting and including "-----BEGIN CERTIFICAT REQUEST-----" up to and including the last five dashes of the "END CERTIFICATE REQUEST-----"



Configuration Result

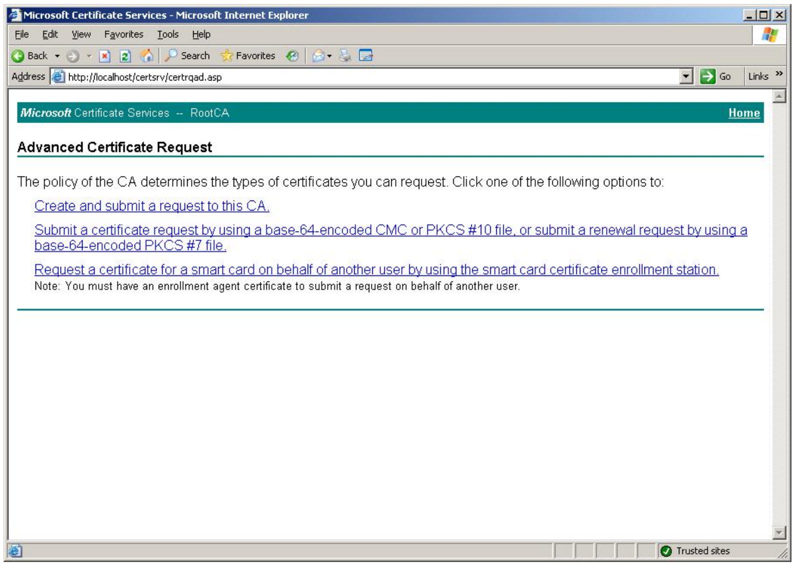
The certificate request has been successfully created.

The certificate request is in PEM/Base64 encoding and needs to be given to a Certificate Authority (CA) for certificate generation and signing. Once you receive your certificate from the CA, rerun this wizard to install it on Jetdirect. Your certificate request is as follows:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB3jCCAUkCAQIwcDEhMB8GA1UEAxMYZmluYW5jZS5leGFtcGxlLmludGVybmFs
MRAwDgYDVQQKEwdFeGFtcGxlMRUwEwYDVQQLEwwwMDBFN0ZFODAxNTcxDzANBgNV
BAsTBko3OTYxQTERMA8GA1UECxMIUHJpbnRpbmcwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMlox034SWjCEj5ibncLF9rlktNoxAeo5KJBqNqy6I4DInauQncj
qKEyHGycV+tyaSTxhNPQql5cu5ZYDtFlFzR5nkeg+xGFEX3U2TcCiGVKlwm0nmTn
DEqyu6oKwM0vXZTxvjgwU6QXVXq9SWEZA4gaHI0j0IXhzwPs2QwrXDf/AgMBAAGg
MDAuBgkqhkiG9w0BCQ4xITAfMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
AjALBgkqhkiG9w0BAQQDgYEADAr+0IPFF0zqSzwak9MR7IcaCYGw0ZAsgljQ6WY0
rU4uoQd58dJiHKP0c63xytyKbqNChGNe+N9rhrzYQhD2QyLkPw8gsk4rDxnPt6R4
nkHPwRU3f/eq2Ae6S3BtptR/LCiyhFk2nZGsr0TWosGaFnKyVL4hzaaC4eLUkrbC
lR0=
-----END CERTIFICATE REQUEST-----
```

Save Cancel

Moving back to the web interface of the Enterprise CA. We have skipped a couple of screen shots and are at the Advanced Certificate Request. Instead of clicking "Create and submit a request to this CA" as we did when we were Importing a certificate, we are going to click the second link "Submit a certificate request…"


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/certsrv/certrqad.asp
Go Links
Trusted sites

Microsoft Certificate Services -- RootCA Home

Advanced Certificate Request

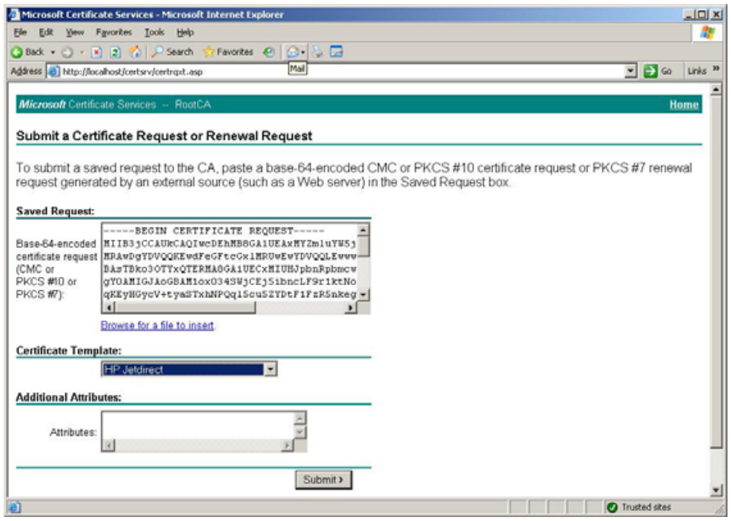
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Here we paste in our Certificate Request and select the HP Jetdirect certificate template. Then click "Submit".


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/certsrv/certrqxt.asp
Mail
Go Links
Trusted sites

Microsoft Certificate Services -- RootCA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB3jCCAUkCAQIwcDEhMB8GA1UEAxMYZmluYW5j
MRAwDgYDVQQKEwdFeGFtcGxlMRUwEwYDVQQLEwww
BAsTBko3OTYxQTERMA8GA1UECxMIUHJpbnRpbmcw
gYOAMIGJAoGBAM1ox034SWjCEj5ibncLF9r1ktNo
qKEyHGycV+tyaSTxhNPQq1ScuS2YDtF1FzR5nkeg
```

Browse for a file to insert.

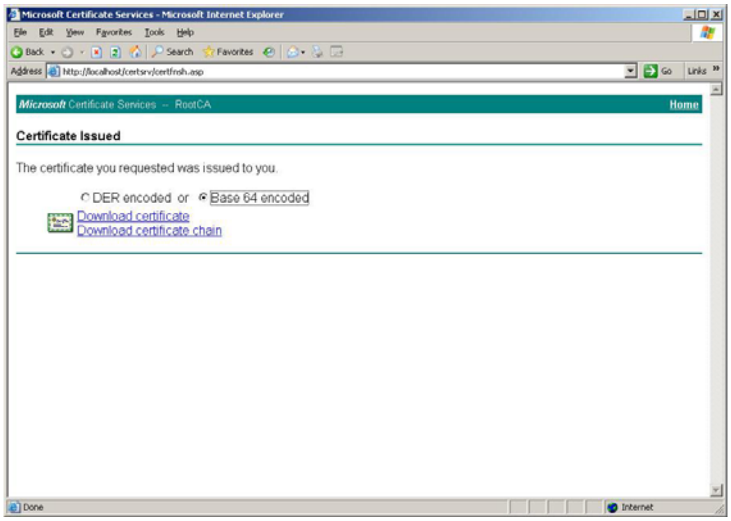
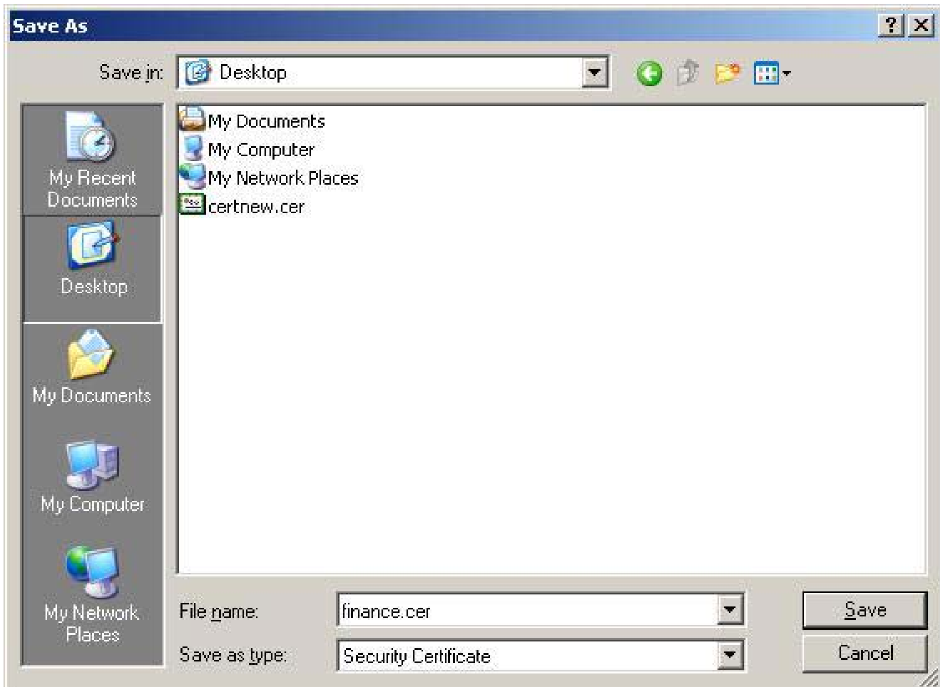
Certificate Template:

HP Jetdirect

Additional Attributes:

Attributes:

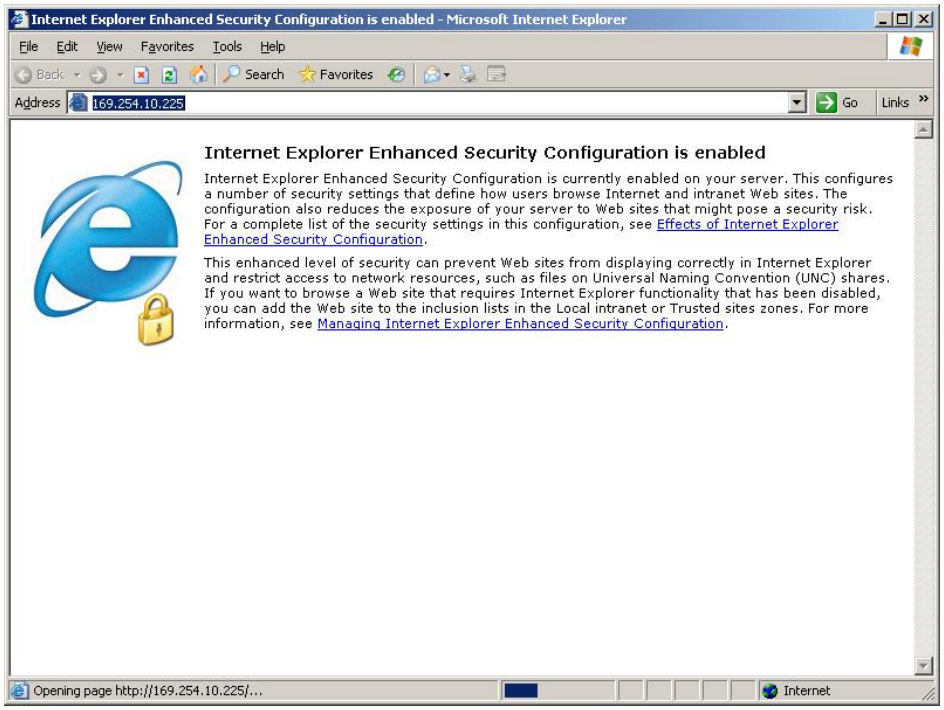
Submit >

Now we have our certificate. Most Jetdirect cards support both DER and Base64, but all support Base64. Simply click “Download Certificate”.	 Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Favorites Tools Help Address http://localhost/certsrv/certfnsh.asp Microsoft Certificate Services -- RootCA Home Certificate Issued The certificate you requested was issued to you. ○ DER encoded or ● Base 64 encoded Download certificate Download certificate chain Done Internet
Save the certificate.	 Save As Save in: Desktop My Recent Documents Desktop My Documents My Computer My Network Places My Documents My Computer My Network Places certnew.cer File name: finance.cer Save as type: Security Certificate Save Cancel

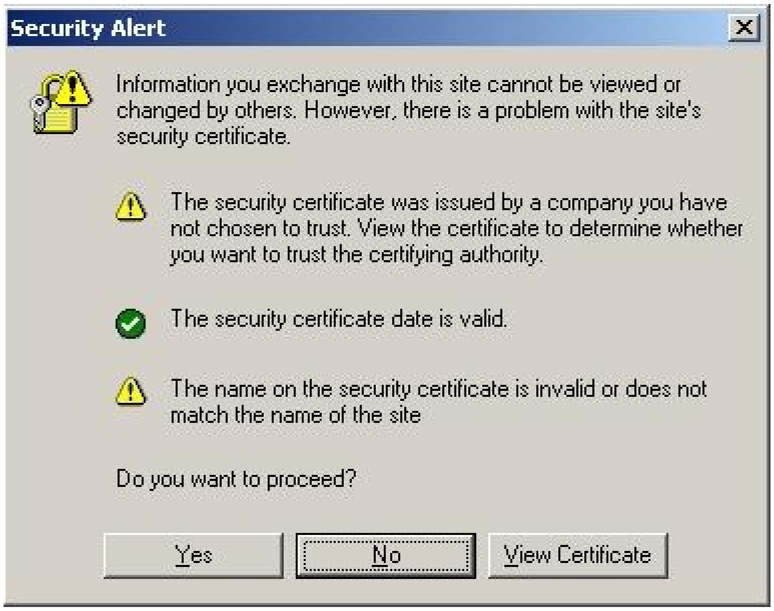
PKI: HP Jetdirect Certificate Configuration

Now we can discuss the HP Jetdirect configuration for certificates. First, we will install the HP Jetdirect Identity Certificate and the CA Certificate on the HP Jetdirect device. The HP Jetdirect certificates are used by SSL, IPsec, as well as 802.1X EAP authentication. Because multiple authentication methods use these certificates, we created the certificates using the certificate template to act as both a client and server.

In order to install HP Jetdirect Identity certificate and the CA certificate, we need to use the Embedded Web Server (EWS).

Point IE at the IP Address of the HP Jetdirect device.	 Internet Explorer Enhanced Security Configuration is enabled - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address 169.254.10.225 **Internet Explorer Enhanced Security Configuration is enabled** Internet Explorer Enhanced Security Configuration is currently enabled on your server. This configures a number of security settings that define how users browse Internet and intranet Web sites. The configuration also reduces the exposure of your server to Web sites that might pose a security risk. For a complete list of the security settings in this configuration, see Effects of Internet Explorer Enhanced Security Configuration. This enhanced level of security can prevent Web sites from displaying correctly in Internet Explorer and restrict access to network resources, such as files on Universal Naming Convention (UNC) shares. If you want to browse a Web site that requires Internet Explorer functionality that has been disabled, you can add the Web site to the inclusion lists in the Local intranet or Trusted sites zones. For more information, see Managing Internet Explorer Enhanced Security Configuration. Opening page http://169.254.10.225/...

With some HP Jetdirect print servers, the browser is automatically redirected to use SSL (https://) For other HP Jetdirect products, change the URL to use https:// rather than http:// to ensure that EWS communication is secure. The redirection to SSL requires the HP Jedirect print server to send its default certificate to Internet Explorer. Because each HP Jetdirect print server is shipped with a self-signed certificate, a security alert is issued because the browser cannot determine if the certificate is valid.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

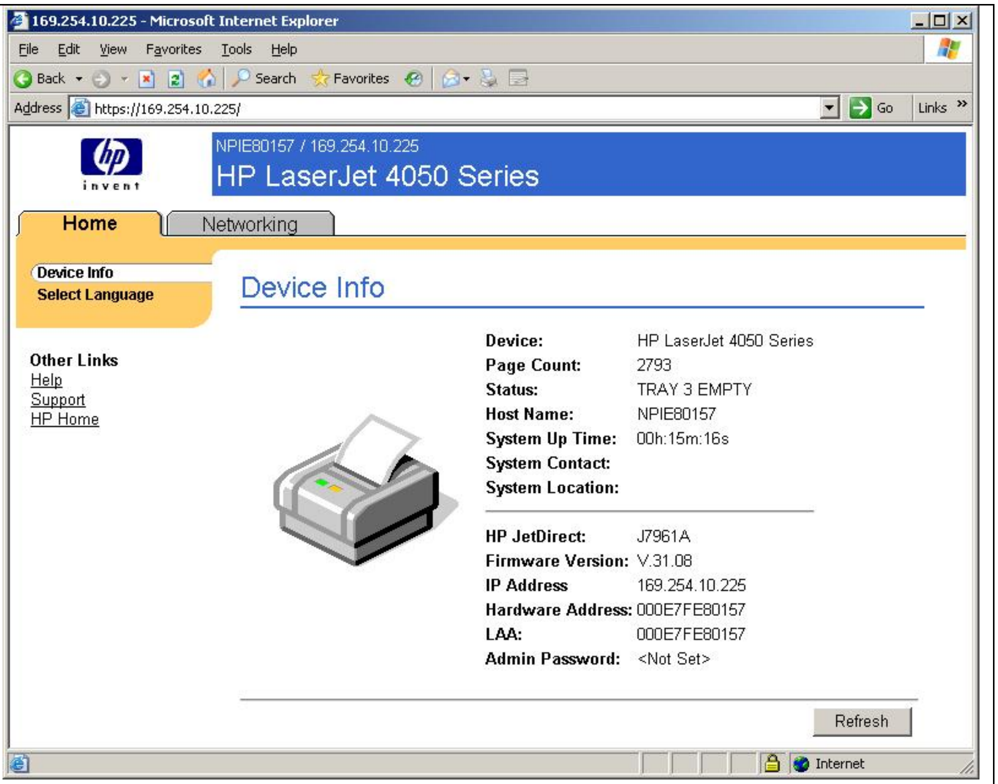
✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Click "Yes" to continue. Once we replace the Jetdirect certificate, the above dialog will change.

Here we have our home page of the HP Jetdirect device. Click the "Networking" Tab.



169.254.10.225 - Microsoft Internet Explorer

https://169.254.10.225/

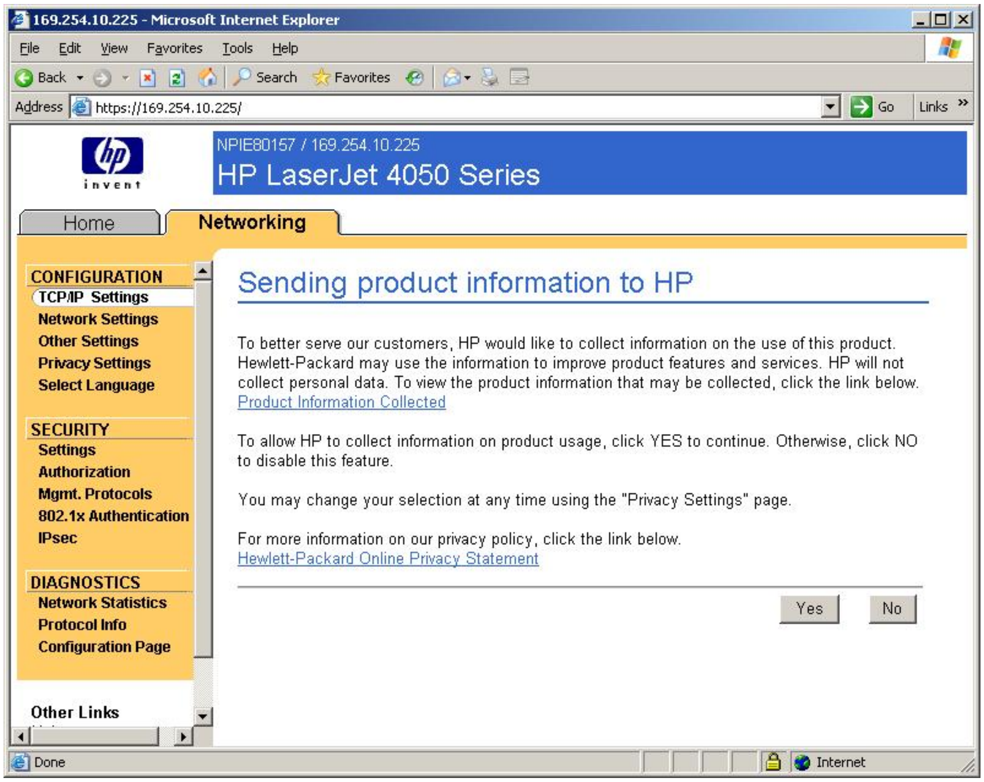
NPIE80157 / 169.254.10.225

HP LaserJet 4050 Series

Device Info

Device:	HP LaserJet 4050 Series
Page Count:	2793
Status:	TRAY 3 EMPTY
Host Name:	NPIE80157
System Up Time:	00h:15m:16s
System Contact:	
System Location:	
HP JetDirect:	J7961A
Firmware Version:	V.31.08
IP Address	169.254.10.225
Hardware Address:	000E7FE80157
LAA:	000E7FE80157
Admin Password:	<Not Set>

Depending on your HP Jetdirect model and firmware, you may see a screen similar to this one. It allows anonymous post sales information to be gathered about the HP Jetdirect configuration. This initiative is completely voluntary. Click Yes or No, depending on your preference.



Sending product information to HP

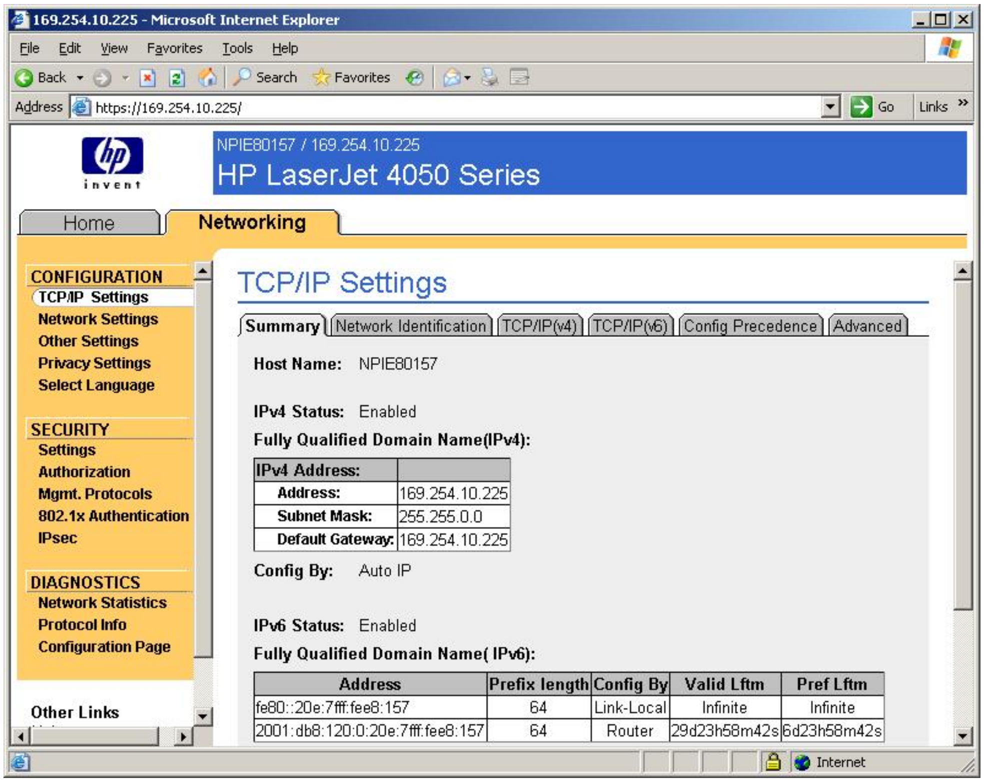
To better serve our customers, HP would like to collect information on the use of this product. Hewlett-Packard may use the information to improve product features and services. HP will not collect personal data. To view the product information that may be collected, click the link below.
Product Information Collected

To allow HP to collect information on product usage, click YES to continue. Otherwise, click NO to disable this feature.

You may change your selection at any time using the "Privacy Settings" page.

For more information on our privacy policy, click the link below.
Hewlett-Packard Online Privacy Statement

At this point, you'll be on the "TCP/IP Settings" link for Jetdirect. On the left hand navigation menu, select "Authorization".



TCP/IP Settings

Host Name: NPIE80157

IPv4 Status: Enabled

Fully Qualified Domain Name(IPv4):

IPv4 Address:	
Address:	169.254.10.225
Subnet Mask:	255.255.0.0
Default Gateway:	169.254.10.225

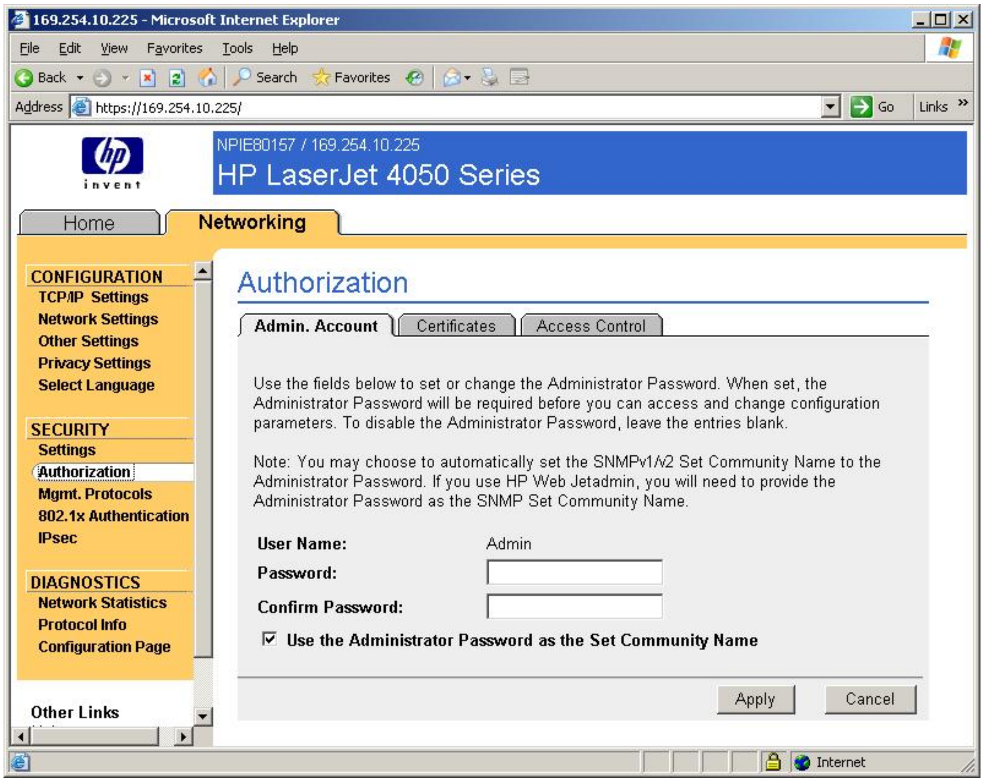
Config By: Auto IP

IPv6 Status: Enabled

Fully Qualified Domain Name(IPv6):

Address	Prefix length	Config By	Valid Lftm	Pref Lftm
fe80::20e:7fff:fee8:157	64	Link-Local	Infinite	Infinite
2001:db8:120:0:20e:7fff:fee8:157	64	Router	29d23h58m42s	6d23h58m42s

Click the "Certificates" tab.



169.254.10.225 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://169.254.10.225/

NPIE80157 / 169.254.10.225

HP LaserJet 4050 Series

Home | Networking

CONFIGURATION
- TCP/IP Settings
- Network Settings
- Other Settings
- Privacy Settings
- Select Language

SECURITY
- Settings
- Authorization
- Mgmt. Protocols
- 802.1x Authentication
- IPsec

DIAGNOSTICS
- Network Statistics
- Protocol Info
- Configuration Page

Other Links

Authorization

Admin. Account | Certificates | Access Control

Use the fields below to set or change the Administrator Password. When set, the Administrator Password will be required before you can access and change configuration parameters. To disable the Administrator Password, leave the entries blank.

Note: You may choose to automatically set the SNMPv1/v2 Set Community Name to the Administrator Password. If you use HP Web Jetadmin, you will need to provide the Administrator Password as the SNMP Set Community Name.

User Name: Admin

Password:

Confirm Password:

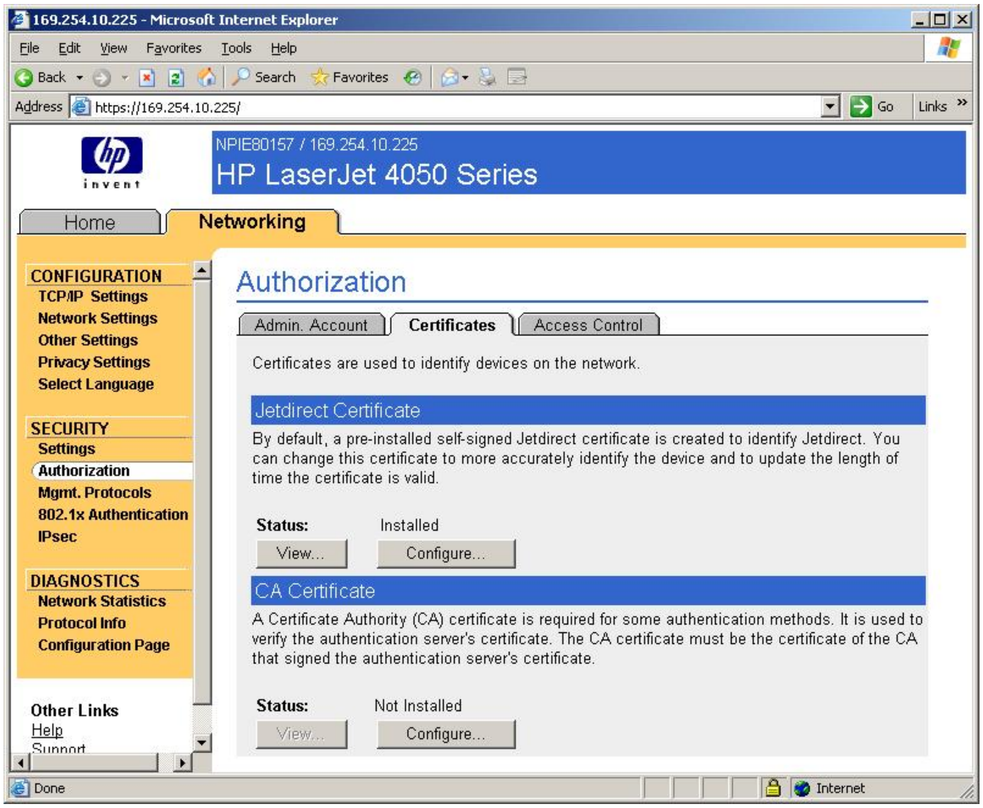
☑ Use the Administrator Password as the Set Community Name

Apply | Cancel

Internet

There are two certificates on HP Jetdirect. One is the HP Jetdirect certificate used for SSL, certain EAP protocols, IPsec, etc… The other is the Certificate Authority (CA) public key certificate which tells HP Jetdirect what CA it is supposed to trust. Certificates may be exchanged and HP Jetdirect needs to be able to verify the received certificate was signed by the trusted CA. We'll install the CA certificate first.

Click "Configure…" under the "CA Certificate" heading.



169.254.10.225 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://169.254.10.225/

NPIE80157 / 169.254.10.225

HP LaserJet 4050 Series

Home | Networking

CONFIGURATION
- TCP/IP Settings
- Network Settings
- Other Settings
- Privacy Settings
- Select Language

SECURITY
- Settings
- Authorization
- Mgmt. Protocols
- 802.1x Authentication
- IPsec

DIAGNOSTICS
- Network Statistics
- Protocol Info
- Configuration Page

Other Links
- Help
- Support

Authorization

Admin. Account | 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 Jetdirect. You can change this certificate to more accurately identify the device and to update the length of time the certificate is valid.

Status: Installed

View… | Configure…

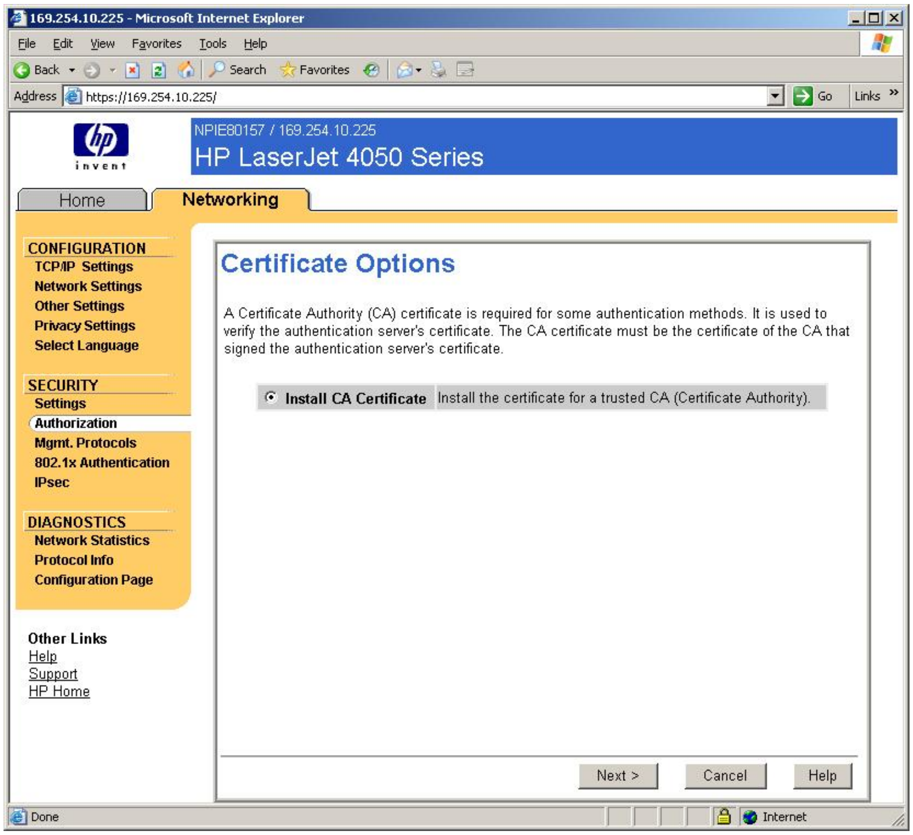
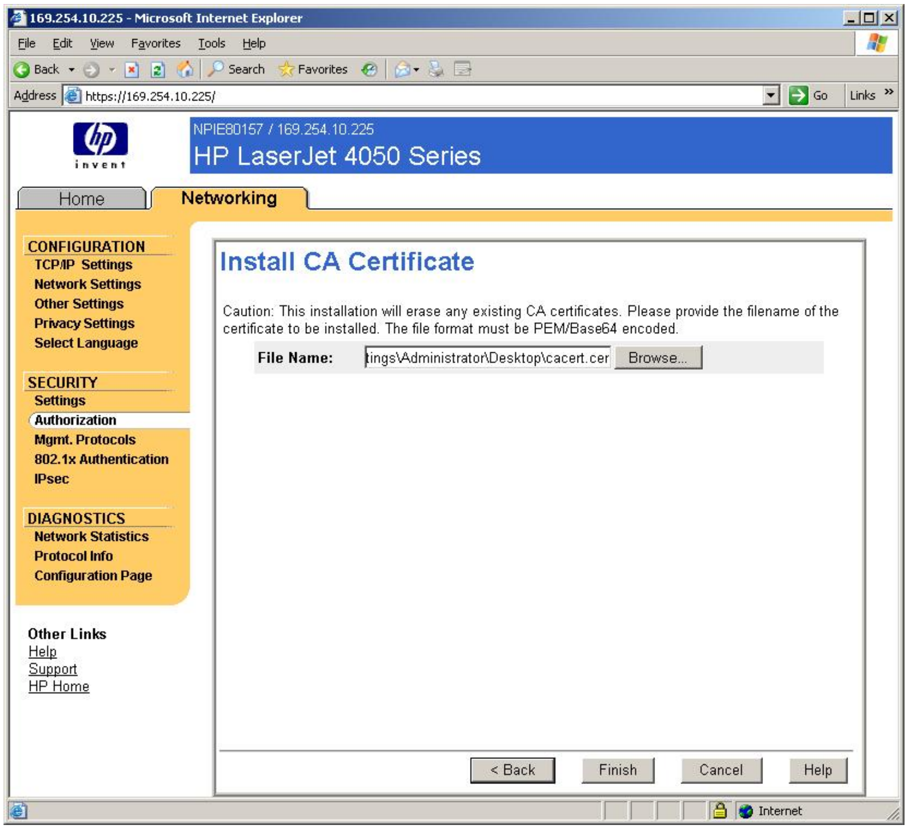
CA Certificate

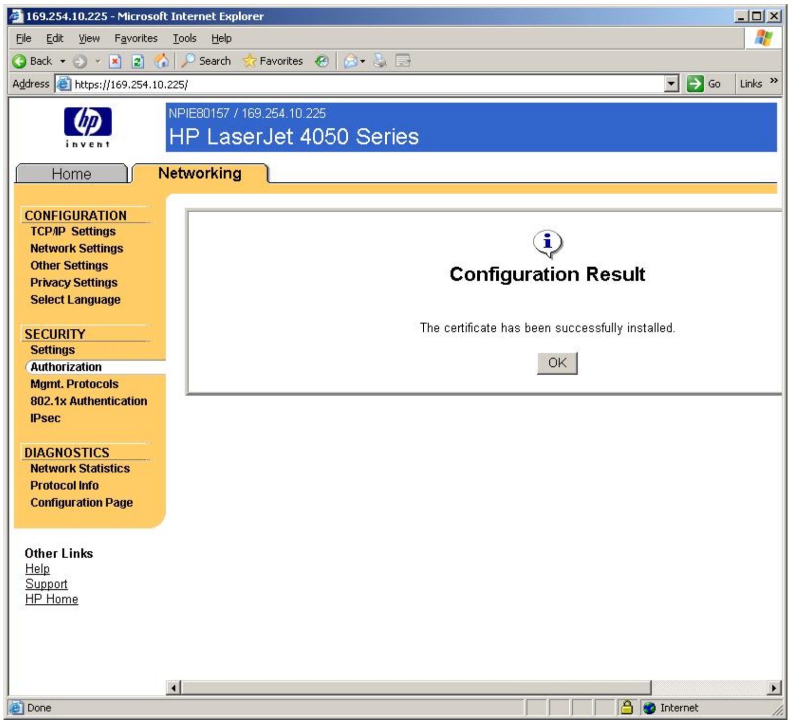
A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate.

Status: Not Installed

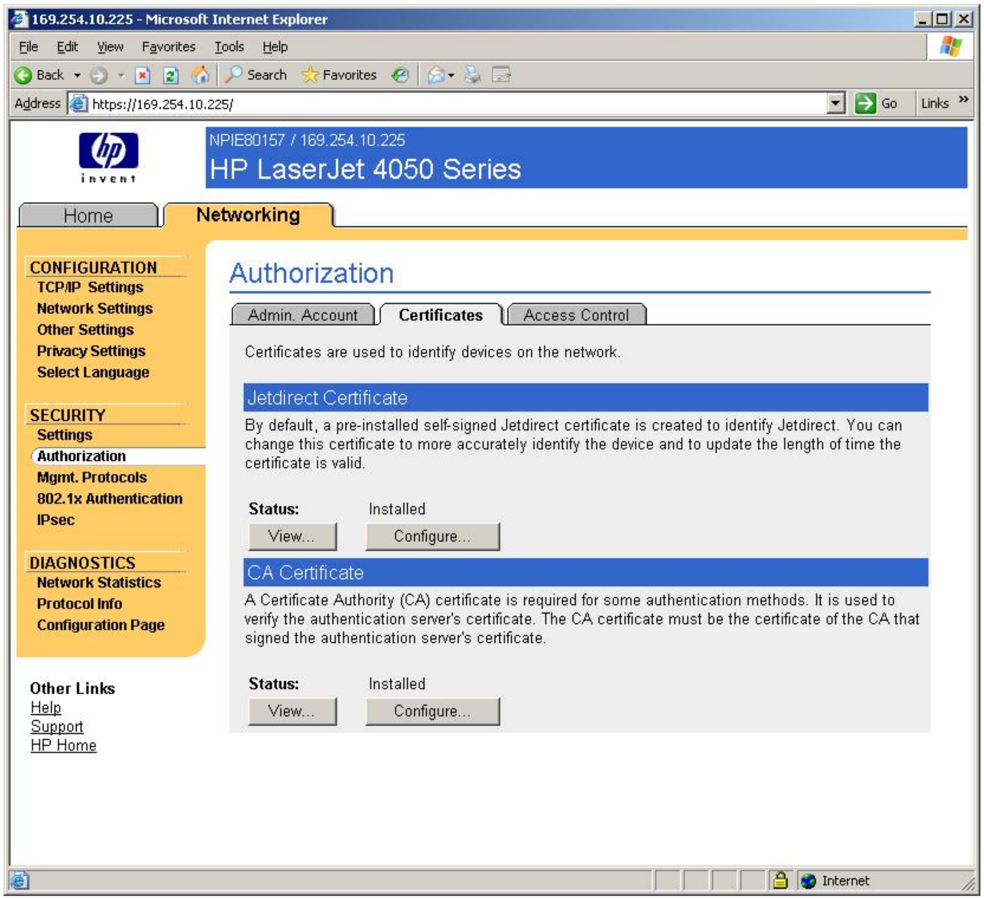
View… | Configure…

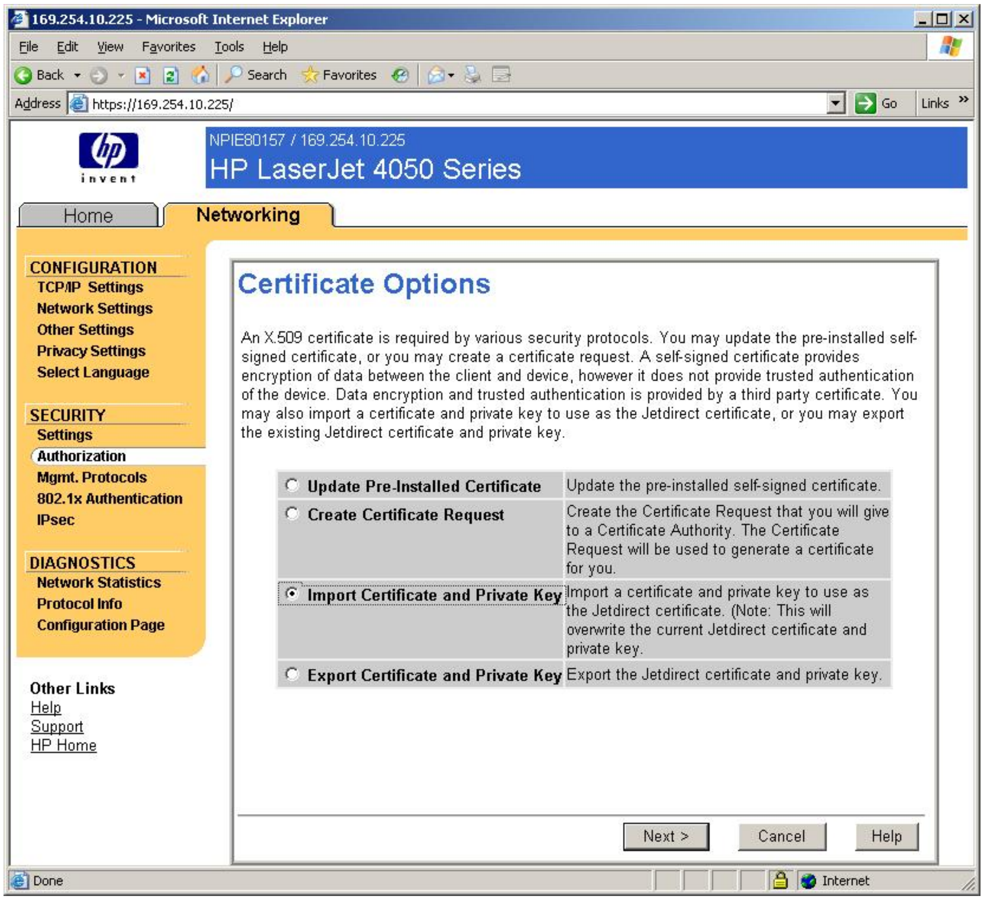
Done | Internet

Install is our only option. Click "Next".	 Address: https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series **Certificate Options** A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate. ● **Install CA Certificate** Install the certificate for a trusted CA (Certificate Authority). 169.254.10.225 - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Go Links invent Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home Next > Cancel Help Done Internet
Point the web browser to the "cacert.cer" file that was created earlier. Click "Finish".	 Address: https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series **Install CA Certificate** Caution: This installation will erase any existing CA certificates. Please provide the filename of the certificate to be installed. The file format must be PEM/Base64 encoded. **File Name:** tings\Administrator\Desktop\cacert.cer 169.254.10.225 - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Go Links invent Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home Browse... < Back Finish Cancel Help Internet

Done!	 169.254.10.225 - Microsoft Internet Explorer https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home OK Done Internet Configuration Result The certificate has been successfully installed.

If you did not use the certificate request method of generating a certificate, we'll want to "Import the Certificate and Private Key" into Jetdirect.

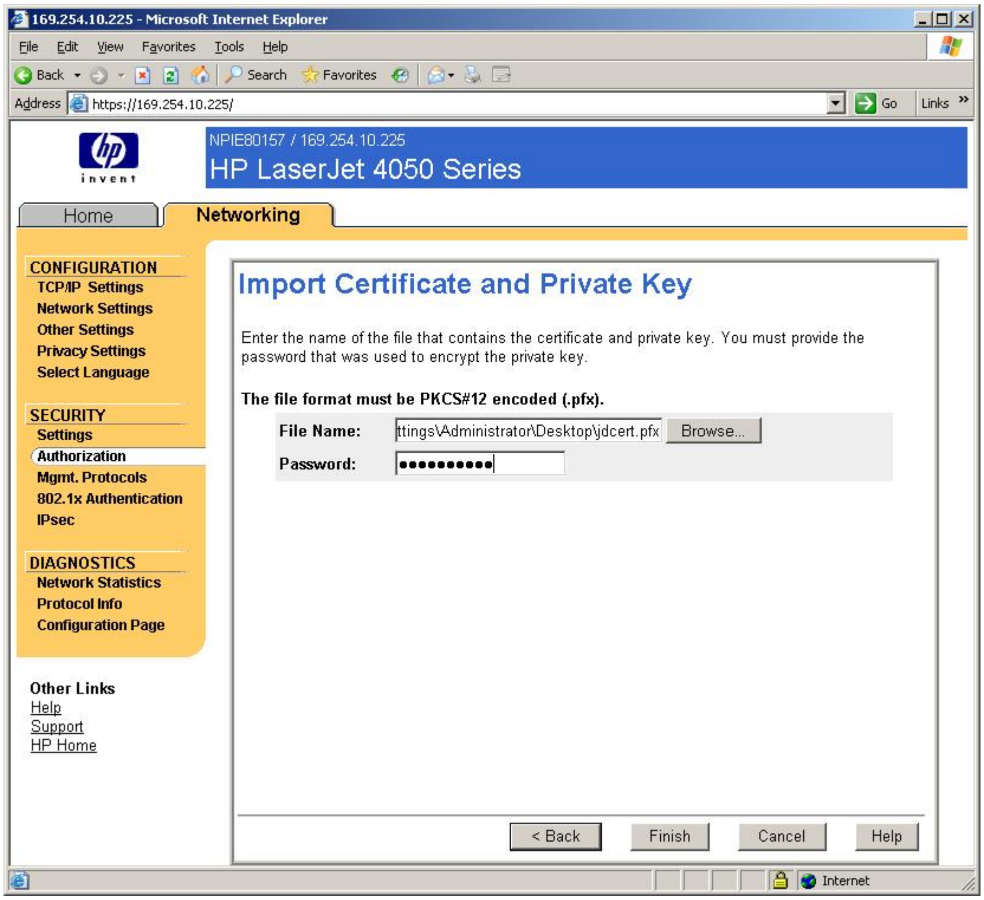
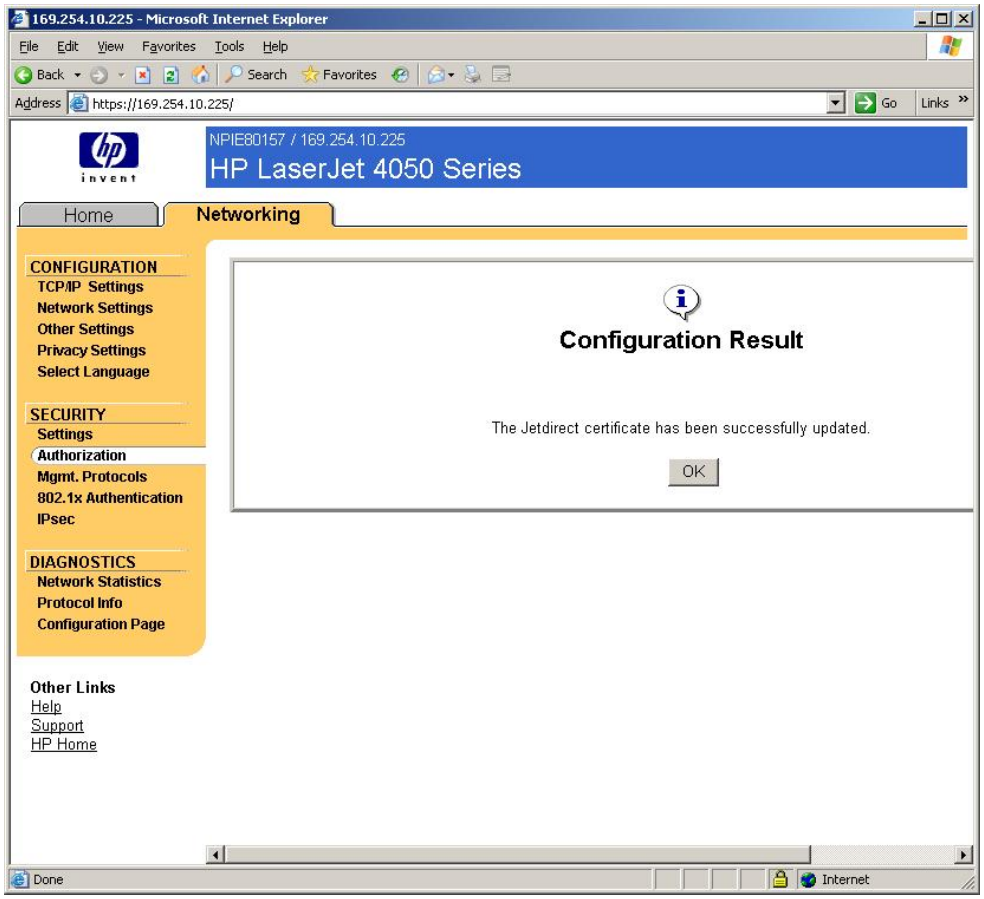
Now we'll import the Jetdirect Certificate – click "Configure..." under the "Jetdirect Certificate" heading.	 169.254.10.225 - Microsoft Internet Explorer https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home Admin. Account Certificates Access Control View... Configure... Internet Authorization Certificates are used to identify devices on the network. Jetdirect Certificate By default, a pre-installed self-signed Jetdirect certificate is created to identify Jetdirect. You can change this certificate to more accurately identify the device and to update the length of time the certificate is valid. Status: Installed CA Certificate A Certificate Authority (CA) certificate is required for some authentication methods. It is used to verify the authentication server's certificate. The CA certificate must be the certificate of the CA that signed the authentication server's certificate. Status: Installed

Select “Import Certificate and Private Key”. Click “Next”.	

Certificate Options

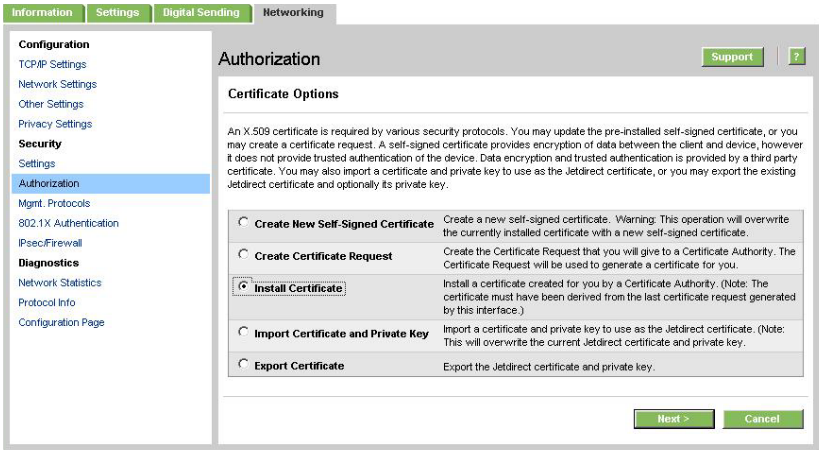
An X.509 certificate is required by various security protocols. You may update the pre-installed self-signed certificate, or you may create a certificate request. A self-signed certificate provides encryption of data between the client and device, however it does not provide trusted authentication of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

○ Update Pre-Installed Certificate	Update the pre-installed self-signed certificate.
○ Create Certificate Request	Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.
● Import Certificate and Private Key	Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key.
○ Export Certificate and Private Key	Export the Jetdirect certificate and private key.

Select the "jdcert.pfx" file that contains the private key of Jetdirect and the password that was used to protect the private key. Click "Finish".	 169.254.10.225 - Microsoft Internet Explorer https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home Browse... < Back Finish Cancel Help **Import Certificate and Private Key** Enter the name of the file that contains the certificate and private key. You must provide the password that was used to encrypt the private key. **The file format must be PKCS#12 encoded (.pfx).** **File Name:** ttings\Administrator\Desktop\jdcert.pfx **Password:** ••••••••••
Done!	 169.254.10.225 - Microsoft Internet Explorer https://169.254.10.225/ NPIE80157 / 169.254.10.225 HP LaserJet 4050 Series Home Networking CONFIGURATION TCP/IP Settings Network Settings Other Settings Privacy Settings Select Language SECURITY Settings Authorization Mgmt. Protocols 802.1x Authentication IPsec DIAGNOSTICS Network Statistics Protocol Info Configuration Page Other Links Help Support HP Home OK Done **Configuration Result** The Jetdirect certificate has been successfully updated.

If you used the certificate request method of generating a certificate, we'll want to select "Install Certificate" instead of "Import Certificate and Private Key".

Going back to the Jetdirect Certificate Wizard, we select the "Install Certificate" option. Click "Next".



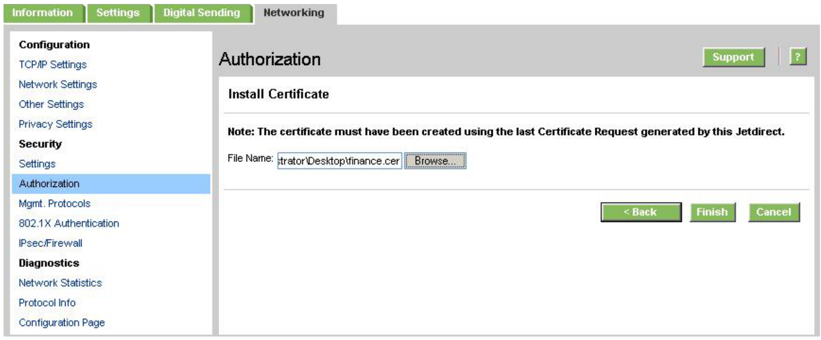
Authorization

Certificate Options

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

○ Create New Self-Signed Certificate	Create a new self-signed certificate. Warning: This operation will overwrite the currently installed certificate with a new self-signed certificate.
○ Create Certificate Request	Create the Certificate Request that you will give to a Certificate Authority. The Certificate Request will be used to generate a certificate for you.
● Install Certificate	Install a certificate created for you by a Certificate Authority. (Note: The certificate must have been derived from the last certificate request generated by this interface.)
○ Import Certificate and Private Key	Import a certificate and private key to use as the Jetdirect certificate. (Note: This will overwrite the current Jetdirect certificate and private key.
○ Export Certificate	Export the Jetdirect certificate and private key.

Select the certificate file saved previously. Click "Finish"



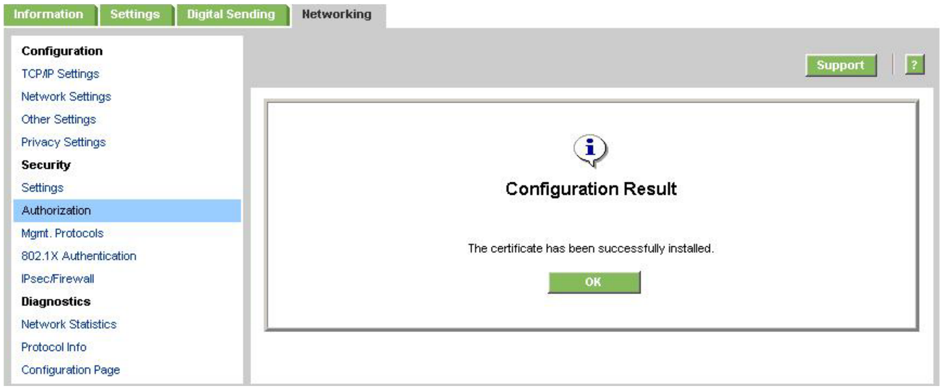
Authorization

Install Certificate

Note: The certificate must have been created using the last Certificate Request generated by this Jetdirect.

File Name: :trator\Desktop\finance.cer

We are done!



Configuration Result

The certificate has been successfully installed.

Now we have the files that represent Jetdirect's identity certificate and the public key certificate of the CA we trust. We can now look to the networking infrastructure to help control access to the network.

Step 3: 802.1X and VLANs

IEEE 802.1X Port Access Control is a generic framework that allows infrastructure devices to control an end-node's access to the network. From an Ethernet perspective, we can refer to Figure 13 – 802.1X Switch Port, and see the breakdown of the Ethernet switch.

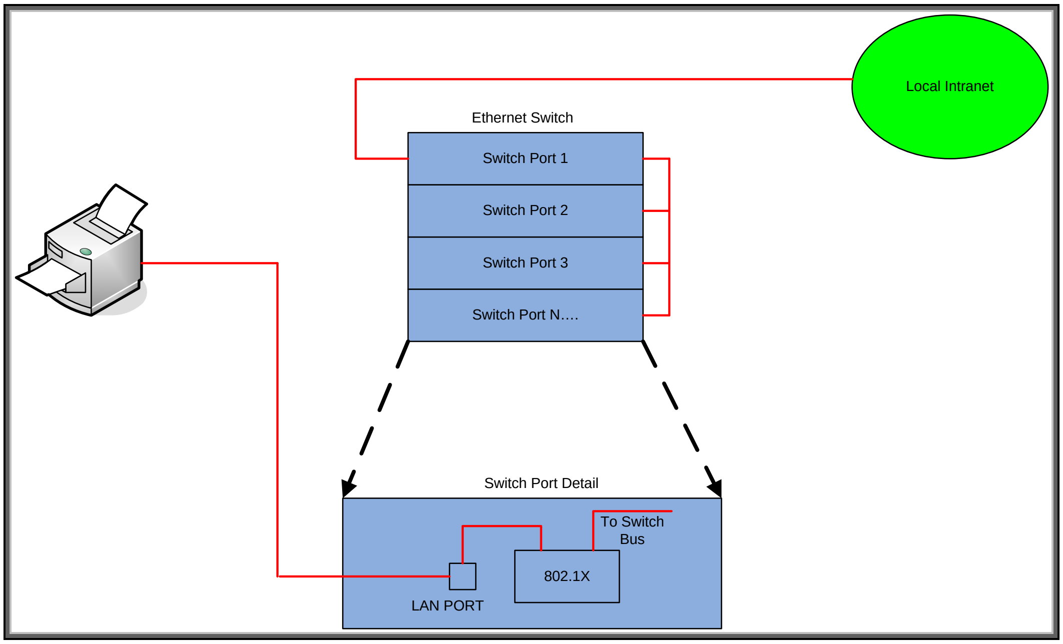


Figure 13 - 802.1X Switch Port

The end-node device must authenticate itself to the network before the local switch will grant it access to the network. The end-node device has a valid link to the switch, but the only frames the switch will forward from the end-node to the network are 802.1X Extensible Authentication Protocol (EAP) frames. The technical terminology for the devices involved is shown in Figure 14 – 802.1X Terms.

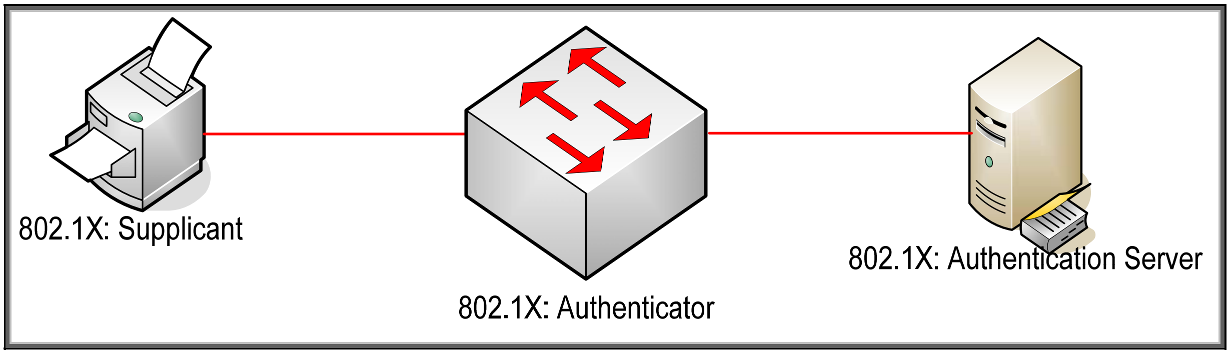


Figure 14 - 802.1X Terms

In reality, the authenticator (switch) forwards 802.1X EAP frames from the Supplicant to an Authentication Server. Based upon the configuration in the Authentication Server and the information supplied by the Supplicant, the Supplicant is authenticated (or not). The result of this authentication determines whether the switch port is "opened up" to the network for the Supplicant to send/receive non-EAP frames for normal network operation. With HP ProCurve switches, the Authentication Server can return much more information, such as the VLAN the Supplicant should be assigned, bandwidth restrictions on the Supplicant, etc., and the switch dynamically configures itself to support those parameters.

Because Extensible is part of the name of EAP, there are multiple protocols that have been developed under the EAP framework. All HP Jetdirect products supporting 802.1X also support Protected EAP or PEAP. Many HP Jetdirect products also support EAP-Transport Layer Security or EAP-TLS. These two EAP flavors are the most popular for wired 802.1X deployments. Both protocols utilize SSL/TLS running under EAP to authenticate the Authentication Server which sets up a secure tunnel. When shopping on the Internet, SSL/TLS is often used to protect the transaction over the network and to establish trust that the web site being contacted is really that web site and not an imposter's web site.

A cornerstone of SSL/TLS is the digital certificate. For PEAP and EAP-TLS, the Authentication Server sends over a digital certificate which the supplicant will attempt to validate. After a series of checks are performed, the supplicant will need to establish that the digital certificate was created by a trusted authority. If it passes that test, an SSL/TLS tunnel can be established. At this point, PEAP and EAP-TLS diverge. PEAP uses the tunnel to securely pass credentials via another protocol, typically a username and password, to the Authentication Server while EAP-TLS uses a client digital certificate for authentication.

For an in-depth discussion of 802.1X configuration on HP Jetdirect, refer to the whitepaper "How to use 802.1X on HP Jetdirect Print Servers".

802.1X: Printing and Imaging Virtual LANs

Let's assume that all the printers for a given building were going to be installed in the same VLAN. Once the printer's identity has been established via 802.1X, it is placed in a VLAN with all the other building's networked printers or MFPs. VLANs are usually assigned their own IP subnet. Therefore, an HP Jetdirect can be pre-configured by the Printing and Imaging Device Administration group with Certificates and a complete IP configuration and then deployed anywhere in the building. Another surprising benefit to an intelligent networking infrastructure is the ability to assign end-nodes that do not have 802.1X configured to an "Open VLAN". This VLAN for instance would have its own IP subnet as well. The Printer Administrator group can run network discoveries and easily determine printers that are in use that are not under the Printer Administrator's control. Refer to Figure 15 – Multiple VLANs.

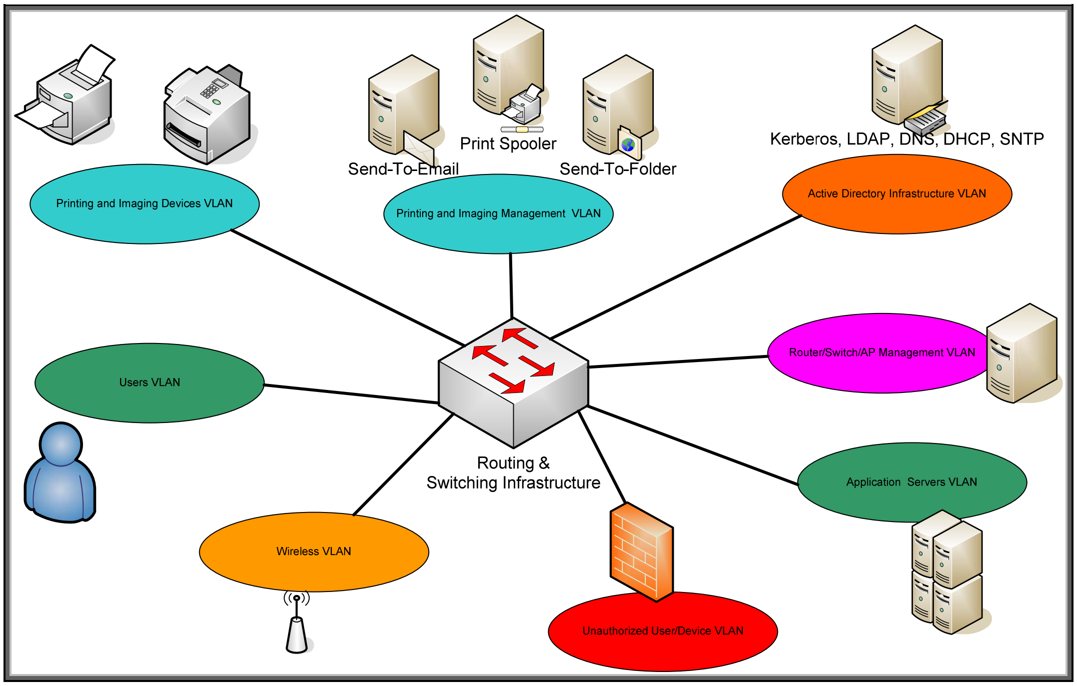

Send-To-Email
Print Spooler
Send-To-Folder
Kerberos, LDAP, DNS, DHCP, SNTP
Printing and Imaging Devices VLAN
Printing and Imaging Management VLAN
Active Directory Infrastructure VLAN
Router/Switch/AP Management VLAN
Users VLAN
Routing &
Switching Infrastructure
Application Servers VLAN
Wireless VLAN
Unauthorized User/Device VLAN

Figure 15 – Multiple VLANs

As an example for Building 10:

- PID VLAN IPv4 subnet for Building10: 10.0.0 /24
- PID VLAN IPv6 subnet for Building10: 2001:0DB8:0000::/64
- Printer Management VLAN IPv4 Subnet for Building 10: 10.0.255/24
- Printer Management VLAN IPv6 Subnet for Building 10: 2001:0DB8:00FF::/64
- Infrastructure Servers VLAN IPv4 172.16 /16
- Infrastructure Servers VLAN IPv6 2001:0DB8:FFFF::/64

NOTE: It is assumed that non IPv4 and non IPv6 protocols are disabled from a routing perspective.

The PID Administration (PIDA) team receives a LaserJet 4345mfp. The PIDA team allocates a static IP address of 10.0.0.25 and 2001:0DB8::25 and requests an Identity certificate with the DNS name of hppid.example.internal as well as the Root CA certificate from the IT Security team. The PIDA team indicates to the Network Infrastructure (NI) team that the VLAN assigned to this device is the PID VLAN and the PID should be placed in this VLAN on successful 802.1X authentication. The LaserJet 4345mfp and the MFP is sent to building 10. Once installed in Building 10, it automatically is put on the PID VLAN when 802.1X authentication is successful.

Because the PID VLAN represents a single point of failure, redundant power-supplies on switches and redundant or trunk interconnect lines are recommended for switches. In addition, standby routers to route between VLANs are also recommended. Finally, as an important security measure, it is recommended that Private VLANs be used. Private VLANs are a way to control which ports can communicate with other ports on the VLAN – in short, the printers on the PID VLAN should only be able to communicate with router ports and not other devices. This forces all printer traffic to go through the router(s).

An alternative design is to place the printers or MFPs in the same VLAN as the group that is using them. This prevents routers from always having to be involved for most printing. However, the advantages of using a PID VLAN will become clear in the next section.

Step 4: Switch Based IP Access Control Lists

A customer reading the previous section may be worried about having all printers on the same VLAN. This customer may be concerned that the printers Finance uses are on the same VLAN and subnet as the printers that Marketing uses. The worry is that an intruder that gains access to the Printer VLAN will have the ability to read just about anything being printed. This worry is justified.

Let us summarize what we have so far for the PID VLAN:

(1) Must pass 802.1X authentication to get on the PID VLAN
(2) If the switch supports Private VLAN, PIDs can only communicate with the Router(s)

One of the fundamental premises of Network Security is "defense-in-depth". We have done what we can to limit access to the Layer 2 functions in our network ((1) and (2) previously stated). Now we will begin looking at Layer 3 and how we can use the router and IPsec to further protect our printing devices.

It would be instructive to continue our Building 10 example. Here the Printer VLAN is 10.0.0 /24 and the Printer Management VLAN is 10.0.255 /24. Right away we can say that the only communication that should happen with a printer/MFP should happen with the Printer Management VLAN. Therefore, we can setup an access control list (ACL) on the VLAN routers as follows

```
access-list permit ipv4 10.0.0.0/24 10.0.255.0/24
access-list permit ipv6 2001:0DB8:000::/64 2001:0DB8:00FF::/64
```

These ACLs are placed on the interface that is part of the PID VLAN in the inbound direction (Router Point of View). Everything else will be dropped. We can also setup the corresponding ACL on the outbound path.

```
access-list permit ipv4 10.0.255.0/24 10.0.0.0/24
access-list permit ipv6 2001:0DB8:00FF::/64 2001:0DB8:000::/64
```

Essentially, only packets coming from the Printer Management VLAN going to the PID VLAN will be allowed. We also need to allow access to the Infrastructure Servers VLAN.

```
access-list permit ipv4 10.0.0.0/24 172.16 /16
access-list permit ipv6 2001:0DB8:000::/64 2001:0DB8:FFFF::/64
access-list permit ipv4 172.16 /16 10.0.0.0/24
access-list permit ipv6 2001:0DB8:FFFF::/642001:0DB8:000::/64
```

Using the Access Control capability of the Routers, we have effectively limited communication between the Printer Management VLAN, the PID VLAN, and the Infrastructure Servers VLAN. However, a knowledgeable attacker can spoof the Source IP address of packets and make them appear to come from the Printer Management VLAN. This is all that is necessary to create Denial of Service conditions. One way of combating source IP address spoofing is to do Ingress Filtering on router interfaces. Ingress filtering drops any packets where the Source IP address does not match the router's configuration. A further security step would be to limit the communication between the PID VLAN and the Infrastructure Servers VLAN to specific protocols – such as Kerberos, DNS, and LDAPS.

We also have another option – IP Security.

Step 5: IP Security (IPsec)

As a further step, we can protect all PIM VLAN and PID VLAN communication using IPsec. IPsec provides transparent security to applications. Because of some chicken-egg situations with the Infrastructure Servers VLAN, we will only protect the PIM VLAN and the PID VLAN with IPsec. We will restrict the PID VLAN and the Infrastructure VLAN protocols to only those necessary – such as Kerberos, LDAPS, and DNS.

IPsec configured in this way will prevent any other VLAN from establishing any communications with the PID VLAN, even if they were able to bypass the routers access control lists.

Example: Router(s) on PID VLAN. Inbound Access Control List.

(1)

Permit
Source IP 10.0.0 /24
Destination IP 10.0.255 /24
Protocol UDP
Port 500

Permit
Source IPv6 2001:0DB8:0000::/64
Destination IPv6 2001:0DB8:00FF::/64
Protocol UDP
Port 500

(2)

Permit
Source IP 10.0.0 /24
Destination IP 10.0.255 /24
Protocol ESP

Permit
Source IPv6 2001:0DB8:0000::/64
Destination IPv6 2001:0DB8:00FF::/64
Protocol ESP

Outbound Access Control List on PID VLAN Router(s)

(1)

Permit
Source IP 10.0.255 /24
Destination IP 10.0.0 /24
Protocol UDP
Port 500

Permit
Source IPv6 2001:0DB8:00FF::/64
Destination IPv6 2001:0DB8:0000::/64
Protocol UDP
Port 500

```
(2)
    Permit
    Source IP 10.0.255 /24
    Destination IP 10.0.0 /24
    Protocol ESP

    Permit
    Source IPv6 102001:0DB8:00FF::/64
    Destination IPv6 2001:0DB8:0000::/64
    Protocol ESP
```

This configuration allows the router(s) to drop packets that are not using ESP or are not part of an Internet Key Exchange (IKE) negotiation between the PID VLAN and the PIM VLAN (In HP Jetdirect's implementation, IKE uses UDP 500). In addition, no communication with the printer/MFP is possible without using IPsec configured for ESP.

These are just example access control lists on the routers and do not detail device or server IPsec configurations. For an in-depth discussion of IPsec configuration of end-nodes, refer to the whitepaper "Practical IPsec Deployment for Printing and Imaging Devices".

IPsec: Printer Management VLAN

The PIM VLAN contains all the devices and services that will interact with the PID VLAN directly. This includes Web Jetadmin, Windows Print Servers, Syslog Servers, Digital Sending Software, etc… It is highly recommended that the machines for user functions (e.g., printing, digital sending) be separate from the machines for Printer Administration. One of the most important servers on this PIM VLAN is an SMTP server. This SMTP server will be used exclusively for MFPs and will probably simply forward mail to the company's main email servers. However, by being separated, this email server can be heavily audited and restricted to what MFP users can do. For instance, email from MFPs to anywhere outside the company may be prohibited. Email from an MFP between 6pm and 6am may be prohibited. Email from an MFP on Saturday, or Sunday, or Holidays may be prohibited as well.

All of these machines need to have the ability to use IPsec when communicating with the Printer VLAN. By default, Windows machines have IPsec capability but it must be configured using the Microsoft Management Console. Also, these machines should be heavily locked down in terms of unneeded services and capabilities.

Based upon our current configuration, all users must print through a Windows Print Server. Each printer in the Printer VLAN will need a corresponding printer defined on the Windows Print Server. This printer would then be accessible via a share where access is controlled by groups defined in the Active Directory for instance. This allows a printer to be "public" or to be restricted to the Marketing Group or to whatever group the printer/MFP is assigned. IPsec policy on these machines can be very specific in that only traffic going to the PID VLAN is IPsec protected while other traffic is not IPsec protected. This means that print traffic destined to the PIM VLAN would be unprotected by IPsec.

Step 6: Device Security

This whitepaper is primarily focused on networking infrastructure and how to use it effectively to help secure HP PIDs. It is highly recommended that the "HP Jetdirect Security Guidelines" whitepaper be read in order to secure the HP PID itself.

Summary

This whitepaper has covered several general techniques for securing a customer's printing assets from attacks and misuse using HP Jetdirect and "Defense-in-Depth" techniques. A customer may not be able to deploy all the suggestions mentioned here, but the hope is to provide a reference point for additional security by leveraging the networking infrastructure.