

Extreme Management Center Secure Deployment Guide



Copyright © 2019 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: <u>support@extremenetworks.com</u>. To expedite your message, enter the product name or model number in the subject line.

- <u>GTAC Knowledge</u> Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- <u>The Hub</u> 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.
- <u>Support Portal</u> 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	14
Installing Extreme Management Center	18
Creating Extreme Management Center Users and Groups	18
Configuring Extreme Management Center	20
Configuring Extreme Management Center Services	20
Configuring Access Control of Extreme Management Center Directory	21
Encrypting the File System Service	22
Encrypting the File System of the Extreme Management Center mysql Directory	22
Configuring the Application Identity Service	23
Configuring Application Control Policies	23
Configuring AppLocker Executable Rules	23
Configuring AppLocker Script rule	29

Configuring RemoteApp Manager	
Windows Firewall Configuration	35
Configuring IPsec	41

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 <u>Configuring Extreme Management Center Users</u> 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 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

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



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.

Local Security Policy	1 Start > Administra	
File Action View Help		
🗢 🏟 🖄 📰 🔒 📓 🖬		
Security Settings Account Policies Account Policies Account Lockout Policy Account Lockout Policy Account Lockout Policy Audit Policy Audit Policy Security Options Windows Firewall with Advanced Security Network List Manager Policies Active Restriction Policies Application Control Policies Advanced Audit Policy Configuration Advanced Audit Policy Configuration	Policy	Security Setting Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure Success, Failure

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.

File Action View Help 	Policy	Security Setting	
← ➡ 2 □ ► I □	Policy	Security Setting	
h Security Settings	Policy	Security Setting	
 Account Policies Coal Policies Coal Policies User Rights Assignment Security Options Windows Firewall with Advanced Sect Network List Manager Policies Policic Key Policies Software Restriction Policies Application Control Policies S IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Accounts: Administrator account status Accounts: Limit local account status Accounts: Limit local account use of blank passwords to co Accounts: Rename guest account Accounts: Rename guest account Audit: Audit the access of global system objects Audit: Audit the use of Backup and Restore privilege Audit: Force audit policy subcategory settings (Windows Vis Audit: Shut down system immediately if unable to log secur DCOM: Machine Access Restrictions in Security Descriptor D DCOM: Machine Access Restrictions in Security Descriptor DCOM: Machine Launch Restrictions in Security Descriptor Devices: Allow undock without having to log on Devices: Restrict Dr.ROM access to locally logged-on user Devices: Restrict Dr.ROM access to locally logged-on user Devices: Restrict IDpy access to locally logged-on user Domain controller: LDAP server signing requirements Domain member: Digitally encrypt or sign secure channel d	Disabled Disabled Enabled xadministrator xguest Disabled Disabled Not Defined Disabled Not Defined Enabled Not Defined Disabled Not Defined Not Defined Enabled Enabled Enabled	<
< >	Domain member: Digitally sign secure channel data (when	Enabled Disabled	•

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

For this policy	Set to
Interactive logon: Message	Enter the following text:
text for users attempting to log on	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:
	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.
	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.
	This IS includes security measures (e.g., authentication and access controls) to protect USG interestsnot for your personal benefit or privacy.
	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.

For this policy	Set to
Interactive logon: Message	Enter the following text:
title for users attempting to log on	U.S. Government (USG) Information System (IS) that is provided for USG authorized use only.
System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing	Enable

Configuring Windows Users and Groups

Creating an Extreme Management Center User Group

- 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.

New Group	२ <mark>४</mark>
<u>G</u> roup name:	netsightusers
Description:	Users that are capable of using Netsight
Members:	
<u>A</u> dd	Remove
Help	Create

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

New User	? ×
User name:	netsightadmin
Full name:	
Description:	
Password:	•••••
Confirm password:	•••••
User must char	nge password at next logon
User cannot ch	hange password
Password neve	er expires
Account is disa	abled
Help	Create Close

- 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.

Select Groups	? ×
Select this object type:	
Groups	Object Types
From this location:	
CEFTEKHAR-PC	Locations
Enter the object names to select (examples):	
netsightusers; Remote Desktop Users	Check Names
Advanced	OK Cancel

- 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

- 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 <u>Configuring Extreme Management Center</u> <u>Users</u>]
- 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

- 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 <u>Configuring Extreme Management</u> <u>Center Users</u>.
- 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

- 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 Statrup 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

- 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

- From your desktop, select Start > Administrative Tools > Server Manager > Configuration > Services.
- 2. Right-click AppLocker and select Properties.
- 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.

x	? <mark>x</mark>		Select User or Group
			Select this object type:
	Object Types		User, Group, or Built-in security principal
			From this location:
	Locations		corp.extremenetworks.com
			Enter the object name to select (examples):
s	Check Names		netsightusers
	Cancel	OK	Advanced
S	Locations Check Names Cancel	ОК	corp.extremenetworks.com Enter the object name to select (examples): netsightusers Advanced

- 6. Click Check Names.
- 7. Click OK.

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

Create Executable Rules		x
Conditions		
Before You Begin Permissions Conditions Path Exceptions Name	 Select the type of primary condition that you would like to create. Publisher Select this option if the application you want to create the rule for is signed by the software publisher. Path Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule. File hash Select this option if you want to create a rule for an application that is not signed. 	
	More about rule conditions Create Create Cancel	

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

Create Script Rules		3
Path		
Before You Begin Permissions Conditions	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.	
Path Exceptions Name	Path: Browse Files Browse Folders	
	More about path rules and path variables	
	< Previous Next > Create Cancel	

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

Create Executable Rules		x
Name and De	scription	
Before You Begin Permissions Conditions	Enter a name to identify this rule.	
Path	Name:	
Exceptions	NetSight	
Name	Description: (Optional)	
	A A A A A A A A A A A A A A A A A A A	
	*	
	< Previous Next > Create Cancel	

The wizard closes and returns to the Local Security Policy.

Local Security Policy						
File Action View Help						
Security Settings	Action	Name		Condition	Exceptions	
Local Policies Windows Firewall with Advanced Sect Windows Firewall with Advanced Sect Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies Application Control Policies	Allow	recogn		Pour		
Cript Rules Cript Rules Script Rules Script Rules Script Rules Advanced Audit Policy Configuration						
< <u> </u>	•		m		Þ	

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.

x	? <mark>x</mark>		Select User or Group
			Select this object type:
	Object Types		User, Group, or Built-in security principal
			From this location:
	Locations		corp.extremenetworks.com
			Enter the object name to select (examples):
s	Check Names		netsightusers
	Cancel	OK	Advanced
S	Locations Check Names Cancel	ОК	corp.extremenetworks.com Enter the object name to select (examples): netsightusers Advanced

- 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.

Create Script Rules		×
Path		
Before You Begin Permissions Conditions Path Exceptions Name	Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.	
	More about path rules and path variables	
	< Previous Next > Create Cance	el

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

Create Executable Rules		×
Name and De	scription	
Before You Begin Permissions Conditions	Enter a name to identify this rule.	
Path	Name:	
Exceptions	NetSight	
Name	Description: (Optional)	
	A	
	< Previous Next > Create Cancel	

The wizard closes and returns to the Local Security Policy.

Local Security Policy						
File Action View Help						
♦ ⇒ 2						
Security Settings	Action	Name	Condition	Exceptions		
Local Policies Windows Firewall with Advanced Secu Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies Application Control Policies Mindows Installer Rules Script Rules Script Rules Advanced Audit Policy Configuration		recorgin				
< <u> </u>	۲			· · · ·		

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.
- 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.

P New Inbound Rule Wizard	×
Rule Type	
Select the type of firewall rule to c	reate.
Select the type of firewall rule to c Steps: Protocol and Ports Action Profile Name	reate. What type of rule would you like to create? Program Rule that controls connections for a program. Port Rule that controls connections for a TCP or UDP port. Predefined: BranchCache - Content Retrieval (Uses HTTP) Rule that controls connections for a Windows experience. Custom Custom Custom rule. Leam more about rule types
	< Back Next > Cancel

- 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.

istom	ize Allow if Secure Settings
Seleo Secu	t one of these options to determine which action Windows Firewall with Advanced rity will take for the incoming or outgoing packets that match the firewall rule criteria.
۲	Allow the connection if it is authenticated and integrity-protected
	Allow only connections that are both authenticated and integrity-protected by using IPsec. Compatible with Windows Vista and later.
0	Require the connections to be encrypted
	This option allows authenticated but unencrypted network packets to be sent while encryption is being negotiated. Compatible with Windows Vista and later.
0	Allow the connection to use null encapsulation Null encapsulation allows you to require that the connection be authenticated, but does not provide integrity or privacy protection for the packet payload. Compatible with Windows 7 and later.
	Override block rules Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or
Le	computer group.
	OK Cancel

- 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.

Prev Inbound Rule Wizard		x
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Protocol and Ports		
Action		
Users	Name:	
Computers	NUE (NDF 135 Access)	
Profile	Description (optional):	
Name		
	< Back Enish Cancel	

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



Port Type	Specific local port	Connection Type	Rule Name
ТСР	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
		 On the Protocols and Ports page, select the following options: 	
		 Protocol type: UDP 	
		 Local port: Specific Ports / 161 	
		2. On the Scope page, select the following options:	
Custom	161	 Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK 	SNMP Access
		 Remote IP addresses: These IP addresses > Add > enter management IP and 64 bit mask of Management Subnet addresses [/64 or /24] > OK 	
		3. Select Allow the Connection.	

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

Port Type	Specific local port	Connection Type	Rule Name
		 On the Protocols and Ports page, select the following options: 	
		Protocol type: UDP	
		• Local port: Specific Ports / 162	
Custom		2. On the Scope page, select the following options:	
Custom	162	 Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK 	SNMP Trap
		 Remote IP addresses: These IP addresses > Add > enter management IP and 64 bit mask of Management Subnet for router/switch [/64 or /24] > OK 	
		3. Select Allow the Connection.	
		 On the Protocols and Ports page, select the following options: 	
		Protocol type: TCP	
		Local port: Specific Ports / 22	
		2. On the Scope page, select the following options:	
Custom	22	 Local IP addresses: These IP addresses > Add > enter ECC server address [/64 or /24] > OK 	SSH Access
		 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 	
		3. Select Allow the Connection.	
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.

Windows Firew	all with Advanced Secu	urity - Lo	ocal Group Policy O				
Domain Profile	Private Profile Public	Profile	IPsec Settings				
Specify beh domain. State	Specify behavior for when a computer is connected to its corporate domain.						
	Firewall state:	On (rec	ommended) 🔻				
	Inbound connections:		Block (default)				
	Outbound connections): 	Allow (default)				
Settings	Specify settings that cont Firewall behavior.	rol Windo	ows Customize				
Logging Specify logging settings for troubleshooting.							
Learn more a	about these settings						
	ОК		Cancel Apply				

- 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 dropdown 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 **O** in the Sessions field.
 - 3. Select the Use Diffie-Hellman for enhanced security checkbox.
 - 4. Click OK.

ollowing securi oher in the list a	y methods for key exchange. re tried first.	
nethods: Encr	ption Key exchange algorit	m
AES- 3DES AES-	CBC 128 Diffie-Hellman Group Diffie-Hellman Group CBC 128 Diffie-Hellman Group	2 (default) 2 14
	lit	Key exchange options
hen a new key ons, a new key is reached.	is generated. If you select is generated when the first	Use Diffie-Hellman for enhanced security. Compatible with Windows Vista
	480 丈	and later.
hen a new ke ns, a new key is reached.	r is generated. If you select is generated when the first 480 - 0 -	Use Diffie-Hellman for enhand security. Compatible with Windows Viand later.

- 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.

Data protection settings are used by connection security rules to protect network traffic. Image: Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first. Data integrity algorithms: Protocol integrity Key Lifetime (minutes/KB) ESP SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Add Ear integrity encryption, and hardware acceleration for IPsec protected network traffic. What are the default values?	tomize Dat	a Protection	Settings				_		23
 Require encryption for all connection security rules that use these settings. Data integrity Protect data from modification and preserve confidentiality on the network with these integrity algorithms. Those higher in the list are tried first. Data integrity algorithms: Protocol Integrity Key Lifetime (minutes/KB) ESP SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Learn more about integrity, encryption, and hardware acceleration for IPsec protected network traffic What are the default values? 	ata protectio	on settings are	used by connection security rules	to protect net	twork traffic.				
Data integrity Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first. Data integrity algorithms: Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first. Data integrity algorithms: Protocol Integrity Encryption algorithms: Protocol Integrity Key Lifetime (minutes/KB) ESP ESP SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Learn more about integrity, encryption, and hardware acceleration for IPsec protected network traffic What are the default values?	Require e	ncryption for a	all connection security rules that us	e these settin	gs.				
Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first. Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first. Data integrity algorithms: Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first. Data integrity algorithms: Protocol ESP SHA-1 60/100.000 SHA-1 AH SHA-1 60/100.000 SHA-1 Add Edt Remove Add Learn more about integrity, encryption, and hardware acceleration for IPsec protected network traffic What are the default values?	Data integrity	y			Data integrity	and encrypt	tion		
Data integrity algorithms: Data integrity and encryption algorithms: Protocol Integrity Key Lifetime (minutes/KB) Protocol Integrity Encryption Key Lifetime (min ESP SHA-1 60/100,000 SHA-1 AES-CBC 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Add Eatern more about integrity, encryption, and hardware acceleration for IPsec protected network traffic What are the default values?	Protect data integrity alg	a from modific orithms. Thos	ation on the network with these e higher in the list are tried first.		Protect data network with higher in the	a from modifie h these integ e list are tried	cation and prese rity and encrypt I first.	erve confidentiality on t ion algorithms. Those	the
Protocol Integrity Key Lifetime (minutes/KB) ESP SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Add Edt Remove .eam more about integrity.encryption. and hardware acceleration for IPsec protected network traffic What are the default values?	Data integri	ity algorithms:			Data integri	ty and encry	ption algorithms:	:	
ESP SHA-1 60/100,000 AH SHA-1 60/100,000 AH SHA-1 60/100,000 Add Edt Remove Add Edt Remove Add Edt Remove Add Edt Remove	Protocol	Integrity	Key Lifetime (minutes/KB)		Protocol	Integrity	Encryption	Key Lifetime (min	
Add Edt Remove Add Edt Remove Add Edt Remove Add Edt Remove	ESP AH	SHA-1 SHA-1	60/100,000 60/100,000		ESP ESP	SHA-1 SHA-1	AES-CBC 3DES	60/100,000 60/100,000	
Add Edt Remove Add Edt Remove Add Edt Remove Add Edt Remove				•					*
eam more about integrity, encryption, and hardware acceleration for IPsec protected network traffic /hat are the default values?	Add	Edi	t Remove		Add	Ec	it	emove	
	earn more ab	default values	encryption, and hardware accelera	tion for IPsec	protected netw	ork traffic			
OK Cancel		Sectore Toloco	<u>er</u>				ſ	OK Ca	ncel

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.

Add Integrity and Encryption Algorithms	×							
Protocol								
ESP (recommended) ESP protocol provides privacy and in payload. ESP is compatible with Netro	itegrity for the packet work Address							
Translation (NAT). ESP and AH Adding the AH protocol provides add header. This option is not compatible	Translation (NAT). ESP and AH Adding the AH protocol provides additional integrity for the IP header. This option is not compatible with NAT.							
Algorithms								
Encryption algorithm:	AES-CBC 128 -							
 Faster and stronger than DES. C Windows Vista and later. 	Faster and stronger than DES. Compatible only with Windows Vista and later.							
Integrity algorithm:	SHA-1							
 Stronger than MD5, uses slightly 	more resources.							
Key lifetimes								
<u>M</u> inutes:	60 牵							
<u>K</u> B:	100,000							
Learn more about data encryption settings								
	OK Cancel							

- 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.

First authentication Specify computer negotiations. Tho	authentication methods to use during IPsec se higher in the list are tried first.		Second authenticat Specify user authe during IPsec nego Second authentica	ion ntication methods or a health certifica sations. Those higher in the list are tri stion methods:	te to use ed first.
Method	Additional Information		Method	Additional Information	
		•			•
Add	Edit Remove		Add	Edit Remove	
Hirst authentic	ation is optional		A second authenti key is in the first au	nucation is optional cation cannot be specified when a pro thentication methods list.	eshared
eam more about aut fhat are the default	hentication settings values?			ок	Cancel

- 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 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.xxx.xxx./64 or 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**.

First authentication Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first. First authentication methods:		Second authentication Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first. Second authentication methods:
Method	Additional Information	Method Additional Information
Add	Edit Remove	Add Edit Remove
First authentic	ation is optional	Second authentication is optional
		A second authentication cannot be specified when a preshared key is in the first authentication methods list.
	thentication settings	

- 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.