Xerox Multifunction Devices

Customer Tips

dc06cc0390
August 4, 2006

… for the user

IPSec Client/Server Configuration Using Pre-Shared Keys in Windows Environments

Overview

A client can use an IPSec tunnel as one method of secure printing available to Xerox devices. The IPSec protocol uses strong cryptography to provide both authentication and encryption services. By using the service you create a secure tunnel to transfer data safely through un-trusted networks. In essence you are creating a VPN (virtual private network).

This document includes the following information:

- Configuration of the IPSec client/server in Windows 2000 with Service Pack 4, 2003 Server and XP environments
- A test of the client setup
- Configuration of IPSec on a Xerox device

This document applies to the Xerox products indicated in the table below. For some products, it is assumed that your device is equipped with the appropriate option to support this document.

x	**WC 7655/7665**
x	**WC Pro 232/238/245/ 255/265/275**
x	**WC 232/238/245/255/ 265/275**
	WC Pro C2128/C2636/ C3545
	WC Pro 165/175
	WC M165/M175
	WC Pro 32/40 Color
	WC Pro 65/75/90
	WC Pro 35/45/55
	WC M35/M45/M55
	DC 555/545/535
	DC 490/480/470/460
	DC 440/432/425/420

IPSec Terminology

This section is part of an article in Microsoft's Knowledge Base (Article 301284). It defines some of the terms you may encounter while setting up IPSec.

Authentication: The process to determine if the identity of a computer is legitimate. Windows 2000/XP IPSec supports three kinds of authentication: Kerberos, certificates, and preshared keys. Kerberos authentication can work only if both endpoints (computers) are in the same Windows 2000/XP domain. If the computers are in different domains, or at least one of them is not in a domain, you must use either certificates or preshared keys. Certificates can work only if each endpoint contains a certificate that is signed by an authority that the other endpoint trusts. Preshared keys have the same problems that passwords do: They do not remain secret for a very long period of time. If the endpoints are not in the same domain and you cannot obtain certificates, preshared keys are your only authentication option.

Encryption: The process of making data indistinct in preparation for transmission between two endpoints. By using well-tested algorithms, each endpoint constructs and exchanges cryptographic keys. The process ensures that only the endpoints know the keys; and if any key-exchange sequences are intercepted, the interceptor obtains nothing of value. Xerox devices support DES and 3DES encryption types.

Filter: A description of the Internet Protocol (IP) addresses and protocols that can trigger the establishment of an IPSec security association.

Filter action: The security requirements that are enabled when the traffic matches the filters in a filter list.

Filter list: A collection of filters.

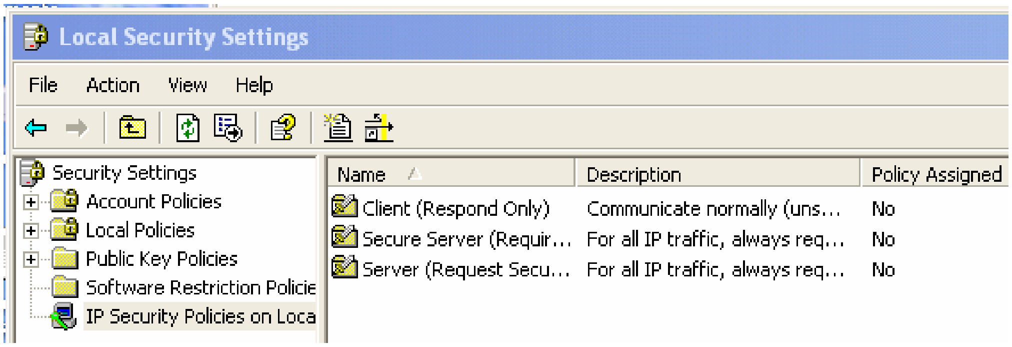
Internet Protocol security policy: The collection of rules that describe how communications between computers are secured.

Rule: The link between a filter list and a filter action. When the traffic matches a filter list, the corresponding filter action is triggered. An IPSec policy can contain multiple rules.

Security association: The collection of authentication and encryption methods that the endpoints negotiate to establish a secure session.

Local Security Policies

To access Local Security Policies, select **Start>Settings>Control Panel>Administrative Tools>Local Security Policy**. When displayed, select **IP security policies on Local Machine** (some selection titles vary with operating system version). The current default policies are displayed in the right pane.

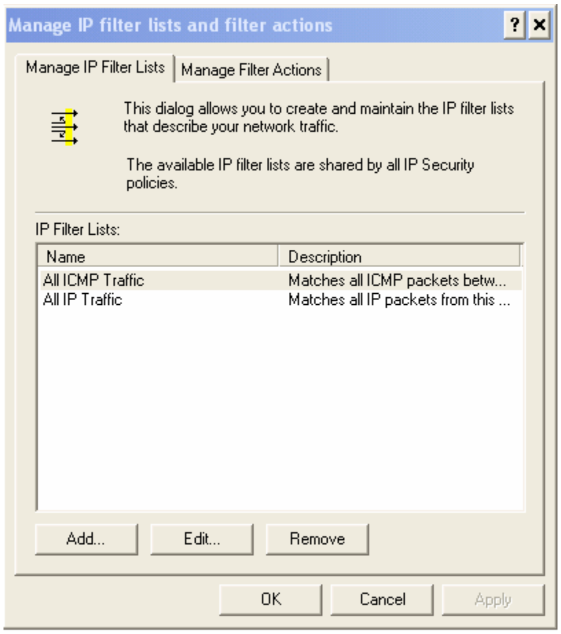


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No

To create a new policy and the rules that go with it, first define the filter lists and filter actions.

Adding a Filter List

1. Right-click on **IP security policies on Local Machine** and select **Manage IP filter lists and filter actions**. The window that appears contains two tabs, **Manage IP Filter Lists** and **Manage Filter Actions**.



This dialog allows you to create and maintain the IP filter lists that describe your network traffic.

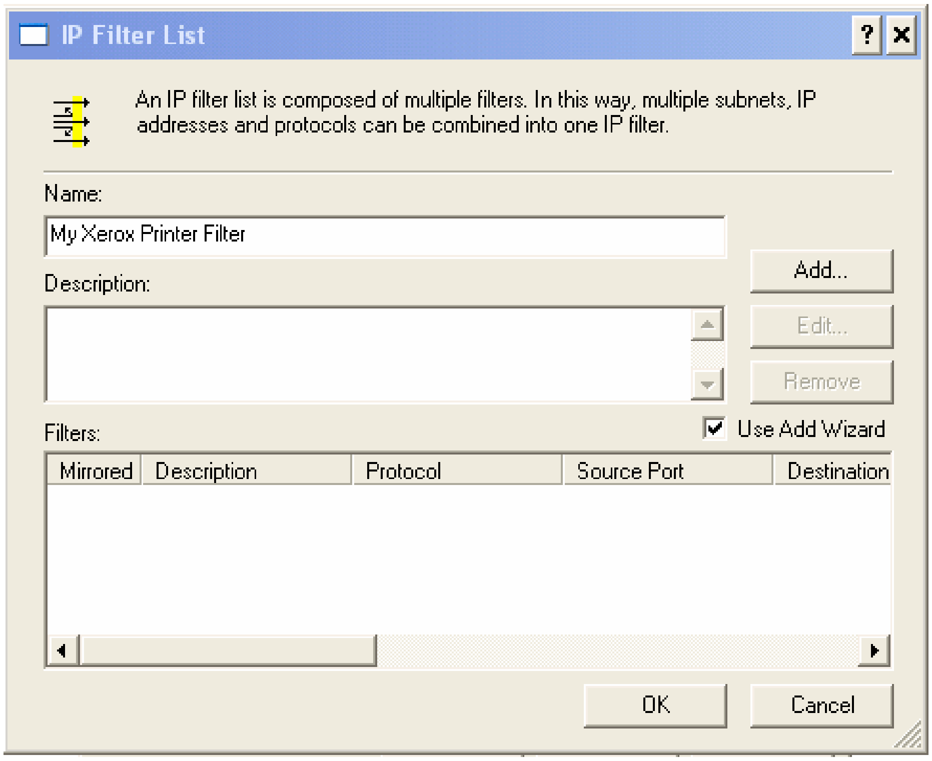
The available IP filter lists are shared by all IP Security policies.

IP Filter Lists:

Name	Description
All ICMP Traffic	Matches all ICMP packets betw...
All IP Traffic	Matches all IP packets from this ...

2. On the **Manage IP Filter Lists** tab click **Add**.

3. On **IP Filter List** enter a **Name** for the filter list, for example, **My Xerox Printer Filter**. Click **Add** again to start the IP Filter Wizard.



An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

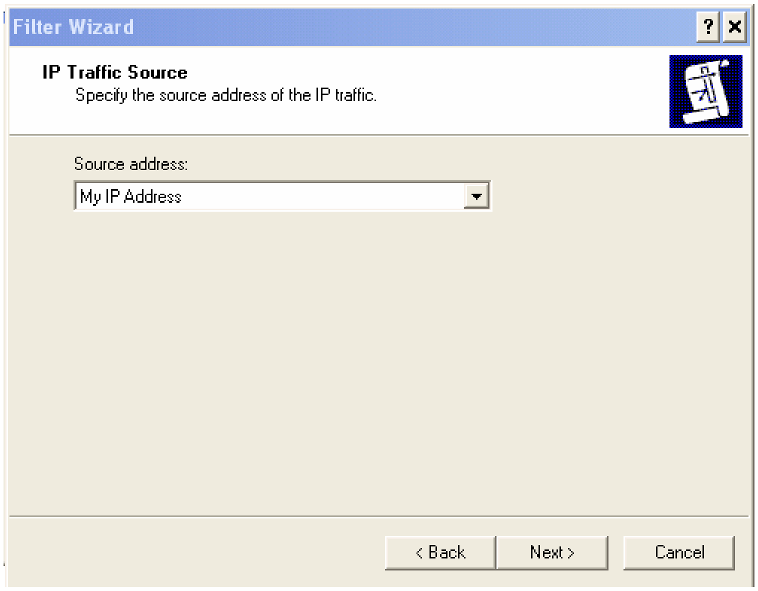
Name: My Xerox Printer Filter

Description:

Filters: ☑ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

4. Click **Next**. For the **Source Address** select **My IP Address**.



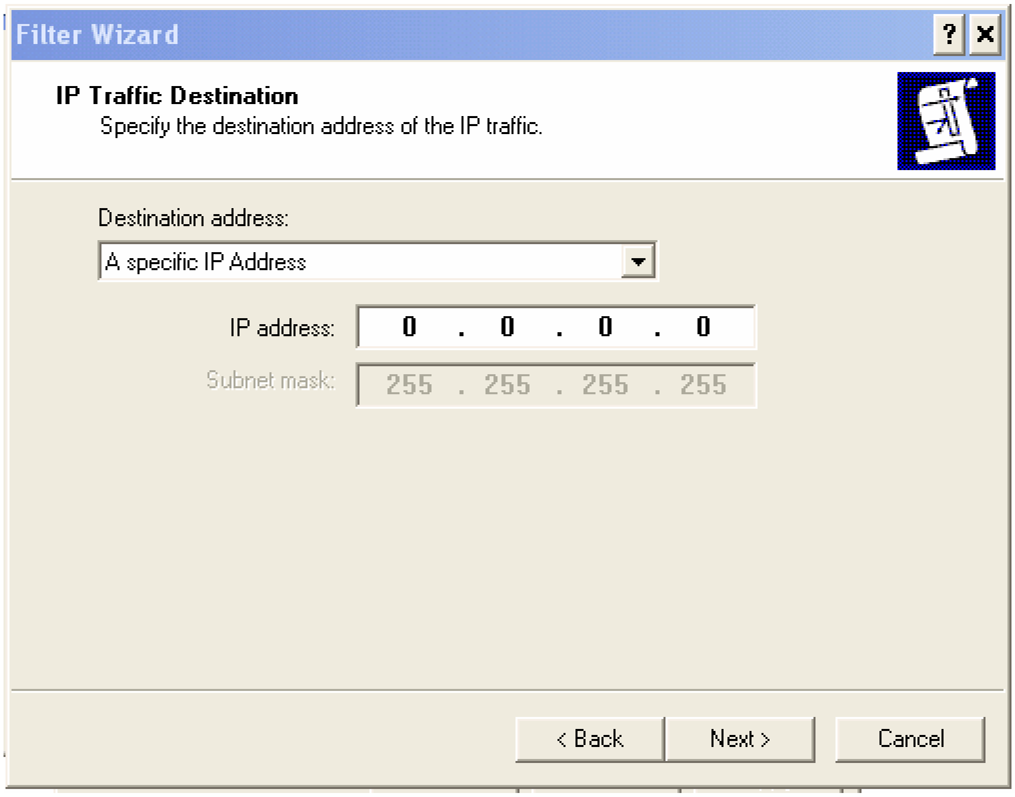
Filter Wizard

IP Traffic Source

Specify the source address of the IP traffic.

Source address: My IP Address

5. Click **Next**. For the **Destination Address** select **A specific IP Address** and enter in the IP address of the Xerox device.



Filter Wizard

IP Traffic Destination

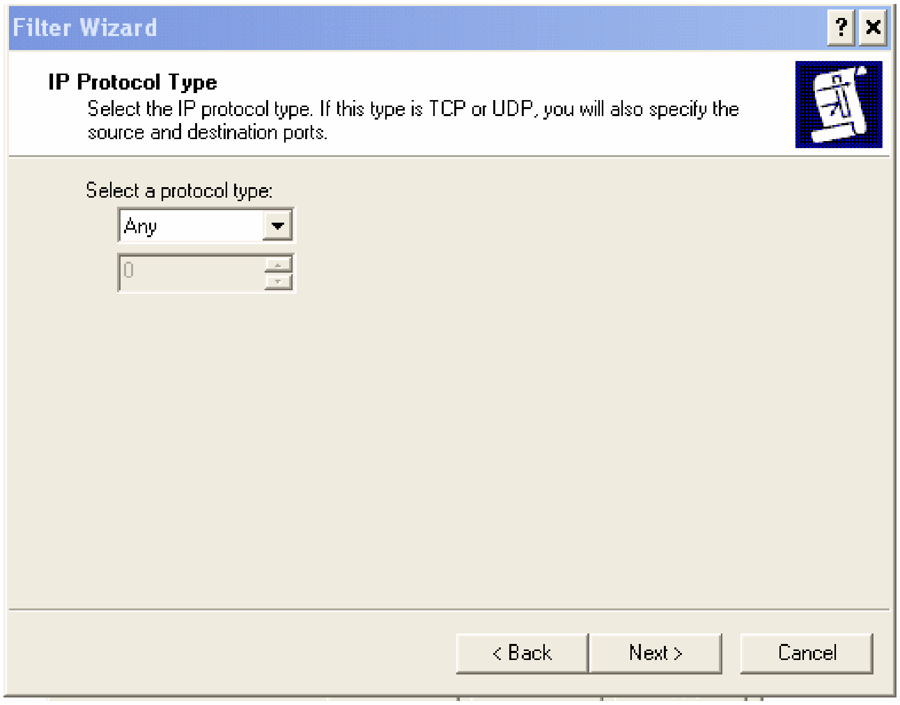
Specify the destination address of the IP traffic.

Destination address: A specific IP Address

IP address: 0 . 0 . 0 . 0

Subnet mask: 255 . 255 . 255 . 255

6. Click **Next**. For **Select a protocol type** select **Any**. This forces any protocol using TCP/IP to run over IPSec through the connection from the Source Address to the Destination Address.



Filter Wizard

IP Protocol Type

Select the IP protocol type. If this type is TCP or UDP, you will also specify the source and destination ports.

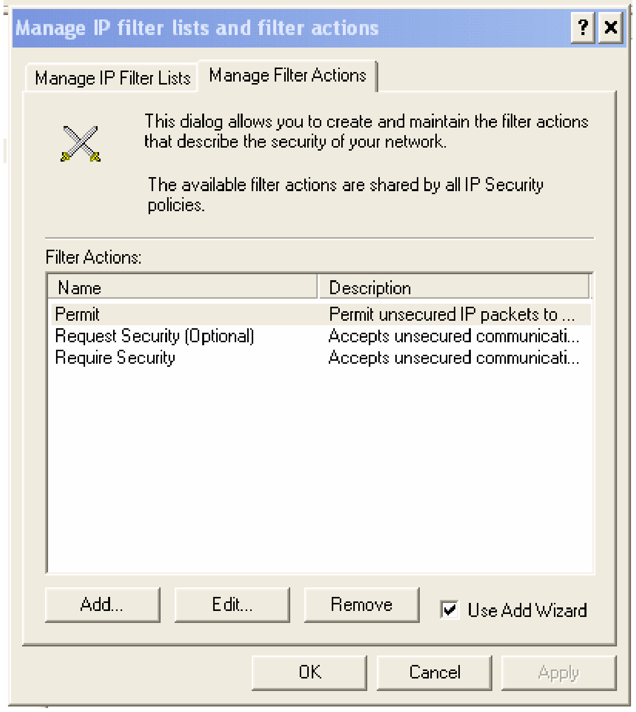
Select a protocol type: Any

0

7. Click **Next**. Click **Finish** then **OK**. The name of the filter list you created, for example, **My Xerox Printer Filter**, appears in the list of available IP filters on the **Manage IP filter lists and filter actions** window.

Adding a Filter Action

1. With the **Manage IP filter lists and filter actions** window displayed, select the **Manage Filter Actions** tab.



Manage IP filter lists and filter actions

This dialog allows you to create and maintain the filter actions that describe the security of your network.

The available filter actions are shared by all IP Security policies.

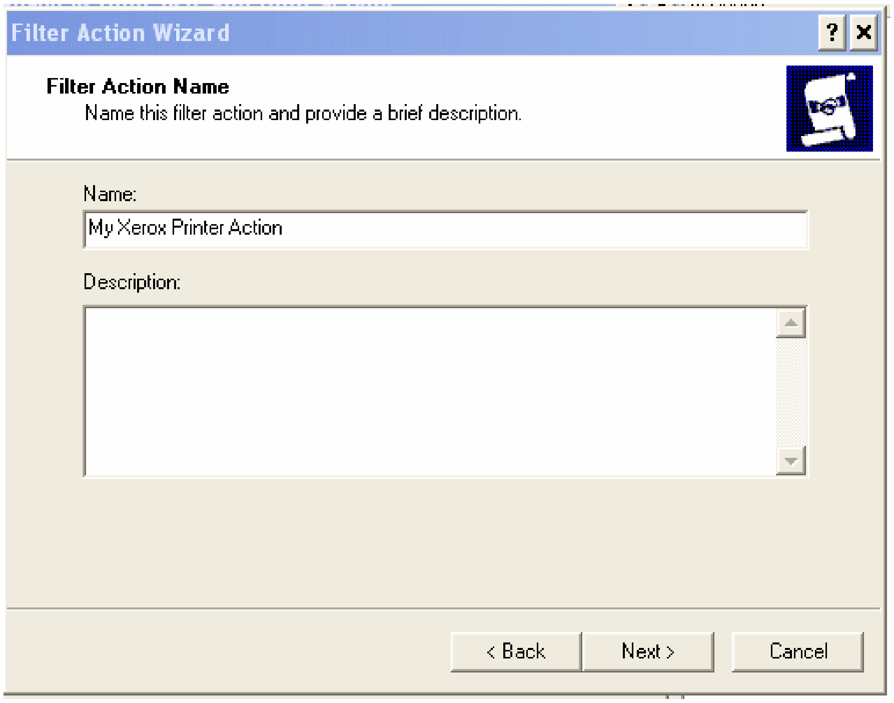
Filter Actions:

Name	Description
Permit	Permit unsecured IP packets to ...
Request Security (Optional)	Accepts unsecured communicati...
Require Security	Accepts unsecured communicati...

☑ Use Add Wizard

2. Click **Add** to start the Filter Action Wizard, then click **Next**.

3. Enter a name for the filter action, for example, **My Xerox Printer Action**, then click **Next**.



Filter Action Wizard

Filter Action Name

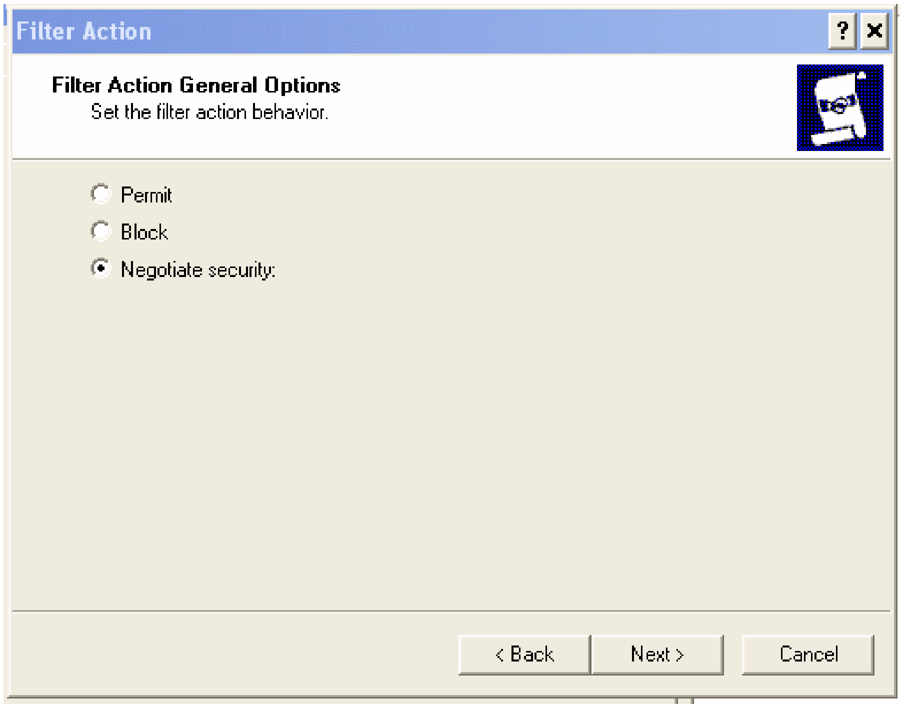
Name this filter action and provide a brief description.

Name:

My Xerox Printer Action

Description:

4. In General Options select **Negotiate Security**, then click **Next.**



Filter Action

Filter Action General Options

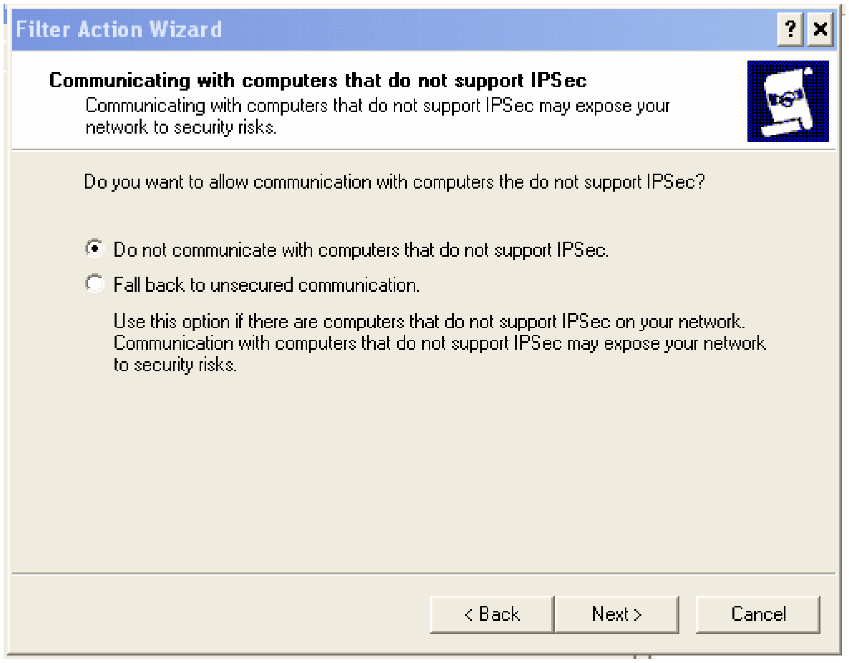
Set the filter action behavior.

○ Permit

○ Block

● Negotiate security:

5. Verify **Do not communicate with computers that do not support IPSec** is selected, then click **Next**.



Communicating with computers that do not support IPSec

Communicating with computers that do not support IPSec may expose your network to security risks.

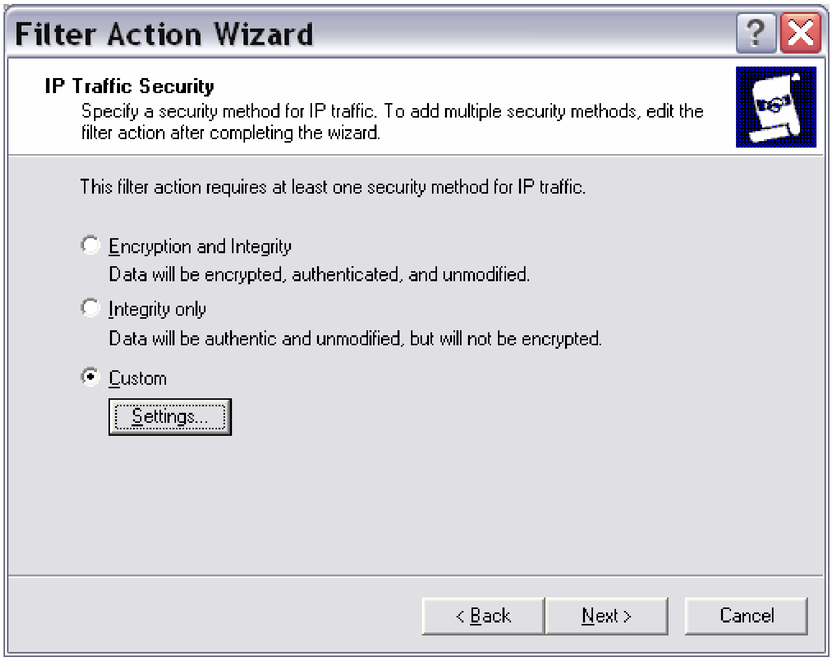
Do you want to allow communication with computers the do not support IPSec?

● Do not communicate with computers that do not support IPSec.

○ Fall back to unsecured communication.

Use this option if there are computers that do not support IPSec on your network. Communication with computers that do not support IPSec may expose your network to security risks.

6. For IP Traffic Security select **Custom**, then click **Settings**.



IP Traffic Security

Specify a security method for IP traffic. To add multiple security methods, edit the filter action after completing the wizard.

This filter action requires at least one security method for IP traffic.

○ Encryption and Integrity

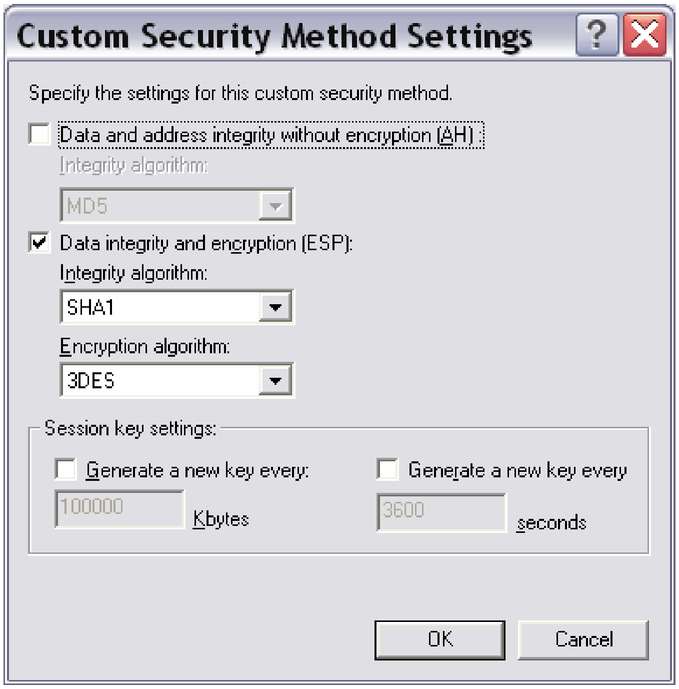
Data will be encrypted, authenticated, and unmodified.

○ Integrity only

Data will be authentic and unmodified, but will not be encrypted.

● Custom

7. In the **Encryption algorithm** field select **3DES**. Leave other settings/entries as they are.



Custom Security Method Settings

Specify the settings for this custom security method.

□ Data and address integrity without encryption (AH)

Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm: SHA1

Encryption algorithm: 3DES

Session key settings:

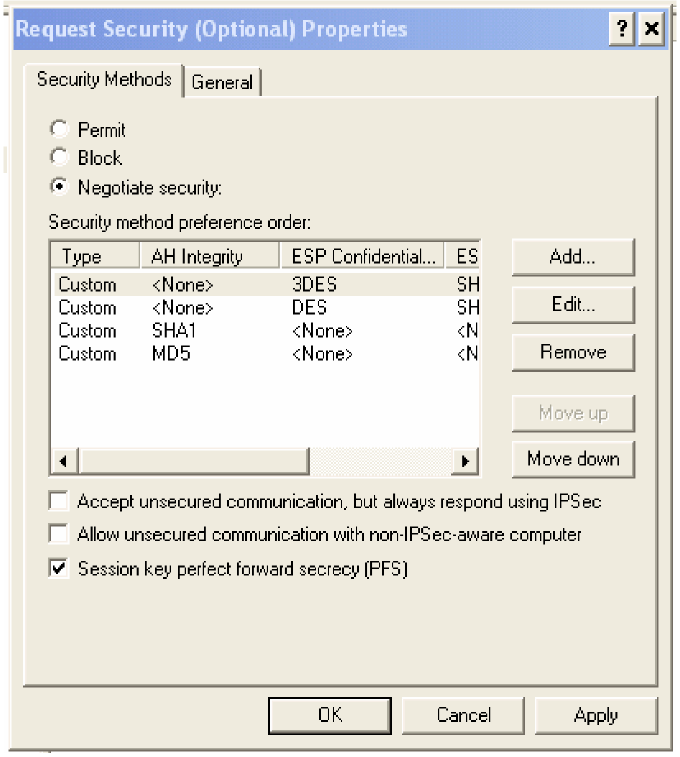
□ Generate a new key every: 100000 Kbytes

□ Generate a new key every 3600 seconds

8. Click **OK**. If a security warning appears, click **OK** then click **Next**.

9. Click **Finish**. The filter action you created, for example, **My Xerox Printer Action**, appears in the list of available Filter Actions.

10. Double-click the action you just created to edit its **Properties**.



Request Security (Optional) Properties

○ Permit

○ Block

● Negotiate security:

Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	DES	SH
Custom	SHA1	<None>	<N
Custom	MD5	<None>	<N

□ Accept unsecured communication, but always respond using IPSec

□ Allow unsecured communication with non-IPSec-aware computer

☑ Session key perfect forward secrecy (PFS)

11. Verify the **Accept unsecured communication, but always respond using IPSec**.and **Allow unsecured communication with non-IPSec-aware computer** are not checked.

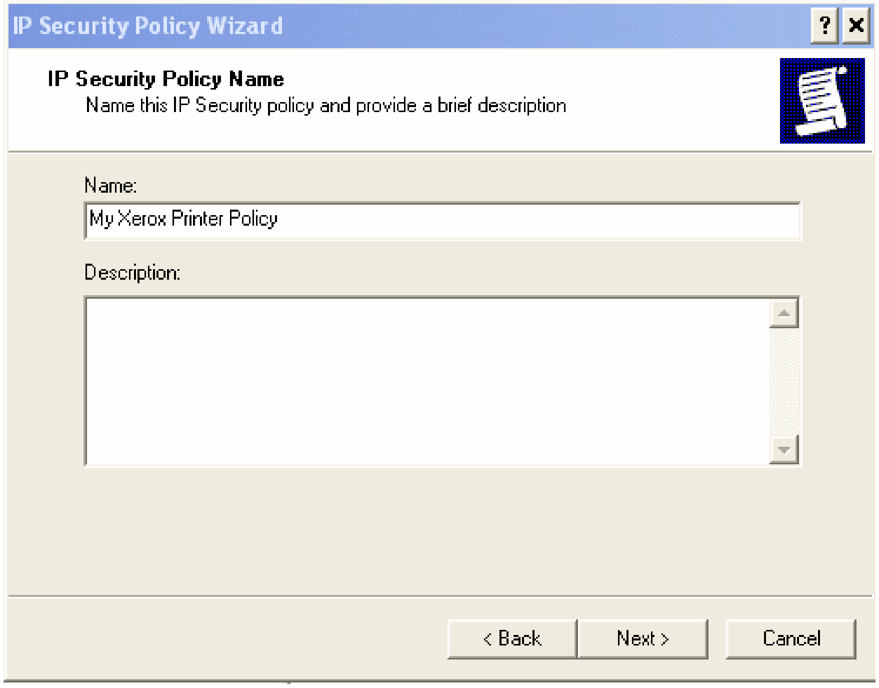
12. Check **Session key perfect forward secrecy (PFS)**.

13. Click **OK**.
14. Click **Close** to finish.

Creating an IP Security Policy Rule

To use an IPSec policy at least one rule that links a filter list to a filter action is required.

1. In the Local Security Settings window right click **IP Security Policies on Local Machine** and select **Create IP Security Policy**, to start the IP Security Policy Wizard.
2. Click **Next**. Enter a name for the policy, for example **My Xerox Printer Policy**.



IP Security Policy Wizard

IP Security Policy Name

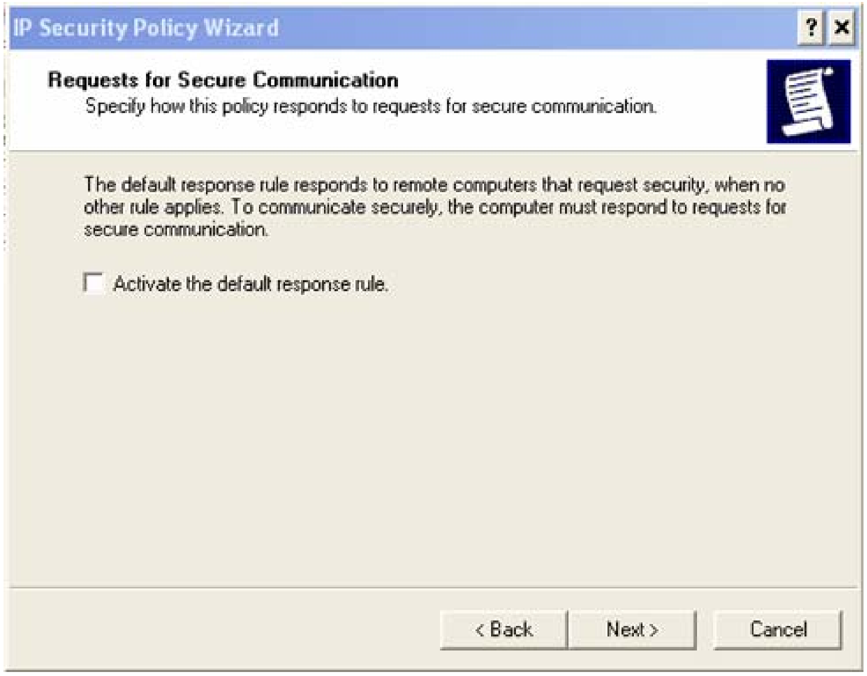
Name this IP Security policy and provide a brief description

Name:

My Xerox Printer Policy

Description:

3. Click **Next**. Uncheck the **Activate the default response rule**.



IP Security Policy Wizard

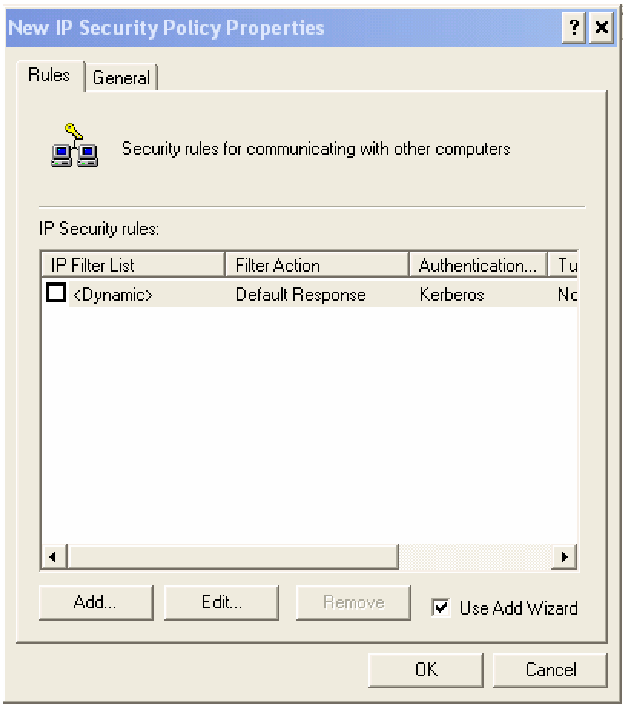
Requests for Secure Communication

Specify how this policy responds to requests for secure communication.

The default response rule responds to remote computers that request security, when no other rule applies. To communicate securely, the computer must respond to requests for secure communication.

☐ Activate the default response rule.

4. Click **Next**, then click **Finish**.
5. The **New IP Security Policy Properties** window appears. Click **Add** to start a new rule.



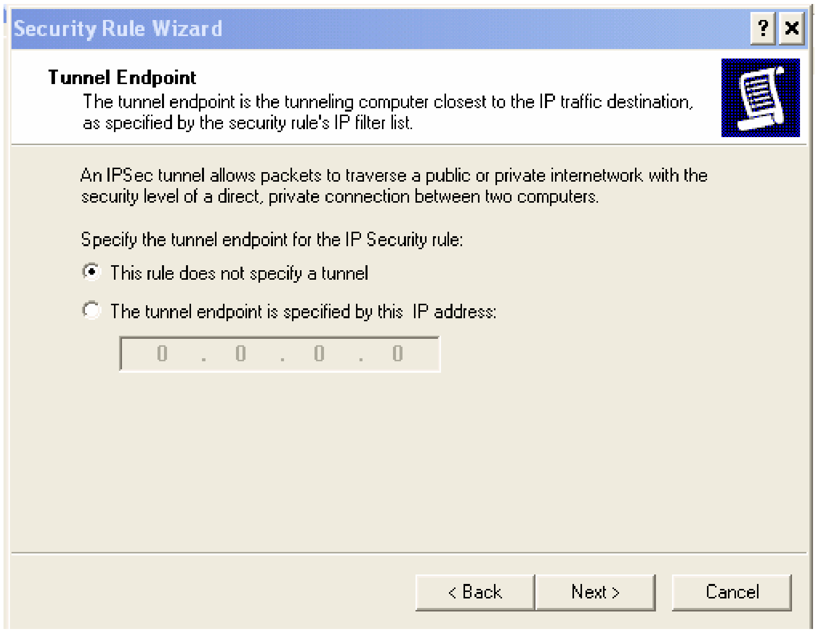
Security rules for communicating with other computers

IP Security rules:

IP Filter List	Filter Action	Authentication...	Tu
□ <Dynamic>	Default Response	Kerberos	Nc

☑ Use Add Wizard

6. Click **Next** to start the Security Rule Wizard.
7. For the **Tunnel Endpoint** select **This rule does not specify a new tunnel** then click **Next**.



Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

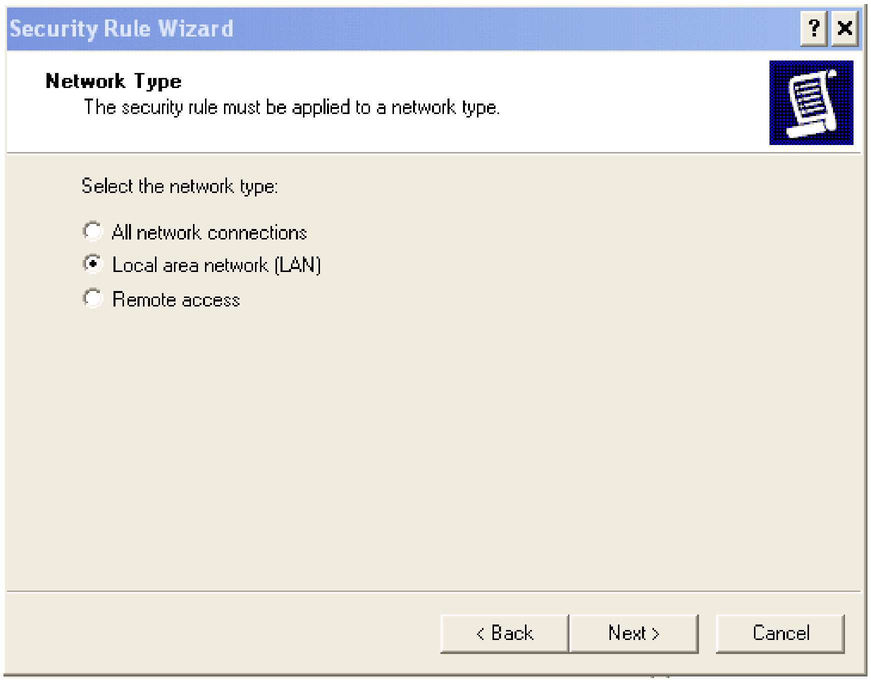
Specify the tunnel endpoint for the IP Security rule:

● This rule does not specify a tunnel

○ The tunnel endpoint is specified by this IP address:

0 . 0 . 0 . 0

8. Select **Local Area Network (LAN)** for **Network Type**



Security Rule Wizard

Network Type

The security rule must be applied to a network type.

Select the network type:

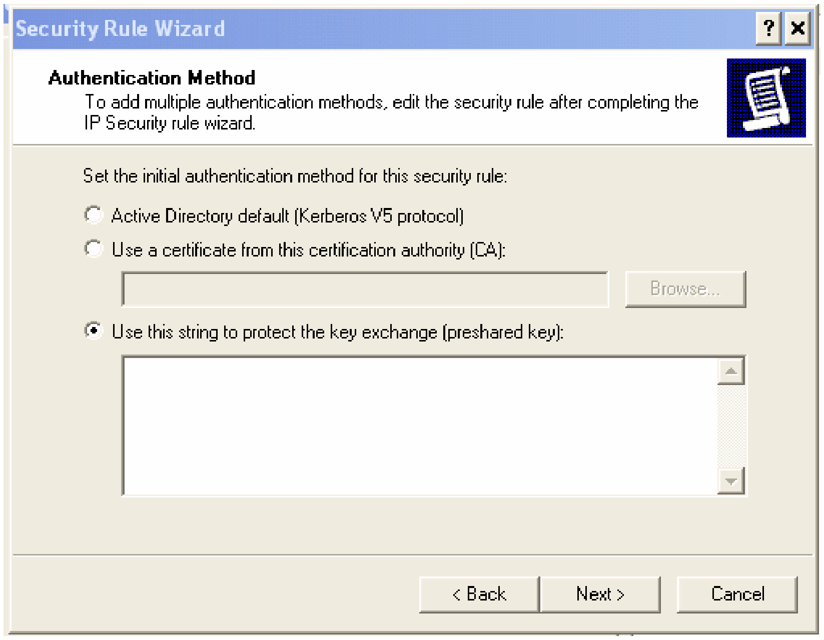
○ All network connections

● Local area network (LAN)

○ Remote access

9. Click **Next**. Select **Use this string to protect the key exchange (preshared key):** for the Authentication Method.

Note: This document only describes the preshared key authentication method. Other authentication methods are available.



Security Rule Wizard

Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP Security rule wizard.

Set the initial authentication method for this security rule:

○ Active Directory default (Kerberos V5 protocol)

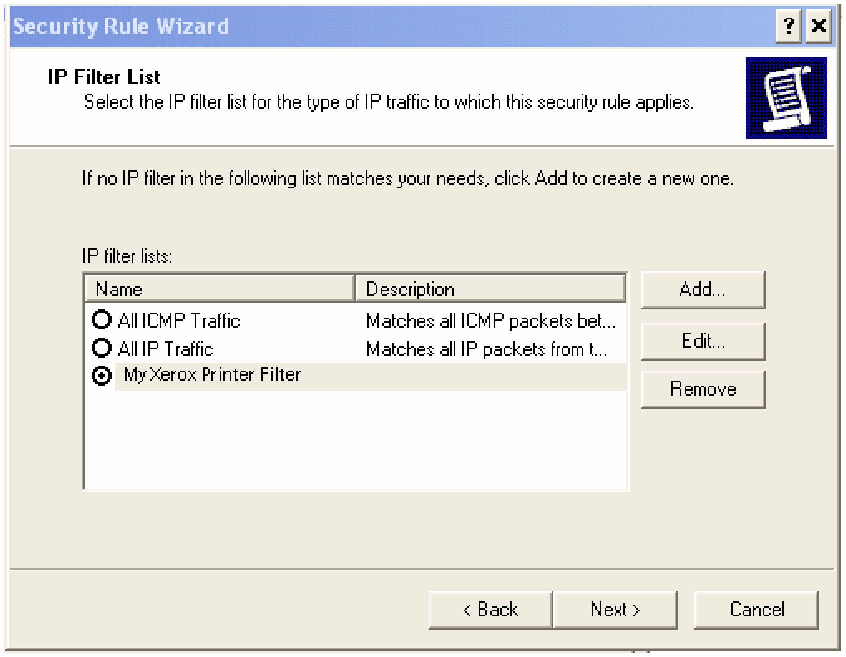
○ Use a certificate from this certification authority (CA):

● Use this string to protect the key exchange (preshared key):

10. Enter a string of alphanumeric characters to serve as the preshared key.

IMPORTANT: You must duplicate this string in the Xerox device IPSec configuration process described in the next section, “Configuring IPSec on a Xerox Device.”

11. Click **Next**. Select the filter created earlier (for example, **My Xerox Printer Filter**) from the list.



IP Filter List

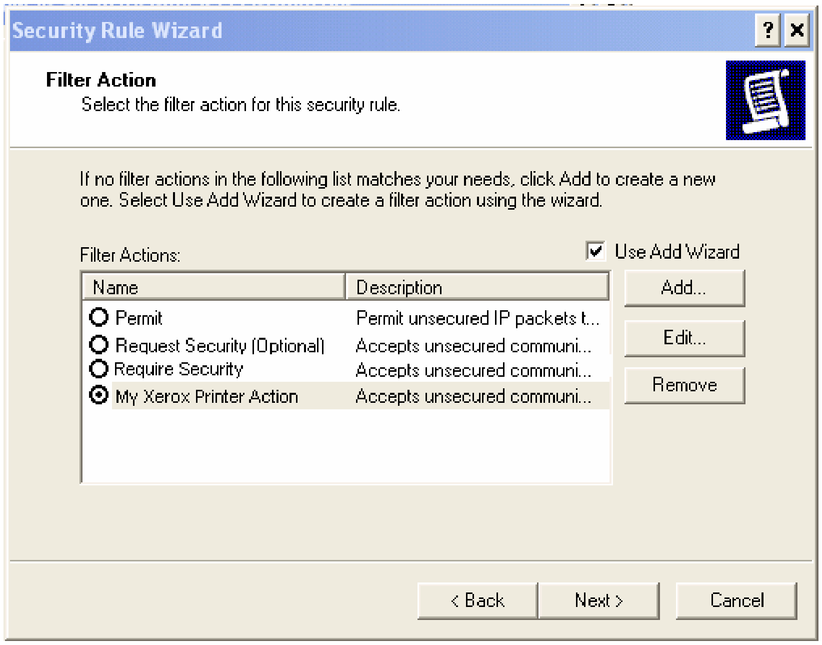
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
● My Xerox Printer Filter	

12. Click **Next**. Select the filter action created earlier (for example, **My Xerox Printer Action**) from the list.



Filter Action

Select the filter action for this security rule.

If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action using the wizard.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
○ Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...
● My Xerox Printer Action	Accepts unsecured communi...

13. Click **Next** then **Finish**.

14. Click **OK** then **Close**.

15. To activate the policy, on the Local Securities Settings window select **IP Security Policies on Local Machine** in the left hand pane, then right click on the **My Xerox Printer Policy** and select **Assign**.

Configuring IPSec on a Xerox Device

Before you can configure IPSec on a Xerox device, you must acquire an SSL certificate and enable SSL.

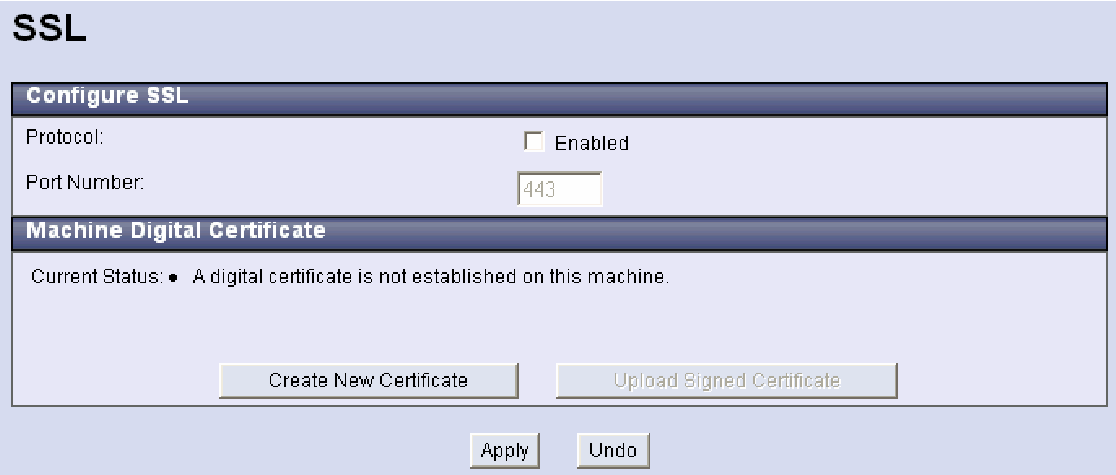
Acquiring an SSL Certificate

The types of SSL certificates available are described in the following list. Use the process in either “Create a Self Signed Certficate,” or “Create a Certificate Signing Request and Upload the Signed Certificate,” to acquire an SSL certificate.

- **Self Signed Certificate: Establish a Self Signed Certificate on this machine.** This option creates a certificate that is not validated by a Certificate Authority. This type of certificate is used primarily to obtain a key. The information you enter is similar to that required to request an external certificate but it serves no real purpose. A self-signed certificate can expire and still have a valid, usable key. Depending on the security level you require, this selection may not be adequate.
- **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.** The information on this page is saved in a .pem.txt file that is sent to an external authority who can issue a certificate.

Create a Self Signed Certificate

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.



SSL

Configure SSL

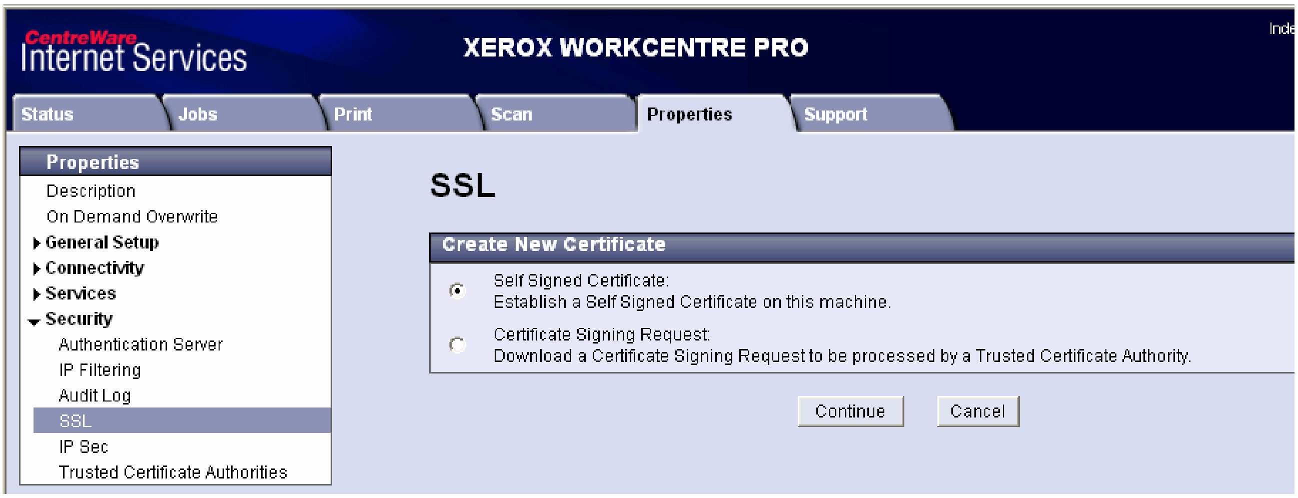
Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status: ● A digital certificate is not established on this machine.

2. Click **Create New Certificate**.



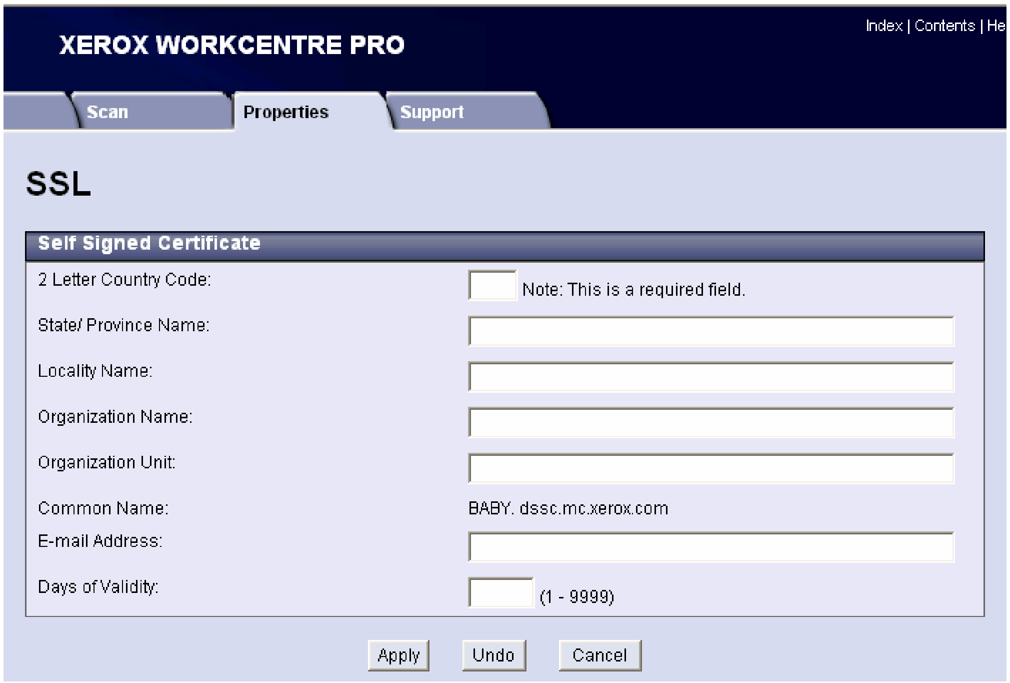
SSL

Create New Certificate

● Self Signed Certificate:
Establish a Self Signed Certificate on this machine.

○ Certificate Signing Request:
Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.

3. Select **Self Signed Certificate: Establish a Self Signed Certificate on this machine** then click **Continue**.



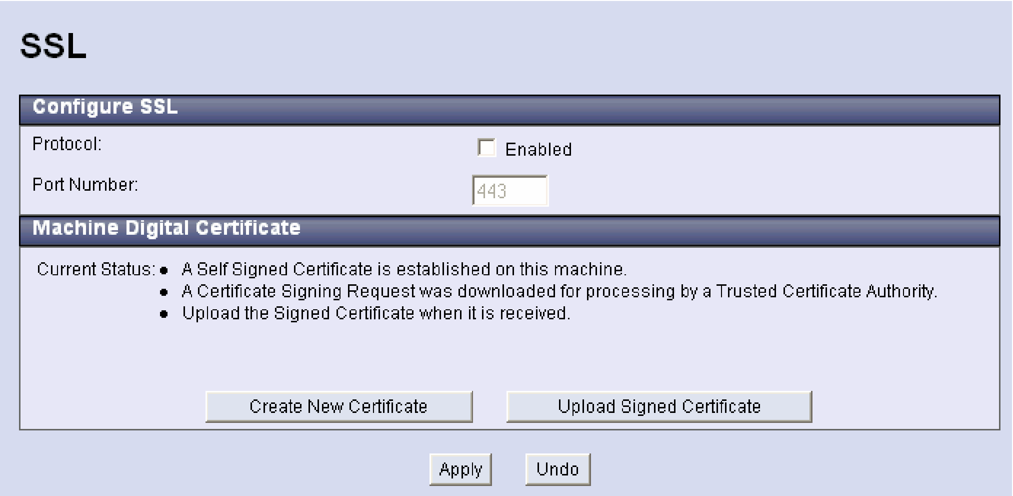
SSL

Self Signed Certificate

2 Letter Country Code:	Note: This is a required field.
State/ Province Name:	
Locality Name:	
Organization Name:	
Organization Unit:	
Common Name:	BABY. dssc.mc.xerox.com
E-mail Address:	
Days of Validity:	(1 - 9999)

Enter information for a self-signed certificate. The country code field entry is required.

4. Click **Apply**. The Administrator Authentication screen may appear. Enter the current User Name and Password and click **OK**. The SSL page appears and shows that the device has a Self Signed Certificate.



SSL

Configure SSL

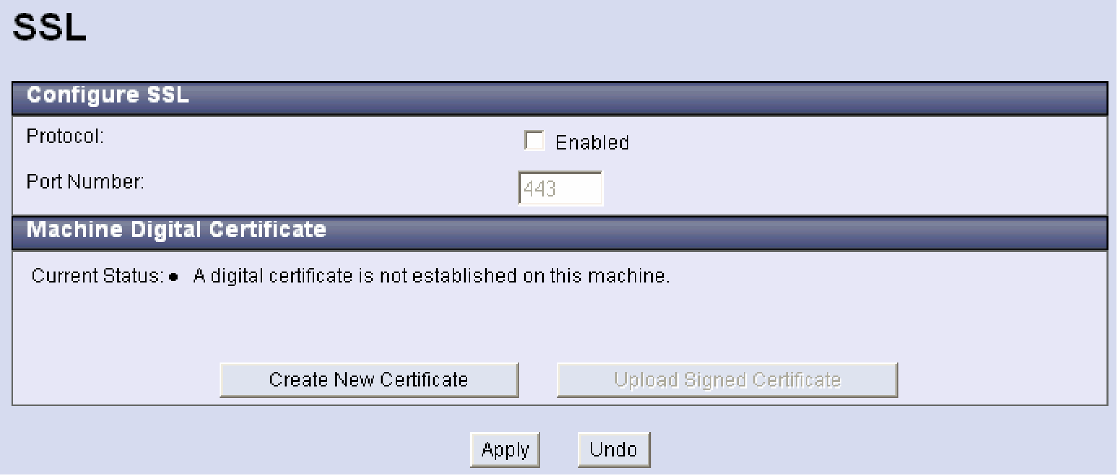
Protocol:	□ Enabled
Port Number:	443

Machine Digital Certificate

Current Status:
- A Self Signed Certificate is established on this machine.
- A Certificate Signing Request was downloaded for processing by a Trusted Certificate Authority.
- Upload the Signed Certificate when it is received.

Create a Certificate Signing Request and Upload the Signed Certificate

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.



SSL

Configure SSL

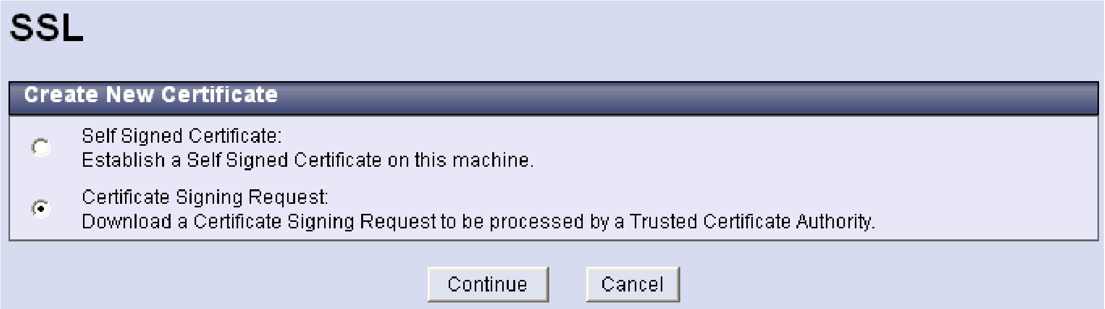
Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status: ● A digital certificate is not established on this machine.

2. Click **Create New Certificate**. Select **Certificate Signing Request: Download a Certificate Signing Request to be processed by a Trusted Certificate Authority** then click **Continue**.



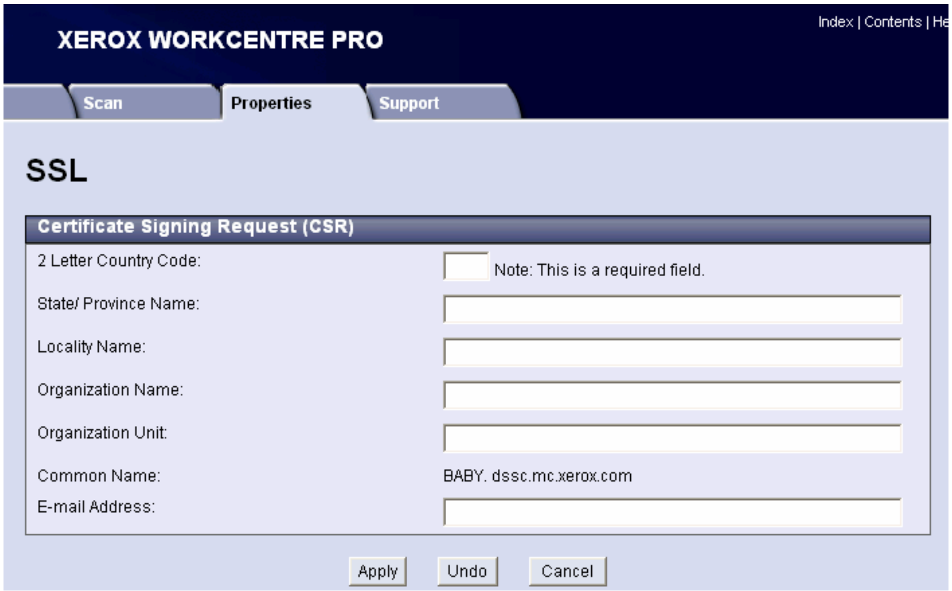
SSL

Create New Certificate

○ Self Signed Certificate:
Establish a Self Signed Certificate on this machine.

● Certificate Signing Request:
Download a Certificate Signing Request to be processed by a Trusted Certificate Authority.

3. Enter the information you wish to appear in your Certificate Signing Request.



SSL

Certificate Signing Request (CSR)

2 Letter Country Code: Note: This is a required field.

State/ Province Name:

Locality Name:

Organization Name:

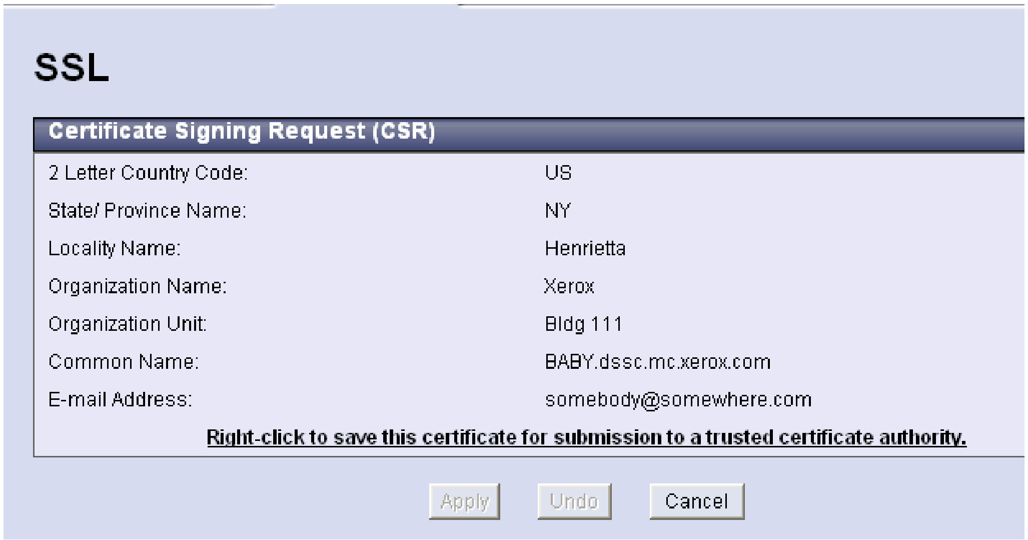
Organization Unit:

Common Name: BABY. dssc.mc.xerox.com

E-mail Address:

4. Click **Apply**. The Administrator Authentication screen may appear. Enter the current User Name and Password and click **OK**.

5. The certificate request information you entered is displayed. Below this data, right-click the link and select **Save Target As**.



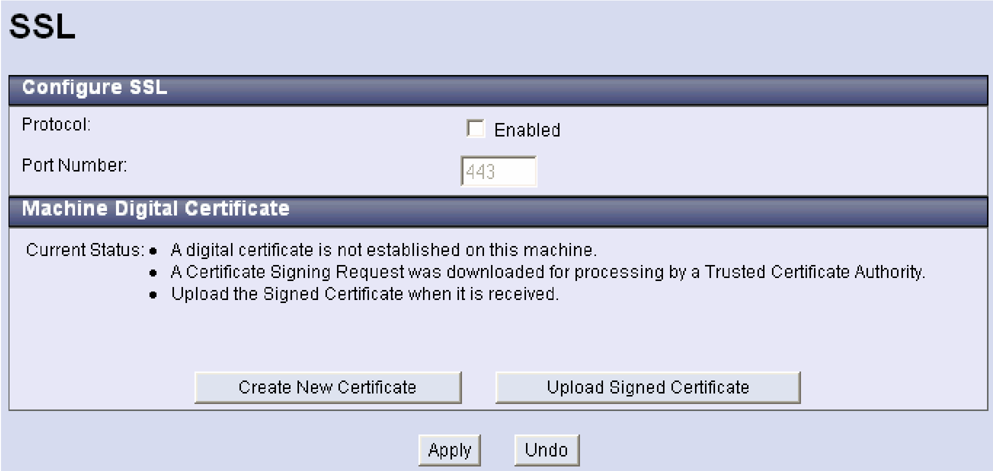
SSL

Certificate Signing Request (CSR)

2 Letter Country Code:	US
State/ Province Name:	NY
Locality Name:	Henrietta
Organization Name:	Xerox
Organization Unit:	Bldg 111
Common Name:	BABY.dssc.mc.xerox.com
E-mail Address:	somebody@somewhere.com

Right-click to save this certificate for submission to a trusted certificate authority.

6. Save the .pem.txt file and send it to a trusted certificate authority. A status message appears on the SSL page indicating a Certificate Signing Request is pending.



SSL

Configure SSL

Protocol: □ Enabled

Port Number: 443

Machine Digital Certificate

Current Status:
- A digital certificate is not established on this machine.
- A Certificate Signing Request was downloaded for processing by a Trusted Certificate Authority.
- Upload the Signed Certificate when it is received.

You receive notification of the signed certificate in a manner that complies with the policy of the authority issuing the certificate (for example, via email).

1. When you receive the signed certificate, access the SSL page again and click **Upload Signed Certificate**.
2. Click **Browse**, locate the certificate (.pem file), and click **Upload Certificate**.
3. **Current Status** on the SSL page shows a Signed Certificate resides on the device.

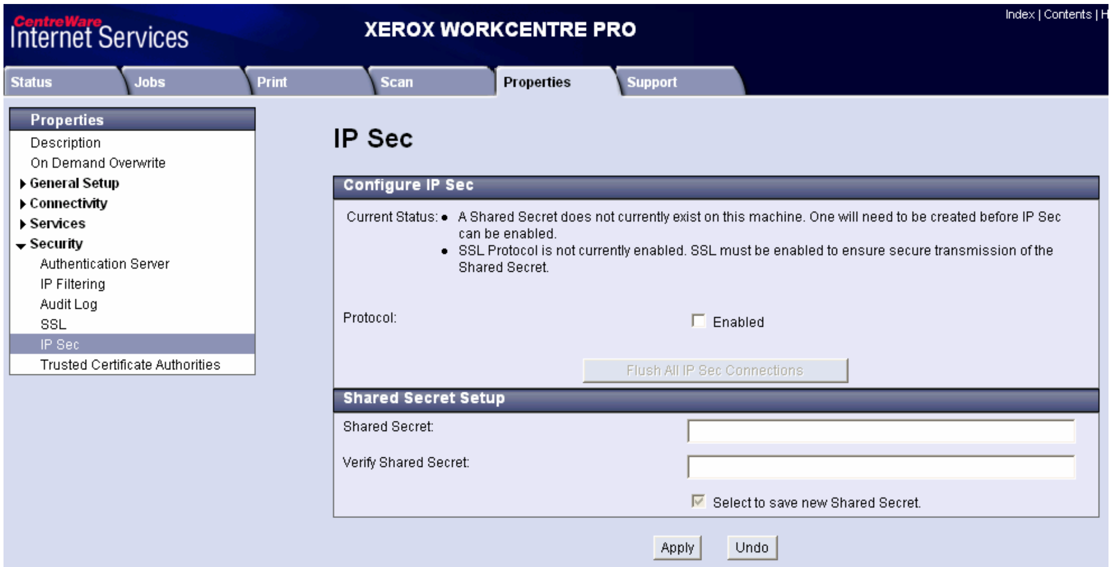
Enable SSL

After a certificate exists you can enable SSL.

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in a browser **Address** field. Select the **Properties** tab, expand **Security** and select **SSL**.
2. Select the **Protocol Enabled** box and click **Apply**.

Enable IPSec

1. Enter the IP address or host name of the WorkCentre or WorkCentre Pro in the browser **Address** field.
2. Select the Properties tab and expand **Security**. Select **IP Sec**.



IP Sec

Configure IP Sec

Current Status:
- A Shared Secret does not currently exist on this machine. One will need to be created before IP Sec can be enabled.
- SSL Protocol is not currently enabled. SSL must be enabled to ensure secure transmission of the Shared Secret.

Protocol: □ Enabled

Shared Secret Setup

Shared Secret:

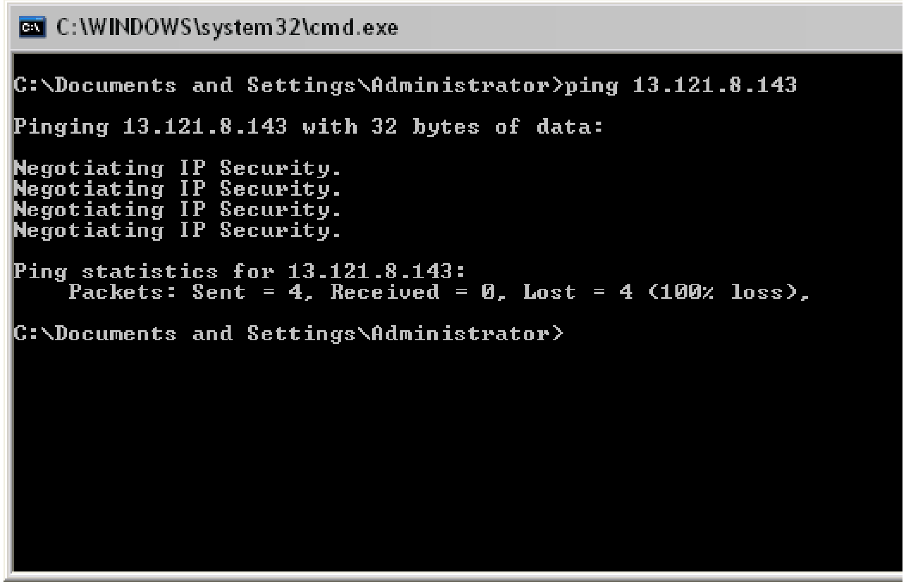
Verify Shared Secret:

☑ Select to save new Shared Secret.

3. Check the **Enabled** box.
4. If required, click **Flush All IP Sec Connections**.
5. In the **Shared Secret** field, enter the pre-shared key string you entered in the Authentication Method screen of the Security Rule Wizard (see “Creating an IP Security Policy Rule”).

Using Your Secure Connection

To test the secure connection select **Start>Run** to open up a console window on the client or server configured for IPsec, enter **cmd** and click **OK**. Use the **ping <IP Address>** command where <IP Address> is the IP of the Xerox device. If the configuration is correct you see the Negotiating security messages and then ping exits.



```
C:\Documents and Settings\Administrator>ping 13.121.8.143

Pinging 13.121.8.143 with 32 bytes of data:

Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.
Negotiating IP Security.

Ping statistics for 13.121.8.143:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

Now, when you send a print job try print to the device from an application, it is using IPSec.

Additional Information

Xerox Customer Support welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA),
TTY 1-800-855-2880 or at http://www.xerox.com.

Other Tips about Xerox multifunction devices are available at the following URL: http://www.office.xerox.com/support/dctips/dctips.html.

XEROX®