



Extreme Management Center Secure Deployment Guide

7/2020
9036782-00
Subject to Change Without Notice

Copyright © 2020 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks/

Contact

If you require assistance, contact Extreme Networks using one of the following methods.

- **[Global Technical Assistance Center \(GTAC\) for Immediate Support](#)**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **[GTAC Knowledge](#)** – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **[The Hub](#)** – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This

community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Table of Contents

Table of Contents	4
Pre-Installation Configuration	6
Installation Prerequisites	6
User Accounts	6
Configuring Server Account Settings to be STIG-Compliant	6
Setting the Password Policy	7
Setting the Account Lockout Policy	8
Setting the Audit Policy	9
Setting the Security Options	10
Configuring Windows Users and Groups	13
Creating an Extreme Management Center User Group	13
Configuring Extreme Management Center Users	13
Installing Extreme Management Center	17
Creating Extreme Management Center Users and Groups	17
Configuring Extreme Management Center	19
Configuring Extreme Management Center Services	19
Configuring Access Control of Extreme Management Center Directory	19
Encrypting the File System Service	20
Encrypting the File System of the Extreme Management Center mysql Directory	21
Configuring the Application Identity Service	21
Configuring Application Control Policies	22
Configuring AppLocker Executable Rules	22
Configuring AppLocker Script rule	28
Configuring RemoteApp Manager	33

Windows Firewall Configuration	34
Configuring IPsec	40

Pre-Installation Configuration

Installation Prerequisites

- Ensure the Windows 2008R2 server has a valid Windows key.
- Ensure Remote Desktop Services is properly installed and has a valid license.
- Verify that certificates, if any, have been created and installed on the server.

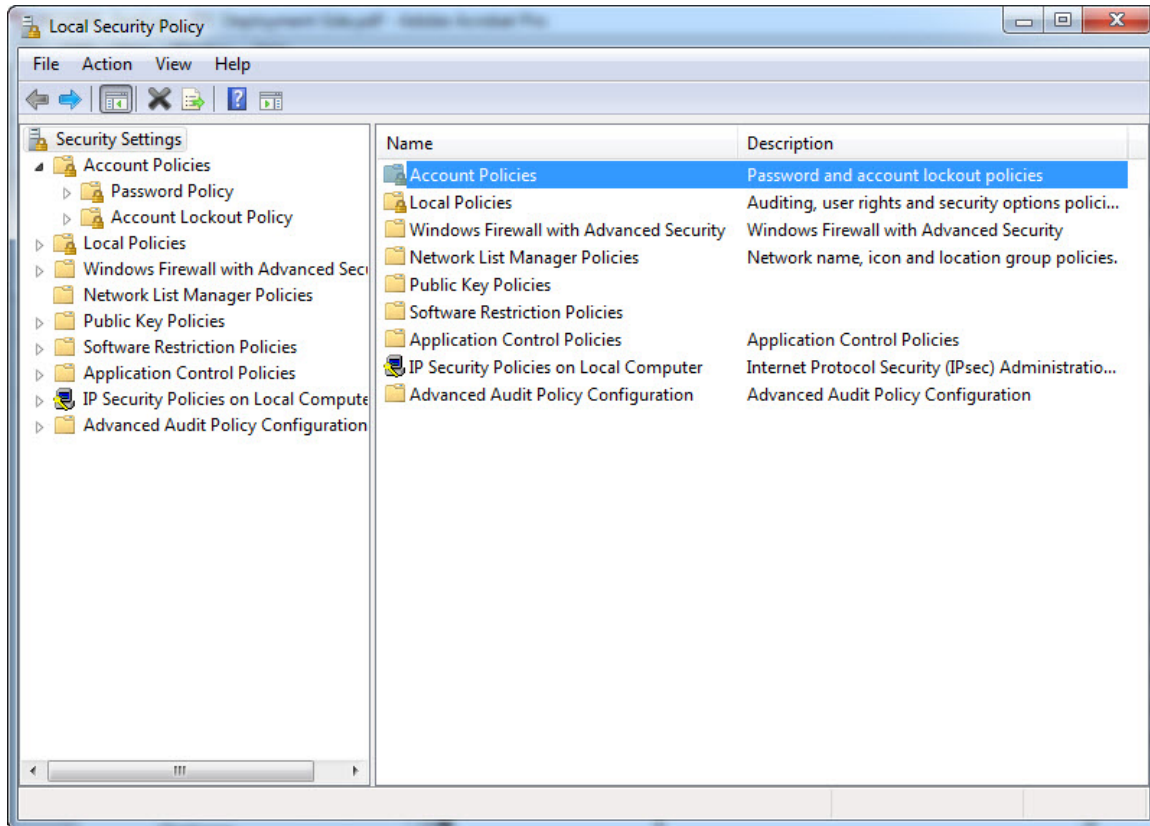
User Accounts

The procedures in this document use the user accounts listed below. They are intended to be examples of various users with certain sets of privileges. User account setup is at the discretion of the Security Administrator.

- **netsightsrv** – Extreme Management Center server administrator with full Remote Desktop privileges
- **netsightadmin** – Extreme Management Center administrator with only Extreme Management Center Remote Desktop privileges
- **netsightuser** – Extreme Management Center user with only Extreme Management Center Remote Desktop privileges
- **xadministrator** – non-default server administrator
- **xguest** – non-default guest account

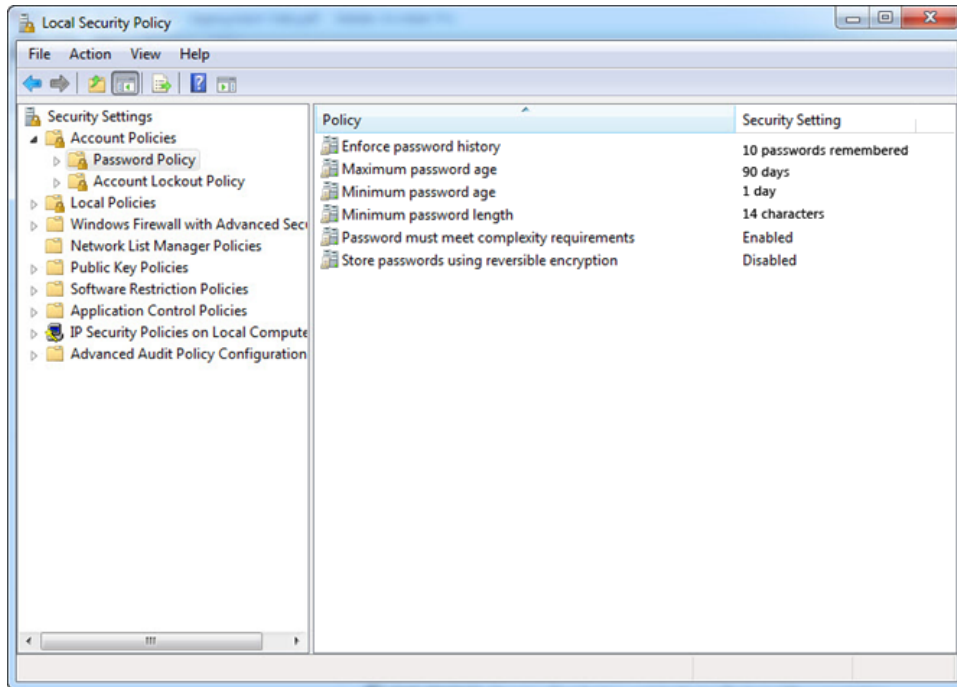
See [Configuring Extreme Management Center Users](#) for setting up user accounts.

Configuring Server Account Settings to be STIG-Compliant



Setting the Password Policy

1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Account Policies > Password Policy**.

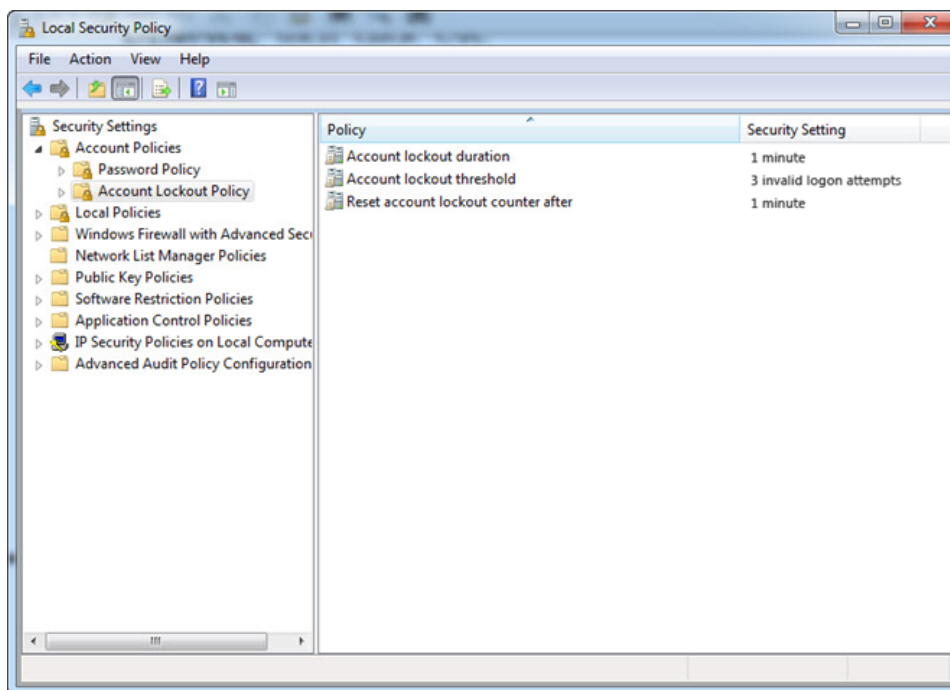


- For each of the following policies, double-click the policy name, set the new policy, and then click **OK**.

For this policy...	Set to...
Enforce password history	10 passwords remembered
Maximum password age	90 days
Minimum password age	1 day
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Setting the Account Lockout Policy

- From your desktop, select **Start > Administrative Tools > Local Security Policy > Account Policies > Account Lockout Policy**.

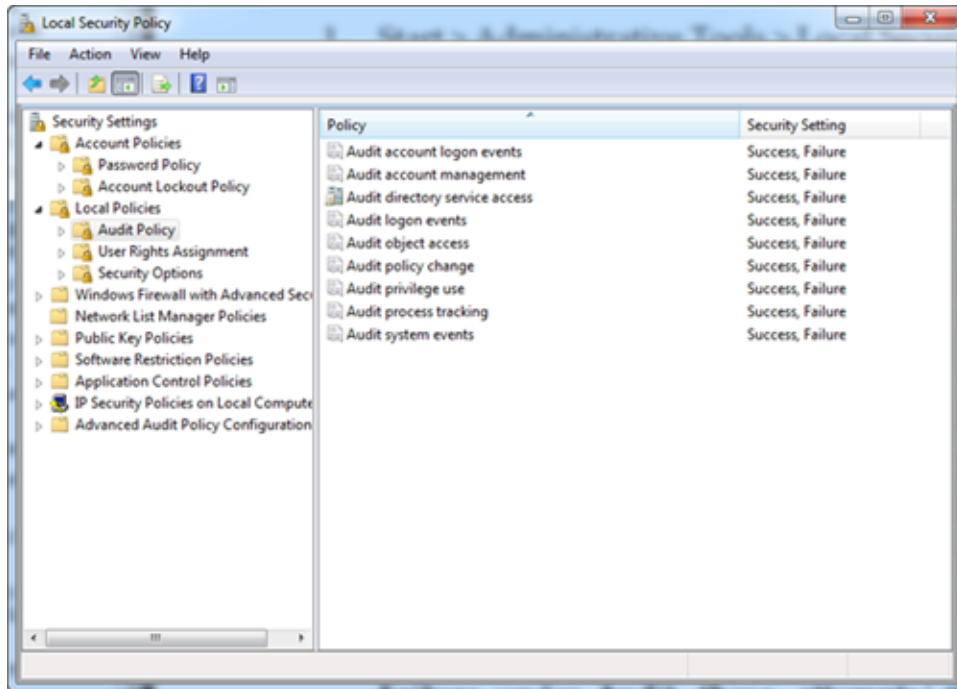


2. For each of the following policies, double-click the policy name, set the new policy, and then click **OK**.

For this policy...	Set to...
Account lockout duration	1 minute
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	1 minute

Setting the Audit Policy

1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Local Policies > Audit Policy**.

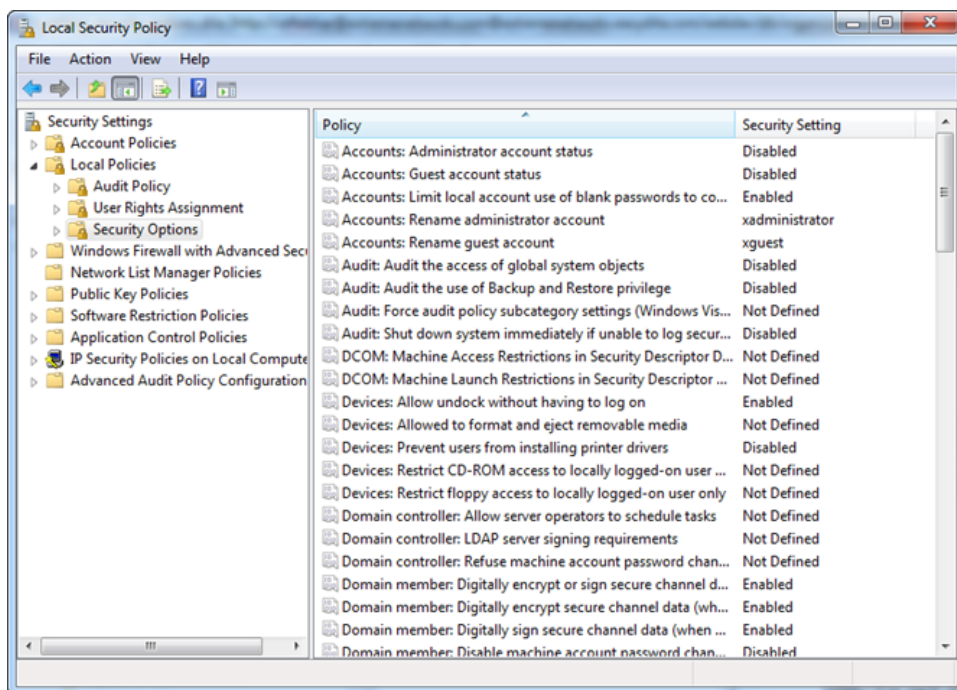


- For each of the following policies, double-click the policy name, set the new policy, and then click OK.

For this policy...	Enable...
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege user	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Setting the Security Options

- From your desktop, select **Start > Administrative Tools > Local Security Policy > Local Policies > Security Options**.



- For each of the following policies, double-click the policy name, set the new policy, and then click OK.

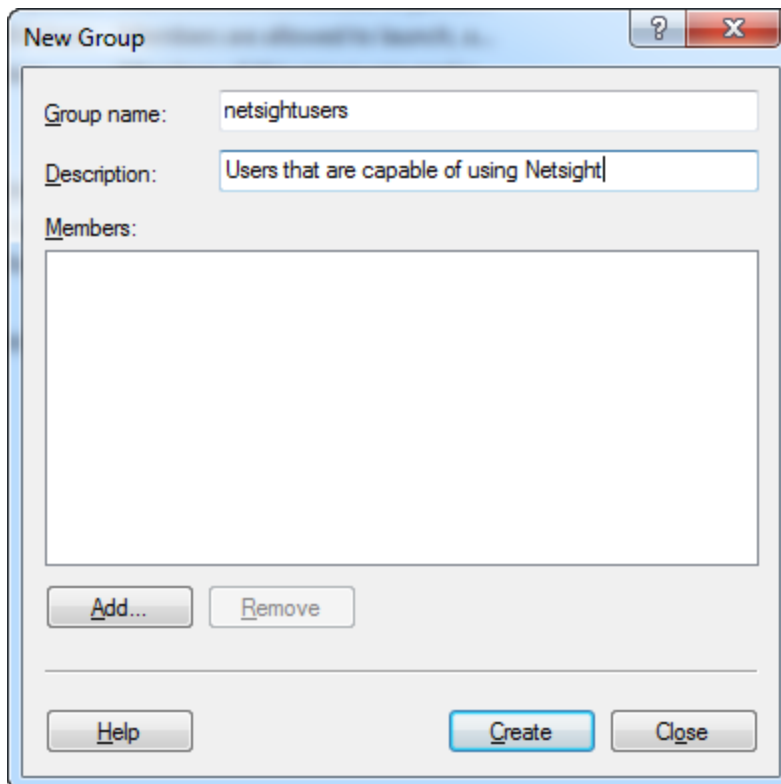
For this policy...	Set to...
Accounts: Rename administrator account	xadministrator
Accounts: Rename guest account	xguest

For this policy...	Set to...
Interactive logon: Message text for users attempting to log on	<p>Enter the following text:</p> <p>You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:</p> <p>The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS.</p> <p>Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.</p> <p>This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.</p> <p>Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.</p>
Interactive logon: Message title for users attempting to log on	<p>Enter the following text:</p> <p>U.S. Government (USG) Information System (IS) that is provided for USG authorized use only.</p>
System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing	Enable

Configuring Windows Users and Groups

Creating an Extreme Management Center User Group

1. From your desktop, select **Start > Administrative Tools > Server Manager > Local Users and Groups > Groups**.
2. Select **Action > New Group**.
3. Enter the following information:
 - **Group name:** netsightusers
 - **Description:** Users that are capable of using Extreme Management Center.



4. Click **Create** and **Close**.

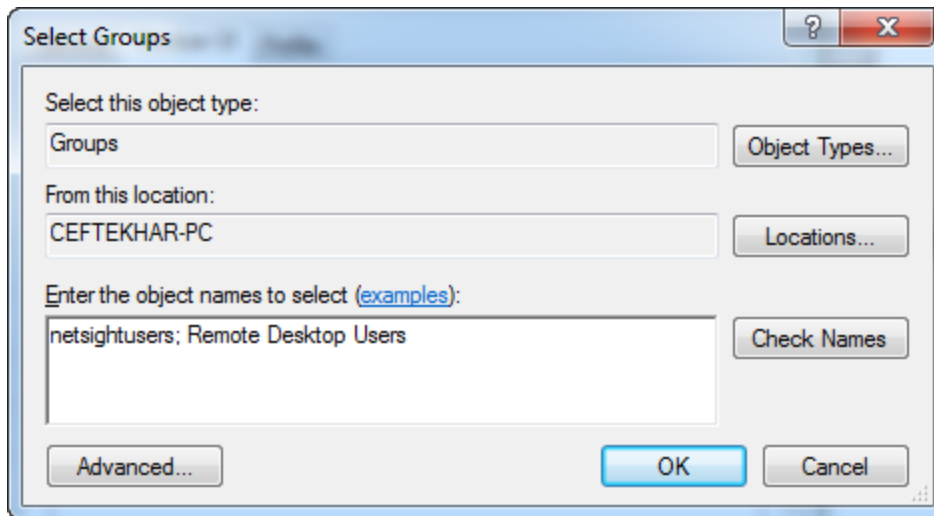
Configuring Extreme Management Center Users

1. From your desktop, select **Start > Administrative Tools > Server Manager > Local Users and Groups > Users**.

2. Select **Action > New User**.
3. Enter the following information:
 - **User name:** netsightadmin
 - **Password:** Enter a password
 - **Confirm password:** Confirm the password

The screenshot shows a 'New User' dialog box. The 'User name' field is filled with 'netsightadmin'. The 'Password' and 'Confirm password' fields are masked with dots. The 'User must change password at next logon' checkbox is checked. The 'Create' button is highlighted in blue.

4. Click **Create** and **Close**.
5. Double-click the **netsightadmin** user.
6. Select the Member of tab.
7. Click **Add**.
8. Enter `netsightusers` and Remote Desktop Users separated by a semicolon.
Note: If this user is not already part of the "User" group, add it now.



9. Click **Check Names** to validate the groups.
10. Click **OK**.
11. Remove any other groups by selecting the group and clicking **Remove**.
12. From the Environment tab, enable **Start the following program at logon**.
13. In the Profile file name field, enter `logoff.exe`.
14. Click **OK**.
15. Select **Action > New User**
16. Enter the following information:
 - **User name:** netsightuser
 - **Password:** Enter a password
 - **Confirm password:** Confirm the password
17. Click **Create and Close**.
18. Double-click the **netsightuser** user.
19. Select the **Member of** tab.
20. Click **Add**.
21. Enter `netsightusers` and `Remote Desktop Users` separated by a semicolon.
22. Click **Check Names** to validate the groups.
23. Click **OK**.
24. Remove any other groups by selecting the group and clicking **Remove**.
25. From the **Environment** tab, enable **Start the following program at logon**.

26. In the **Profile file name** field, enter `logoff.exe`.
27. Click **OK**.
28. Select **Action > New User**
29. Enter the following information:
 - **User name:** netsightsrv
 - **Password:** Enter a password
 - **Confirm password:** Confirm the password
30. Click **Create** and **Close**.
31. Double-click the **netsightsrv** user.
32. Select the **Member of** tab.
33. Click **Add**.
34. Enter `netsightusers` and `Administrators` separated by a semicolon.
35. Click **Check Names** to validate the groups.
36. Click **OK**.
37. Remove any other groups by selecting the group and clicking **Remove**.
38. From the Environment tab, enable **Start the following program at logon**.
39. In the Profile file name field, enter `logoff.exe`.
40. Click **OK**.
41. Click **Apply** and **OK**.

Installing Extreme Management Center

To install Extreme Management Center, you must be logged in as "netsightsrv".

1. Initiate the Extreme Management Center install by double-clicking the install package (via the .exe file) or install DVD.
2. From the Install GUI Welcome Screen, click **Next**.
3. Accept the terms of the license agreement, and click **Next**.
4. Enter your Extreme Management Center Product License, and then click **Next**.
5. From the next screen, clear **TFTP** and **BOOTP**, and then click **Next**.
6. Change the Install Folder to: `C:\Enterasys Networks\NetSight`, and then click **Next**.
7. If the folder does not exist, click **OK** to create folder when prompted.
8. Wait until the following status is shown: `Server is ready for connections`, and then click **Finish**.

Creating Extreme Management Center Users and Groups

1. Select **Start > All Programs > Extreme Networks > Extreme Control Center > Clients > Console**.
2. When prompted to login, use the following credentials and click **OK**:
 - **Server:** localhost
 - **User name:** netsightsrv
 - **Password:** [password defined in [Configuring Extreme Management Center Users](#)]
3. Navigate to **Tools > Authorization/Device Access**.
4. Click **Add Group** and complete the following fields:
 - **Authorization Group name:** netsightuser
 - **Membership Criteria:** basic netsight capabilities
5. From the Capabilities tab, select or clear the user's capabilities depending on the user's privileges.
6. Click **Apply**.

7. Click **Add Group** and complete the following fields:
 - **Authorization Group name:** netsightadmin
 - **Membership Criteria:** admin netsight capabilities
8. From the Capabilities tab, select or clear the user's capabilities depending on the user's privileges.
9. Click **Apply** and **Close**.
10. Click **Add User** and complete the following fields:
 - **User name:** netsightuser
 - **Domain/Host name:** localhost
 - **Authorization group:** netsightuser
11. Click **Apply**.
12. Click **Add User** and complete the following fields:
 - **User name:** netsightadmin
 - **Domain/Host name:** localhost
 - **Authorization group:** netsightadmin
13. Click **Apply**.
14. Click **Close**.
15. Exit the Extreme Management Center Console Program.

Configuring Extreme Management Center

Configuring Extreme Management Center Services

1. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
2. Double-click **BootP Service**.
3. From the **General** tab, select **Disabled** from the Startup type drop-down list.
4. From the **Log On** tab, enable **This account**.
5. Click **Browse** and enter the object name as `netsightsrv`.
6. Click **Check Names** to validate the object name.
7. Click **OK**.
8. Enter and confirm the password assigned in [Configuring Extreme Management Center Users](#).
9. Click **OK**.
10. Repeat the above steps for the following services:

For this service...	Change Startup Type to...
Extreme Management Center Database Service	Automatic
Extreme Management Center Server Service	Automatic
Extreme Management Center SNMP Trap Service	Automatic
Extreme Management Center Syslog Service	Automatic
Extreme Management Center TFTP Service	Disabled

11. Click **OK**.
12. Restart the computer and log in again as user `netsightsrv`.

Configuring Access Control of Extreme Management Center Directory

1. Navigate to the C:\ drive (**Start > Computer > OS (C:)**).
2. Right-click the directory named **Extreme Networks** and select **Properties**.

3. From the **Security** tab, click **Advanced**.
4. Click **Change Permissions**.
5. Clear the **Include inheritable permissions from this object's parent** checkbox.
6. Click **Add**.
7. Select **Replace all child object permissions with inheritable permissions from this object**.
8. Click **Add**.
9. In the **Enter the object name to select** field, type `netsightusers`.
10. Click **Check Names**.
11. Click **OK**.
12. Select **Allow** for the following permissions:
 - Traverse folder / execute file**
 - List folder / read data**
 - Read attributes**
 - Read extended attributes**
 - Create files / write data**
 - Create folders / append data**
 - Write attributes**
 - Write extended attributes**
 - Read permissions**
13. Select **Apply these permissions to objects and/or containers within this container only**.
14. Click **OK**.
15. Select **Users (NETSIGHT-1\Users)** and then click **Remove**.
16. Click **OK**, **Yes**, and **OK** twice to exit.

Encrypting the File System Service

1. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
2. Double-click **Encrypting File System (EFS)**.
3. From the **General** tab, select **Automatic** from the Startup type drop-down list.
4. Click **Start**.

5. Once the service starts, click **OK**.

Encrypting the File System of the Extreme Management Center mysql Directory

1. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
2. Double-click **Database Service**.
3. From the **General** tab, click **Stop**.
4. Once the Service has stopped, click **OK**.
5. From your desktop, navigate to the C:\ directory (**Start > Computer > OS (C:)**).
6. Navigate to **C:\Extreme Networks\NetSight**.
7. Right-click on the **mysql** directory and select **Properties**.
8. Click **Advanced**.
9. Select **Encrypt contents to secure data**.
10. Click **Apply**.
11. When prompted, select **Apply changes to this folder, subfolders and files**.
12. Click **OK** twice to exit.
13. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
14. Double-click **Database Service**.
15. From the **General** tab, click **Start**.
16. Once the Service has started, click **OK**.

Configuring the Application Identity Service

1. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
2. Double-click **Application Identity**.
3. From the **General** tab, select **Automatic** from the Startup type drop-down list.

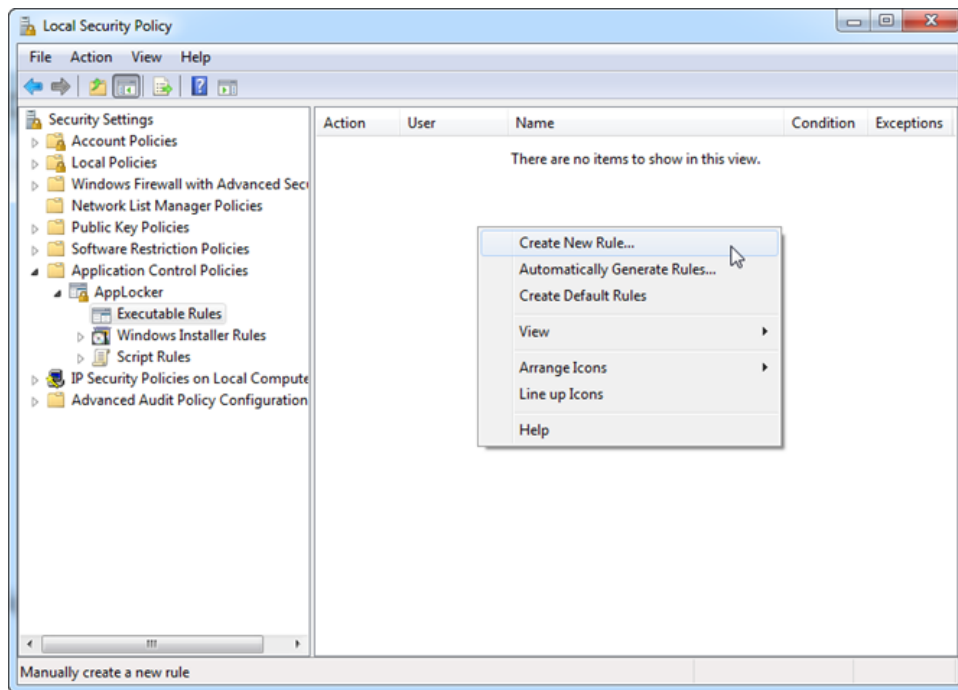
4. Click **Start**.
5. Once the service has started, click **OK**.

Configuring Application Control Policies

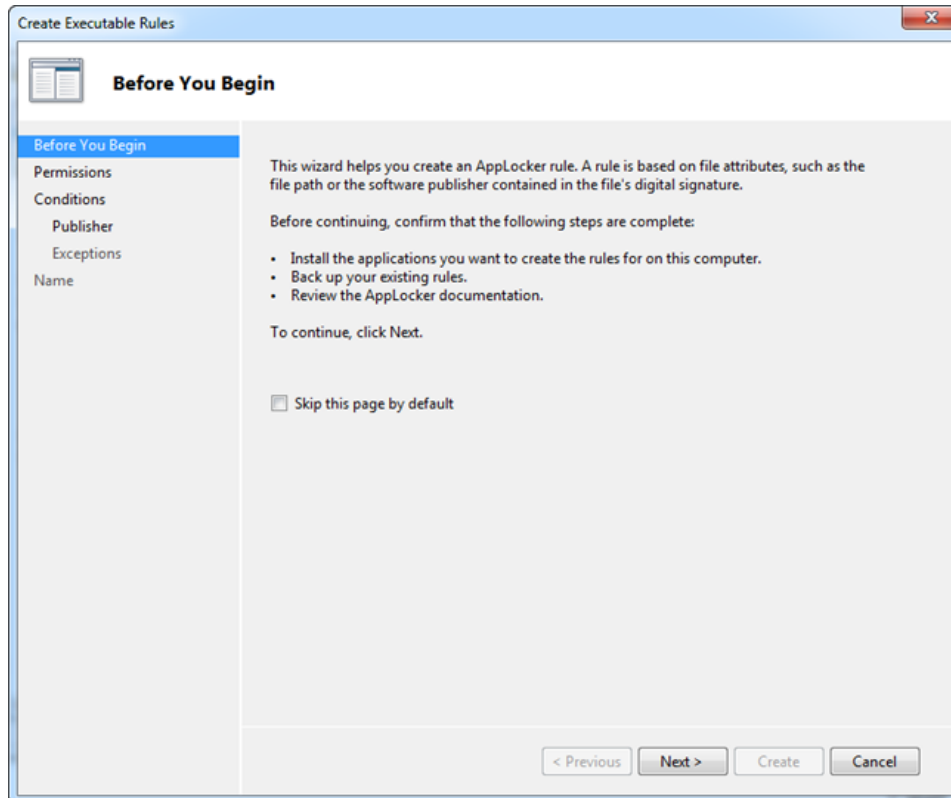
1. From your desktop, select **Start > Administrative Tools > Server Manager > Configuration > Services**.
2. Right-click **AppLocker** and select **Properties**.
3. Select **Configured** from the following sections:
Executable rules
Windows Installer rules
Script rules
4. Click **OK**.

Configuring AppLocker Executable Rules

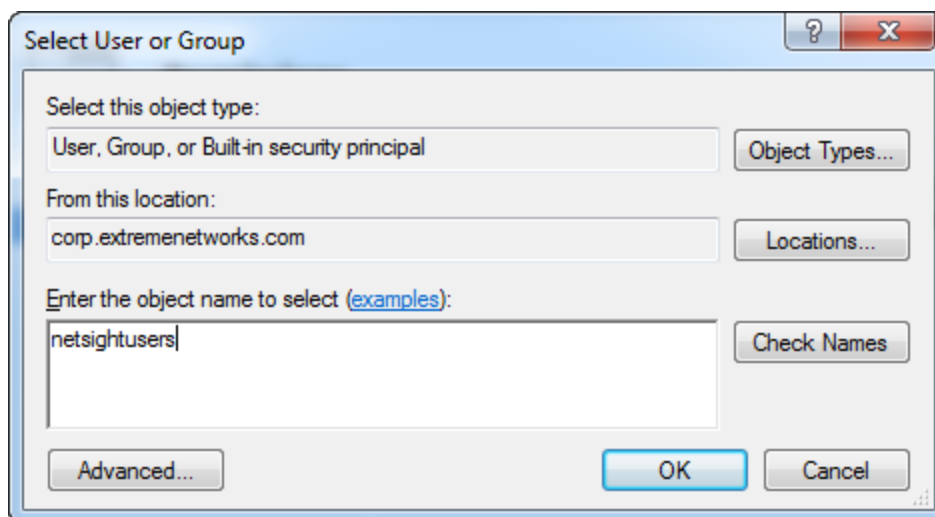
1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Application Control Policies > AppLocker > Executable Rules**.
2. Right-click in blank area and select **Create new Rule.....**



3. The Create Executable Wizard opens. Click **Next** and then select **Allow** if it is not selected by default.

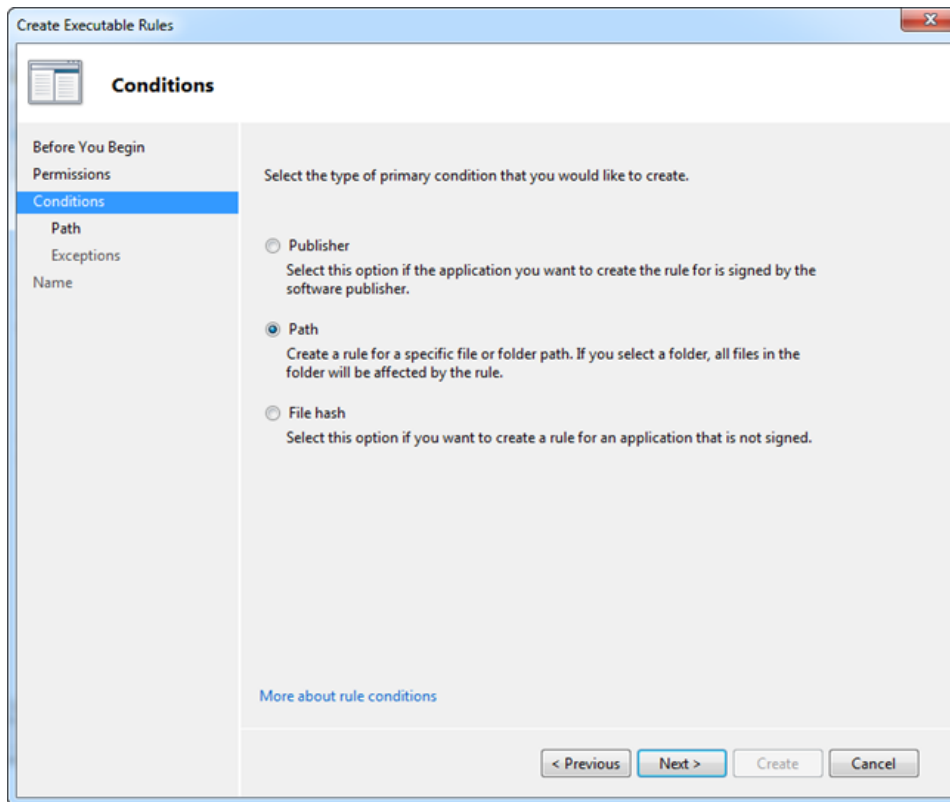


4. Click **Select**.
5. Type `netsightusers` in the following dialog.

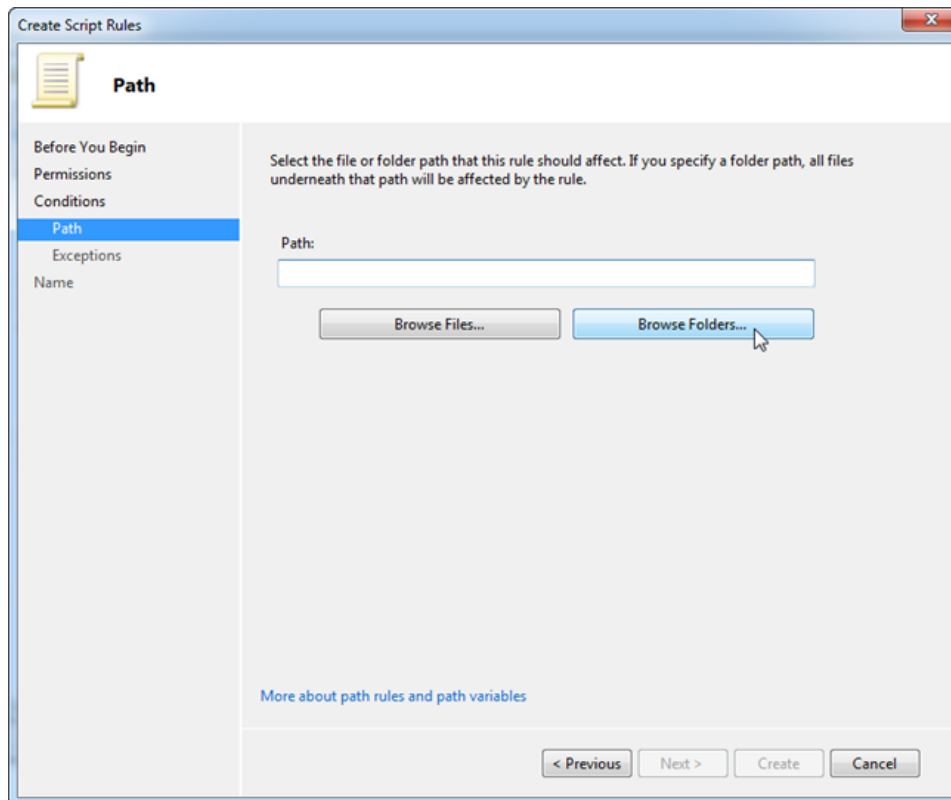


6. Click **Check Names**.
7. Click **OK**.

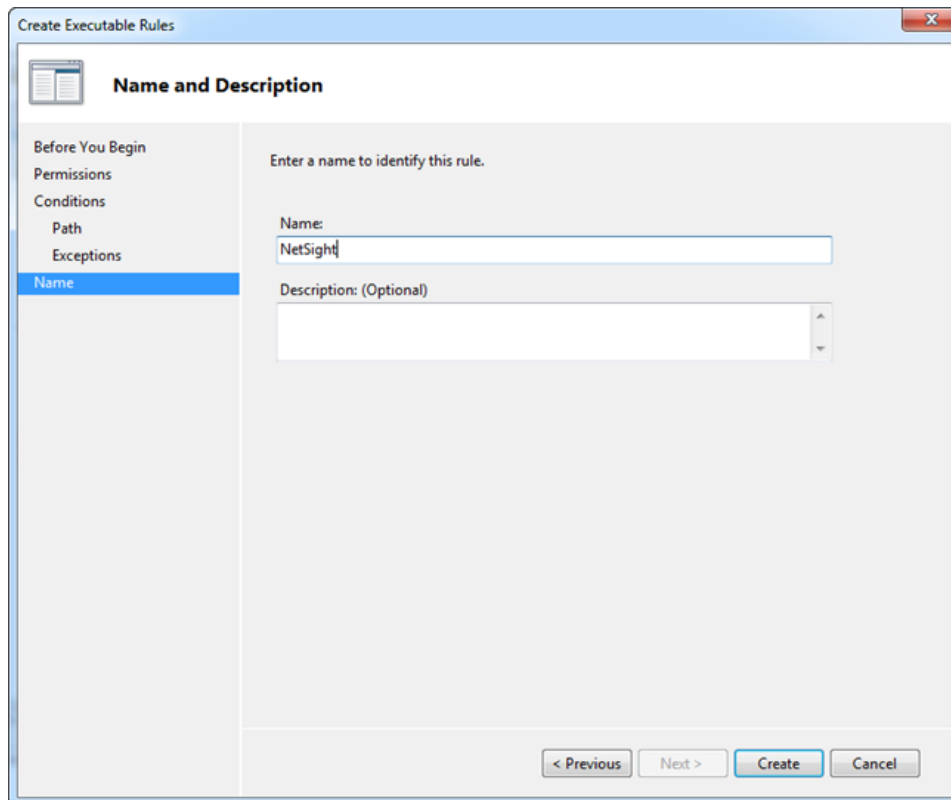
8. Click **Next**.
9. Select the **Path** option, and click **Next**.



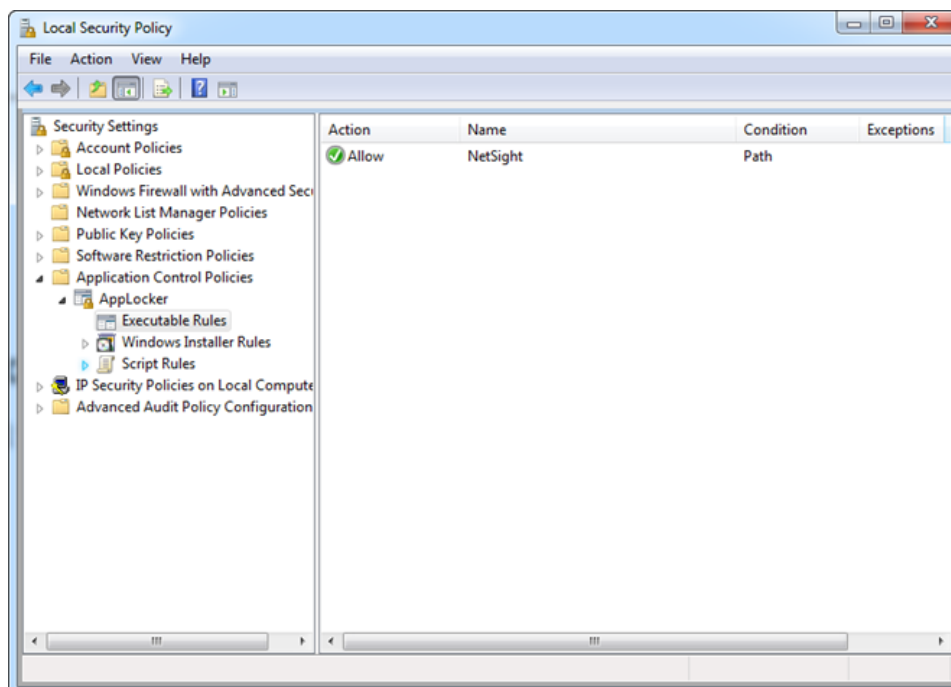
10. Click **Browse Folders...** and select the `C:\Extreme Networks` path.



11. Click **OK** and then **Next** twice.
12. In the Name field, type `NetSight`, and then click **Create**.



The wizard closes and returns to the Local Security Policy.

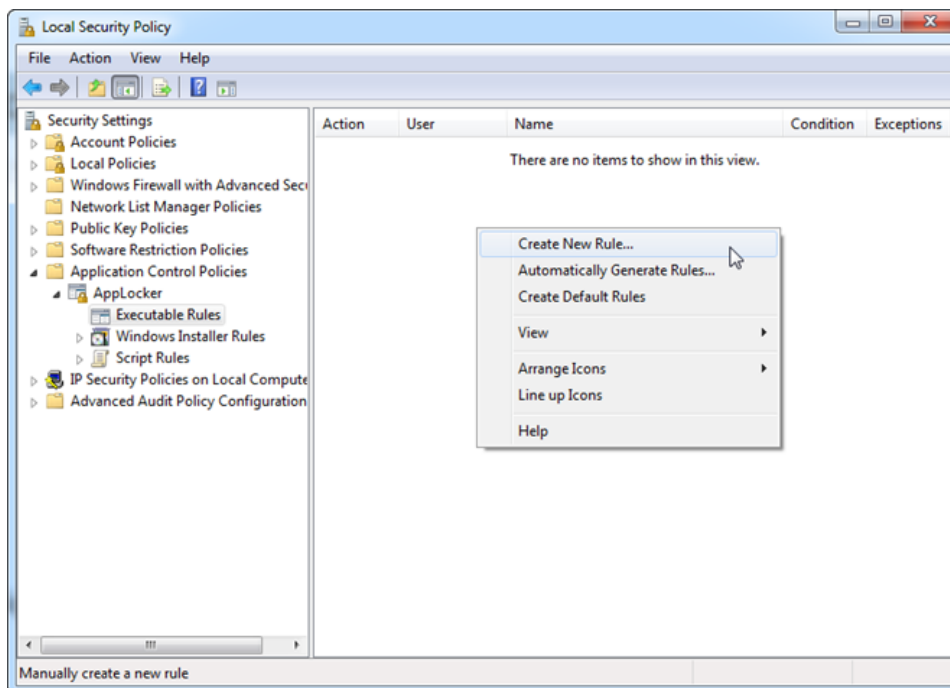


13. Repeat the preceding steps to create the following rules:

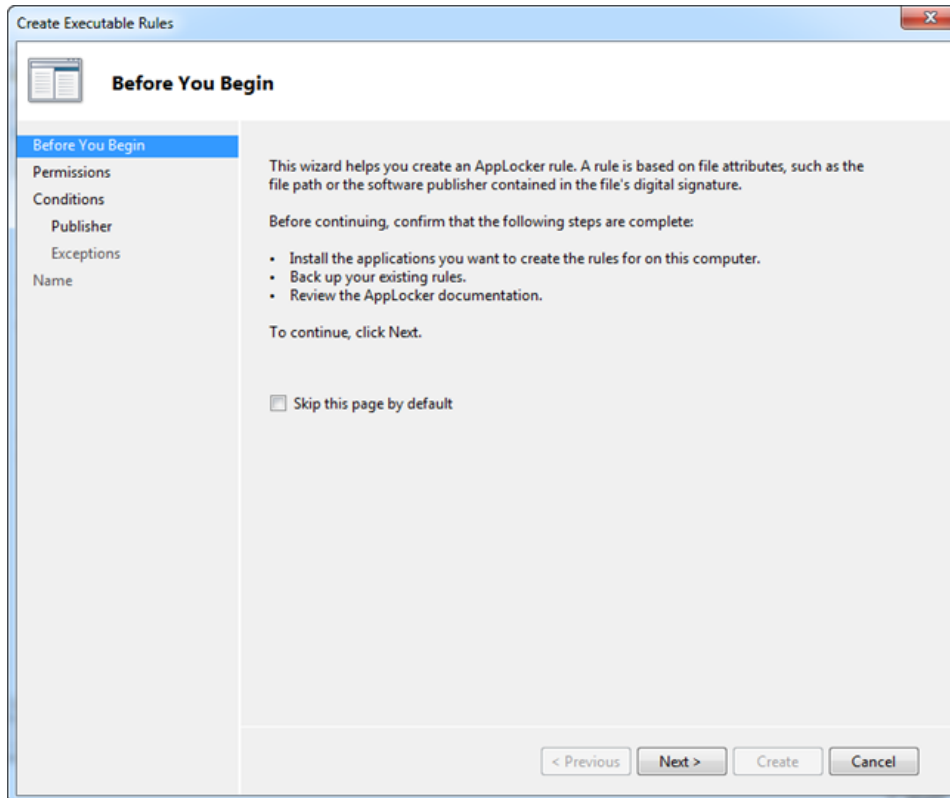
Rule Identification Name	File Path
netsightsrv	C:\Users\netsightsrv
netsightadmin	C:\Users\netsightadmin
netsightuser	C:\Users\netsightuser

Configuring AppLocker Script rule

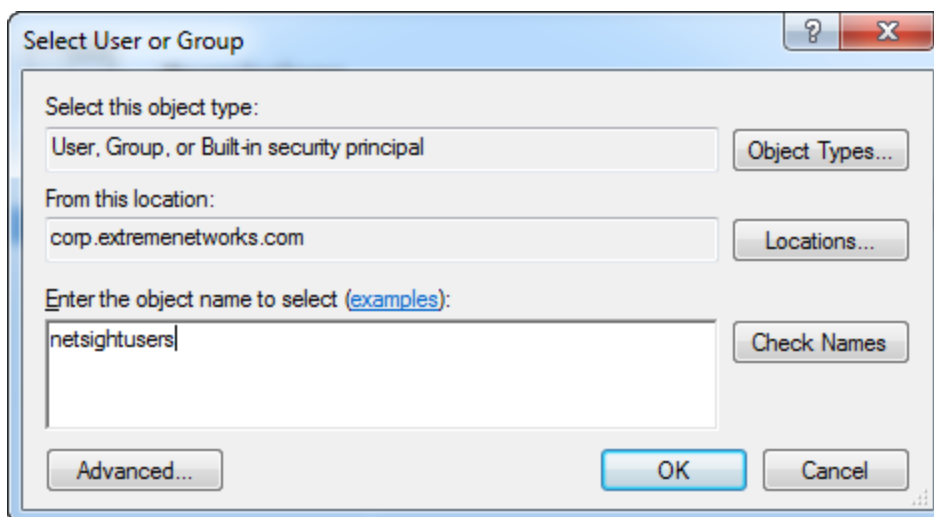
1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Application Control Policies > AppLocker > Script Rules**.
2. Right-click in blank area and select **Create New Rule.....**



3. The Create Executable Wizard opens. Click **Next** and then select **Allow** if it is not selected by default.

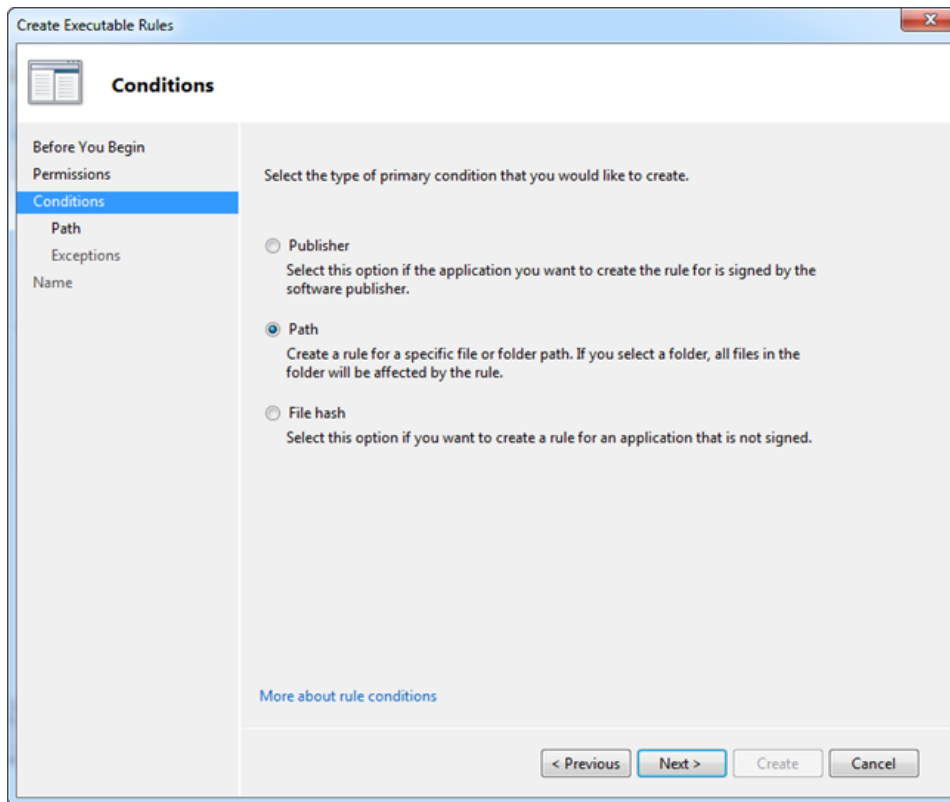


4. Click **Select**.
5. Type `netsightusers` in the following dialog.

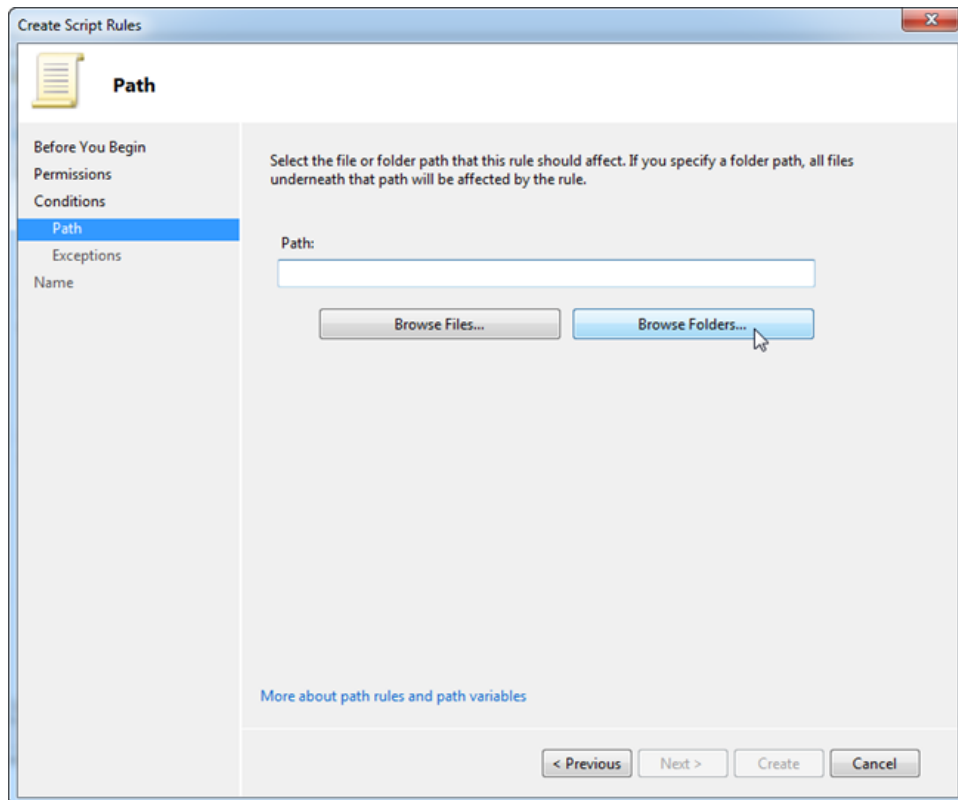


6. Click **Check Names**.
7. Click **OK**.

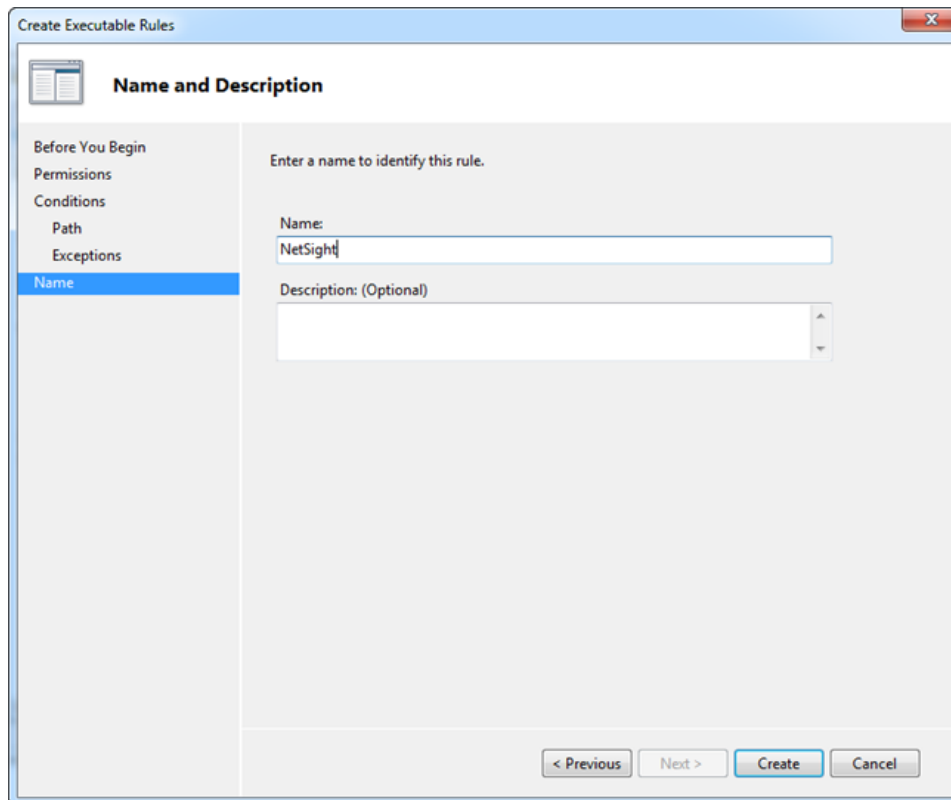
8. Click **Next**.
9. Select the **Path** option, and click **Next**.



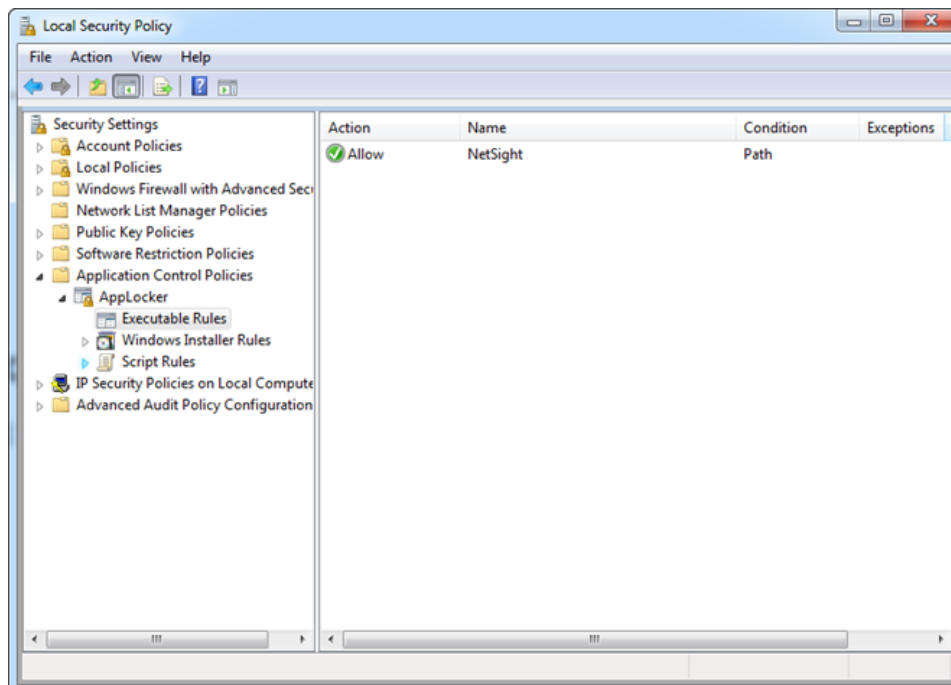
10. Click **Browse Folders...** and select the `C:\Extreme Networks` path.



11. Click **OK** and then **Next** twice.
12. In the Name field, type `NetSight`, and then click **Create**.



The wizard closes and returns to the Local Security Policy.



13. Repeat the preceding steps to create the following rules:

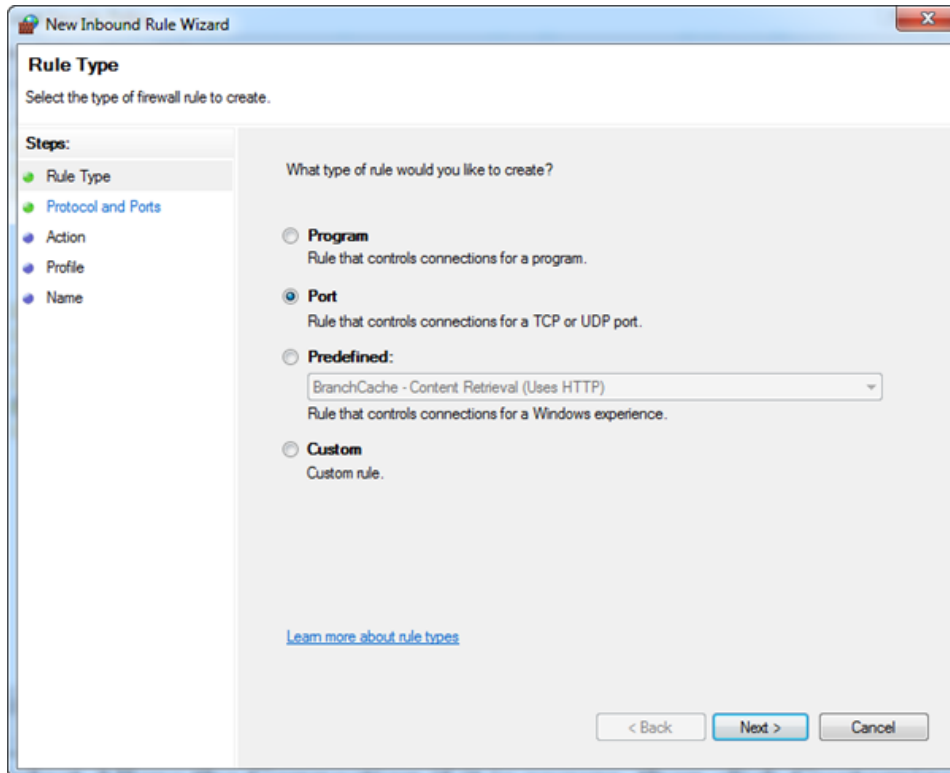
Rule Identification Name	File Path
netsightsrv	C:\Users\netsightsrv
netsightadmin	C:\Users\netsightadmin
netsightuser	C:\Users\netsightuser

Configuring RemoteApp Manager

1. From your desktop, select **Start > Administrative Tools > Server Manager > Roles > RemoteApp Manager**.
2. Right-click **RemoteApp Manager** and select **Add RemoteApp Programs**.
3. Click **Next**.
4. Select the following Apps:
Automated Security Manager
Console
Inventory Manager
NAC Manager
Policy Manager
5. Click **Next** and then **Finish**.
6. In the right column under **RemoteApp Programs**, perform the following steps for each program:
 1. Right-click the program and select **Create Windows Installer Package**.
 2. Click **Next** three times.
 3. Click **Finish**.
7. From your desktop, navigate to **C:\Program Files\Packaged Programs**.
8. Copy the MSI packages just created onto a USB drive or other storage medium.
9. Transfer and install MSI packages onto the Extreme Management Center client computer.

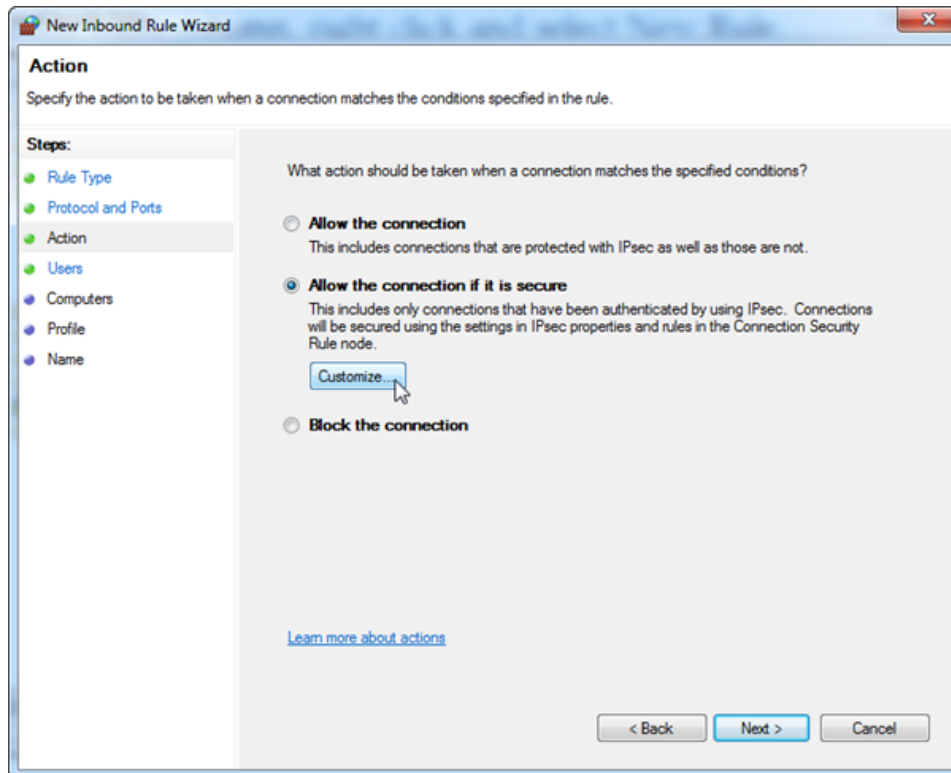
Windows Firewall Configuration

1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Windows Firewall with Advanced Security > (expand folder) > Inbound Rules**.
2. In the blank area, right-click and select **New Rule**.
The New Inbound Rule Wizard opens.



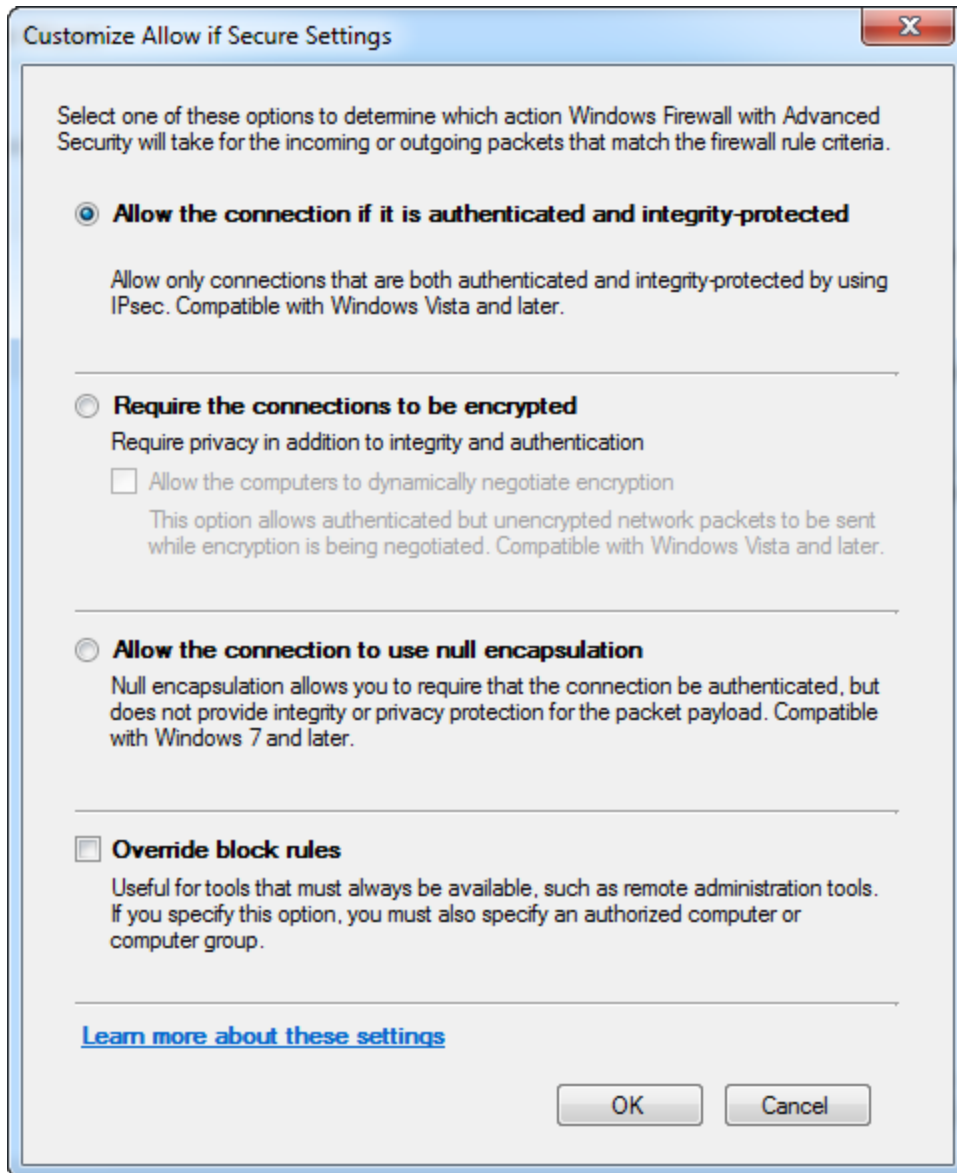
3. Select the **Port** option and then click **Next**.
4. If not already selected, choose the **TCP** option.
5. Type **135** in the **Specific local ports** field.
6. Click **Next**.

7. Select the second option, **Allow the Connection if it is secure**.



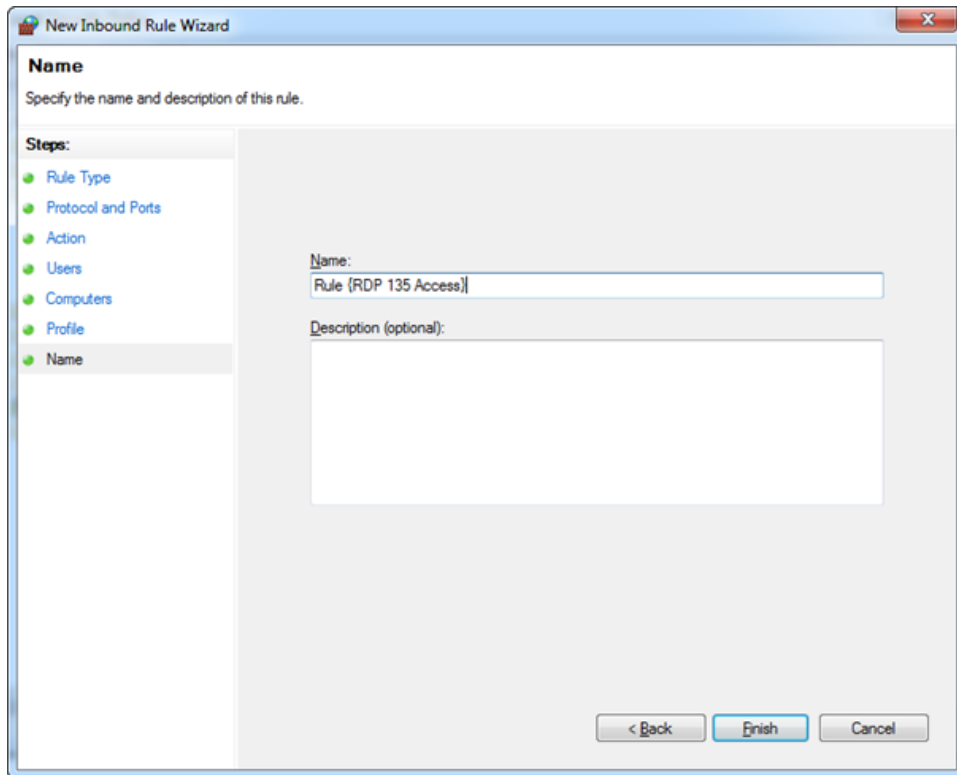
8. Click **Customize....**

9. Select **Allow the connection if it is authenticated and integrity-protected**.

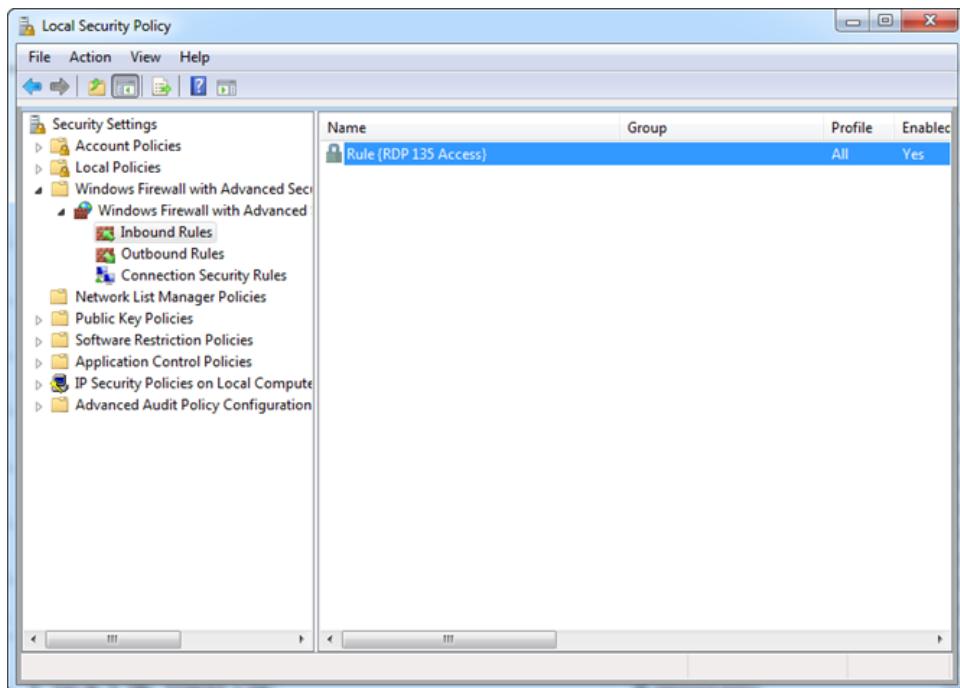


10. Click **OK** and then **Next** three times.
11. On the **Profile** page, leave **Domain**, **Private**, and **Public** selected, and then click **Next**.

12. In the **Name** field, type **RDP 135 Access**, and then click **Finish**.



The wizard closes and returns to the **Local Security Policy** window.



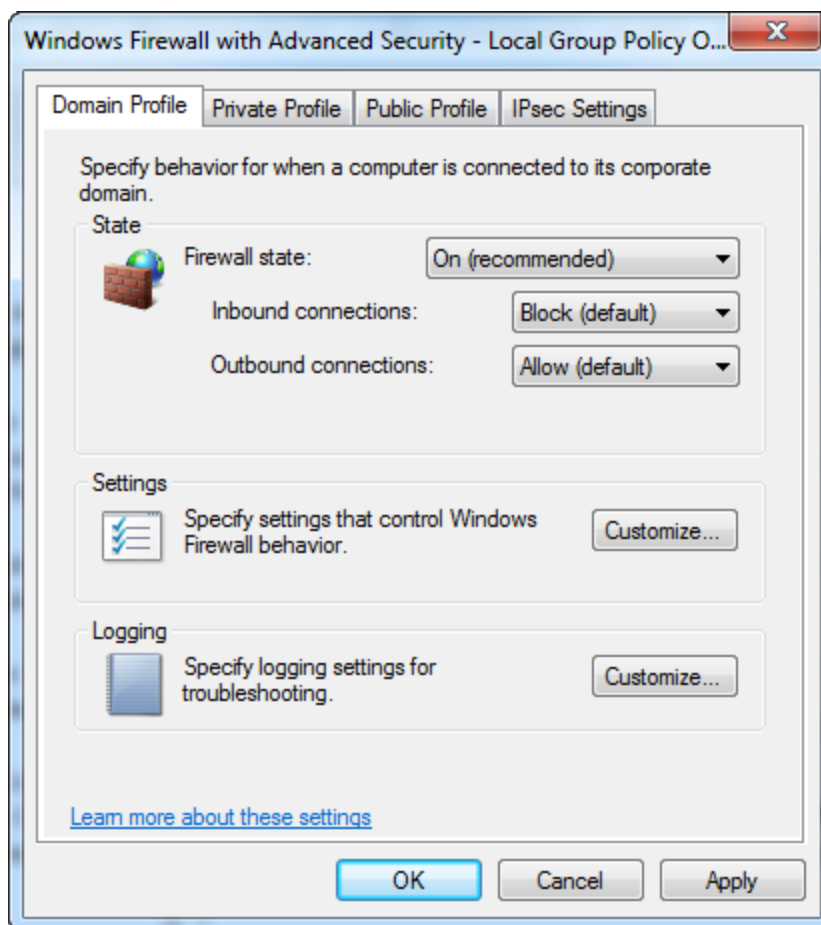
13. Repeat the preceding steps to create the following rules:

Port Type	Specific local port	Connection Type	Rule Name
TCP	3389	Allow the Connection if it is secure / Allow the connection if it is authenticated and integrity-protected	RDP 3389 Access
UDP	137	Allow the Connection	RDP UDP 137 Access
Custom	161	<ol style="list-style-type: none"> On the Protocols and Ports page, select the following options: <ul style="list-style-type: none"> Protocol type: UDP Local port: Specific Ports / 161 On the Scope page, select the following options: <ul style="list-style-type: none"> Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK Remote IP addresses: These IP addresses > Add > enter management IP and 64 bit mask of Management Subnet addresses [/64 or /24] > OK Select Allow the Connection. 	SNMP Access

Port Type	Specific local port	Connection Type	Rule Name
Custom	162	<ol style="list-style-type: none"> On the Protocols and Ports page, select the following options: <ul style="list-style-type: none"> Protocol type: UDP Local port: Specific Ports / 162 On the Scope page, select the following options: <ul style="list-style-type: none"> Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK Remote IP addresses: These IP addresses > Add > enter management IP and 64 bit mask of Management Subnet for router/switch [/64 or /24] > OK Select Allow the Connection. 	SNMP Trap
Custom	22	<ol style="list-style-type: none"> On the Protocols and Ports page, select the following options: <ul style="list-style-type: none"> Protocol type: TCP Local port: Specific Ports / 22 On the Scope page, select the following options: <ul style="list-style-type: none"> Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK Remote IP addresses: These IP addresses > Add > enter management IP address and 64 bit mask of management subnet for router/switch [/64 or /24] > OK Select Allow the Connection. 	SSH Access
UDP	514	Allow the Connection	Syslog UDP 514 Access

Configuring IPsec

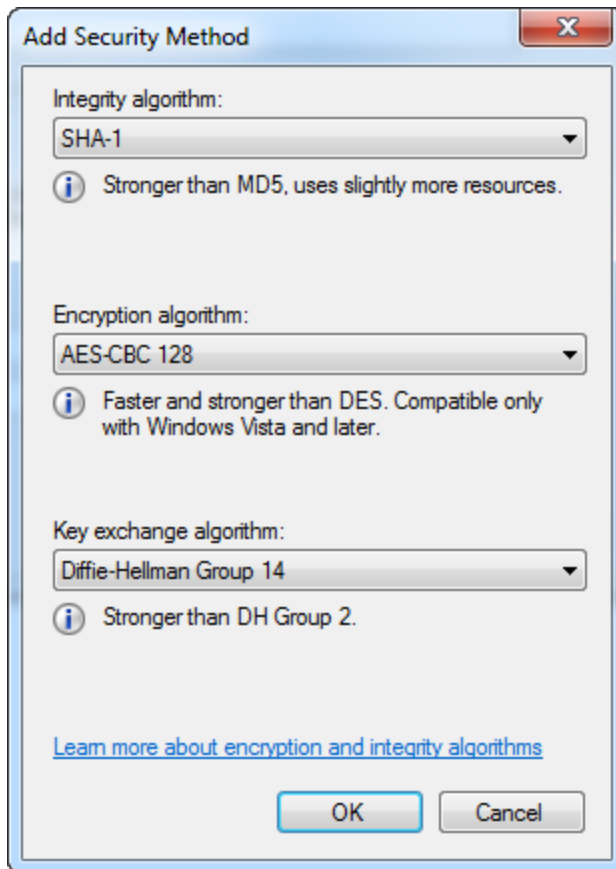
1. From your desktop, select **Start > Administrative Tools > Local Security Policy > Windows Firewall with Advanced Security**.
2. Right-click **Windows Firewall with Advanced Security - Local Group Policy Object** and select **Properties**.
3. From the **Domain Profile** tab, select **On** from the **Firewall state** drop-down list.
4. Select **Block** from the **Inbound connections** drop-down list.
5. Select **Allow** from the **Outbound connections** drop-down list.



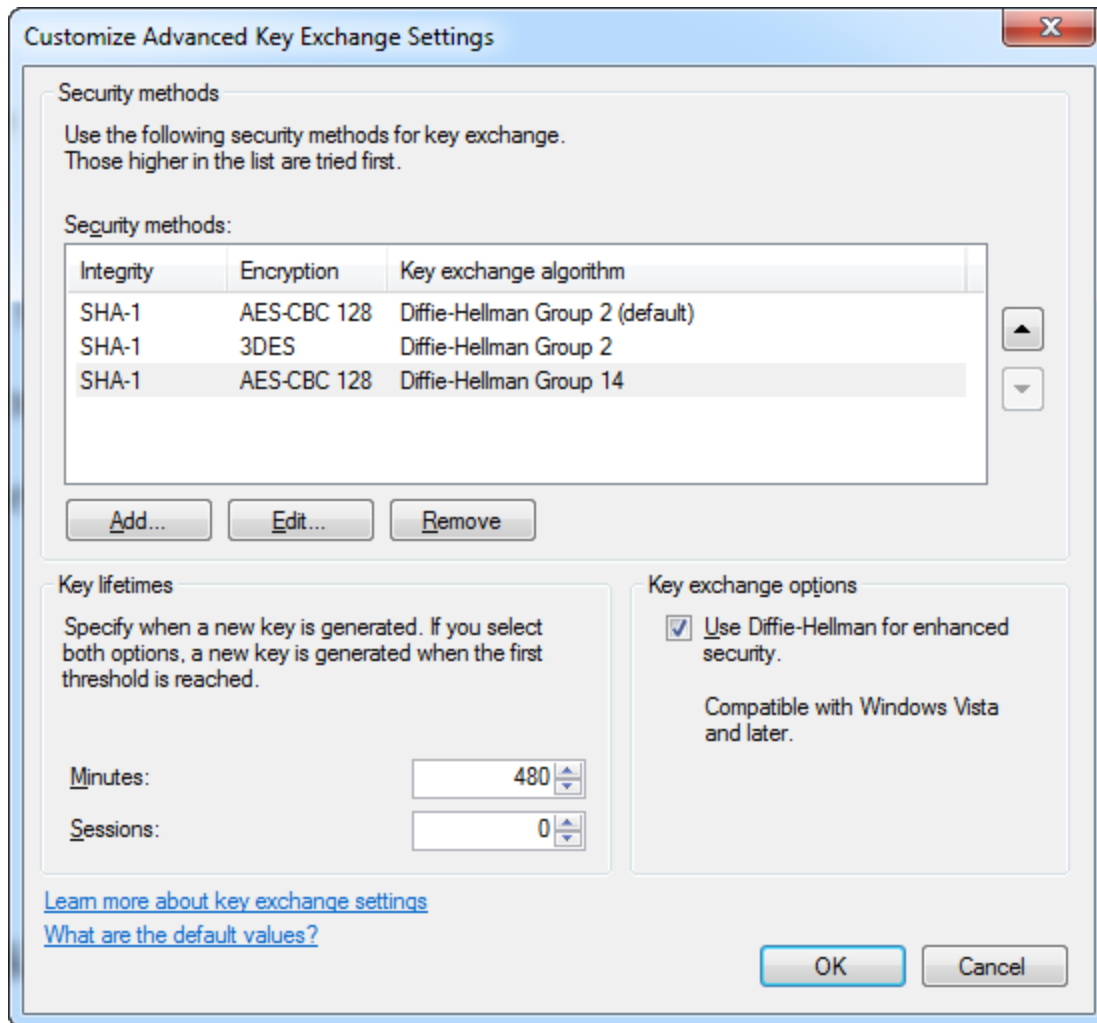
6. From the **IPsec Settings** tab, click **Customize...** in the **IPSec Defaults** area.
7. In the resulting dialog, select the **Advanced** radio button in the **Key exchange (Main Mode)** area.
8. Click **Customize....**

9. Click **Add**.
10. Ensure the following security methods are selected: **SHA-1** is selected in the drop-down list.

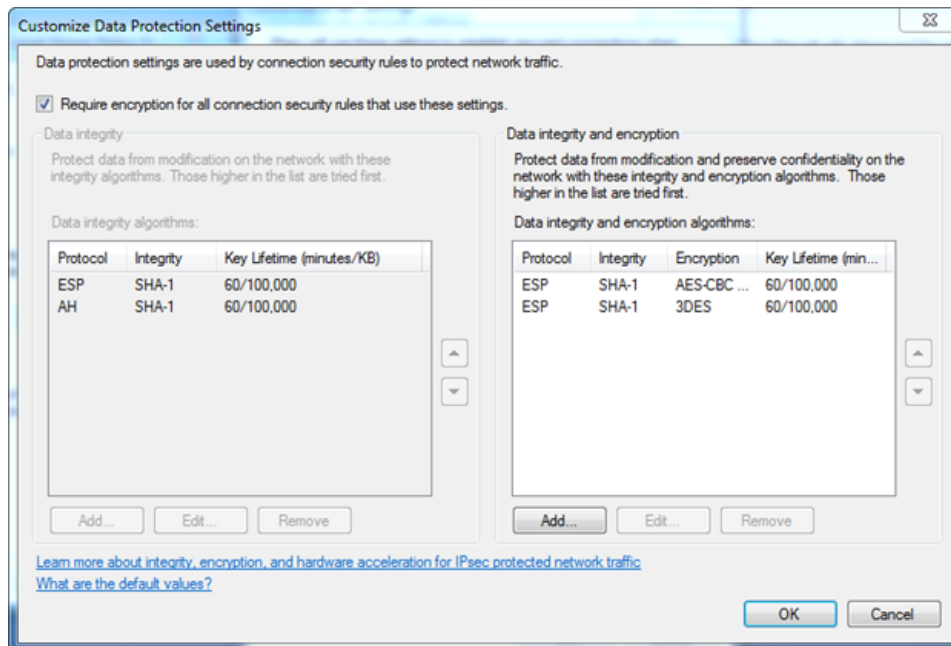
Drop-down List	Selection
Integrity algorithm	SHA-1
Encryption algorithm	AES-CBC 128
Key exchange algorithm	Diffie-Hellman Group 14



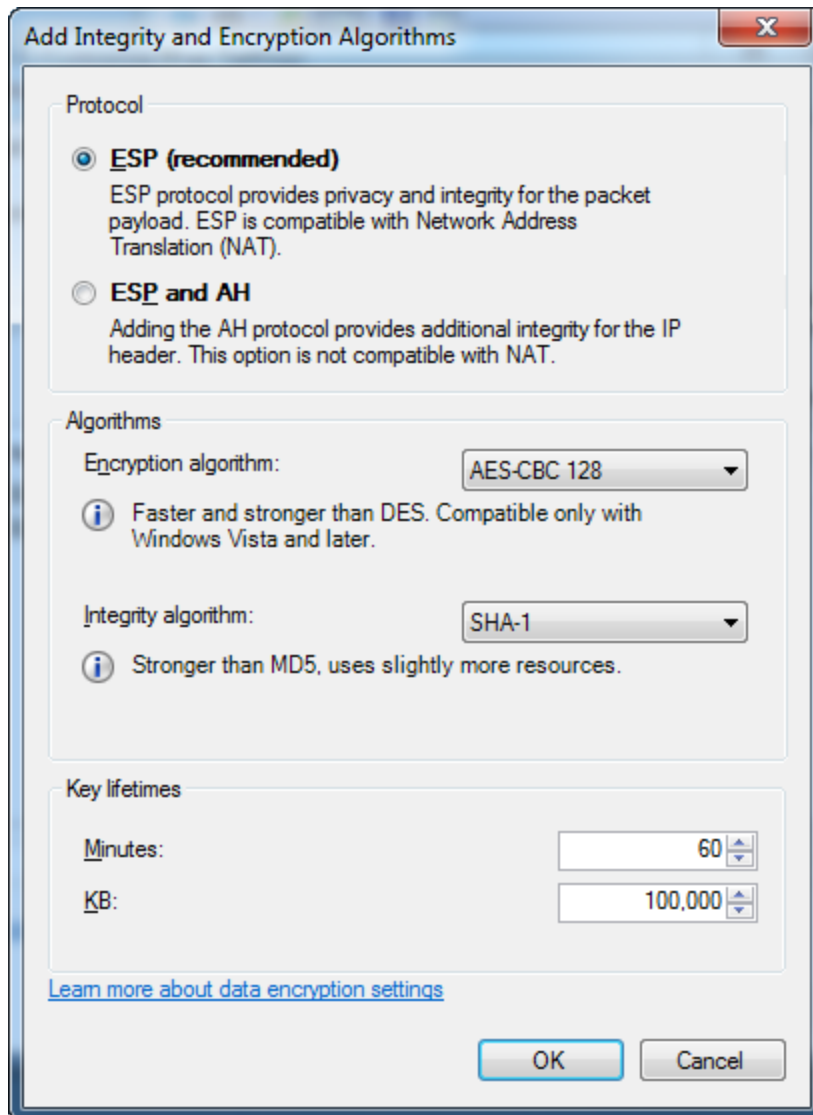
11. Click **OK** when finished.
12. Back on the **Customize Advanced Key Exchange Settings**, do the following:
 1. Enter **480** in the Minutes field (Key lifetimes area).
 2. Enter **0** in the Sessions field.
 3. Select the **Use Diffie-Hellman for enhanced security** checkbox.
 4. Click **OK**.



13. Select the **Advanced** radio button in the **Data protection (Quick Mode)** area.
14. Click **Customize...** and then **Add**.
15. Select the **Require encryption for all connection security rules that use these settings** checkbox.

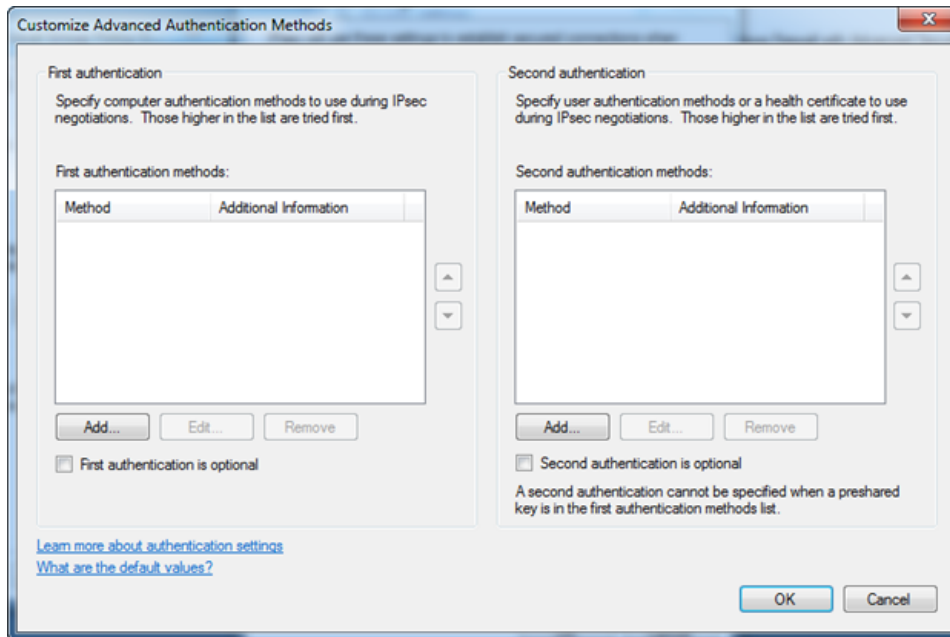


16. In the **Data integrity and encryption** area, click **Add**.
17. Select the following options:
Select ESP (recommended).
Choose **AES-CBC 128** from the **Encryption algorithm** drop-down list.
Choose **SHA-1** from the **Integrity algorithm** drop-down list.
In the **Key lifetimes** area, type **60** for Minutes and **100,000** for KB.

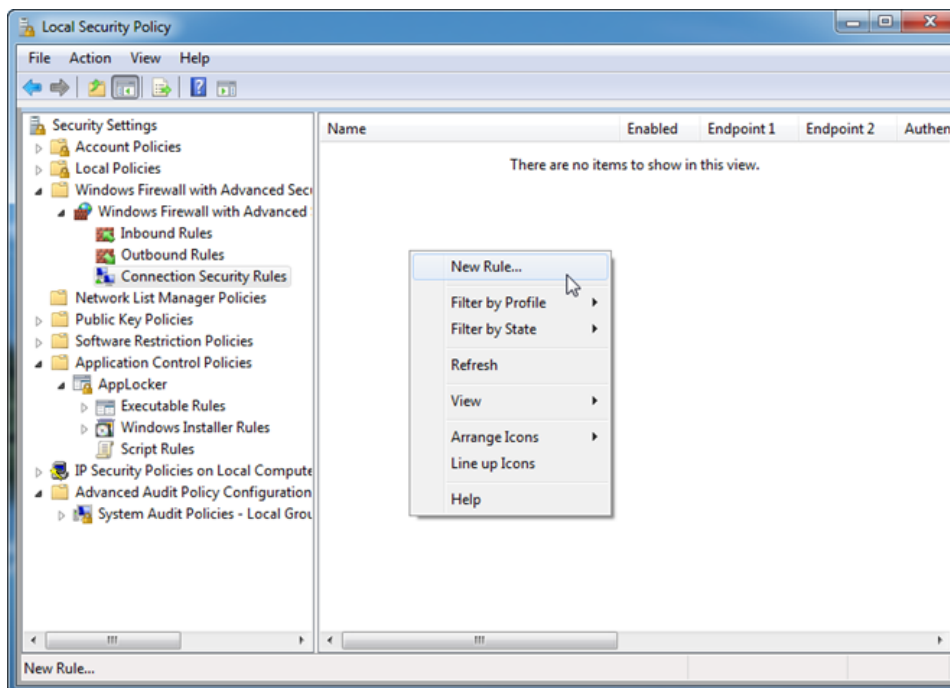


18. Click **OK** twice to exit.
19. Select **Advanced** for **Authentication method**, and then click **Customize**.
20. Click **Add**.

21. Ensure that the **First authentication is optional** is *not* selected, and then click OK.



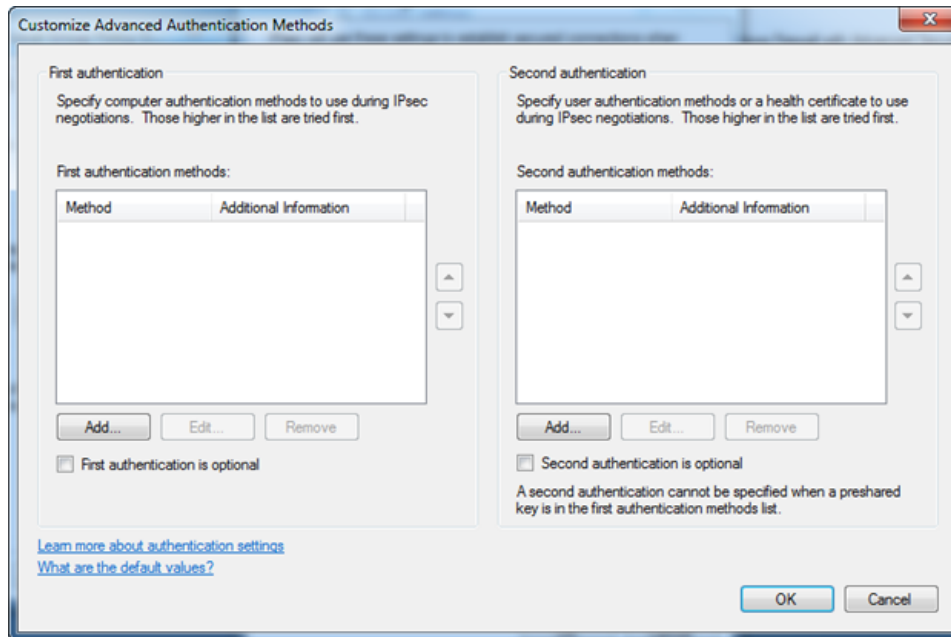
22. Click **OK** again to exit the **Customize IPsec Settings** dialog.
23. Select **None** from the **IPsec tunnel authorization** area, and click **OK** to exit.
24. Back in the **Local Security Policy** window, click **Connection Security Rules**.
25. In the blank area, right-click and select **New rule...**



The **New Connection Security Rule Wizard** opens.

26. Select **Custom** and then click **Next**.
27. For **Which computers are in Endpoint 1?**, choose **These IP address** and then click **Add....**
28. In the **This IP address or subnet**, type the IP address of NetSight server in
xxxx . xxxx . xxxx . xxxx format.
29. Click **OK**.
30. For **Which computers are in Endpoint 2?**, choose **These IP addresses** and click **Add**.
31. In the **This IP address or subnet**, type the IP address and 64-bit mask of Extreme Management Center client(s) in
xxxx . xxxx . xxxx . xxxx . xxxx . xxxx . xxxx . xxxx / 64 or
xxx . xxx . xxx . xxx / 24 format.
32. Click **OK** and then **Next**.
33. Select **Require authentication for inbound and outbound connections** (third option), and then click **Next**.
34. Select **Advanced** (fourth option), and then click **Customize....**
35. In the **First authentication** area, click **Add....**
36. Select **Preshared key**, and **Enter** .
37. Click **OK** to exit.

38. Ensure that the **First authentication is optional** is *not* selected, and then click **OK**.



39. Click **Next**.
40. On the **Protocols and Ports** page, select the following options:
Protocol type: Any
Endpoint 1 port: All Ports
Endpoint 2: All Ports
41. Click **Next**.
42. On the **Profile** page, leave **Domain**, **Private**, and **Public** selected, and then click **Next**.
43. On the **Name** page, enter the rule name and click **Finish**.
 You are returned to the **Local Security Policy** dialog. If the new rule is not enabled, right-click the rule and select **Enable rule**.
44. Repeat the above configure IPsec for the NetSight client, but reverse the Endpoint 1 and Endpoint 2 IP addresses.