NetSight Secure Deployment Guide

This document describes how to install NetSight securely on a Windows 2008R2 server. Included in this document are instructions on how to configure the security features of the Windows 2008R2 server to ensure the security of the NetSight application.

Following the procedures in this document makes the NetSight installation STIG (Security Technical Implementation Guide)-compliant.

1.1 Pre-Installation Information

1.1.1 Installation Prerequisites

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

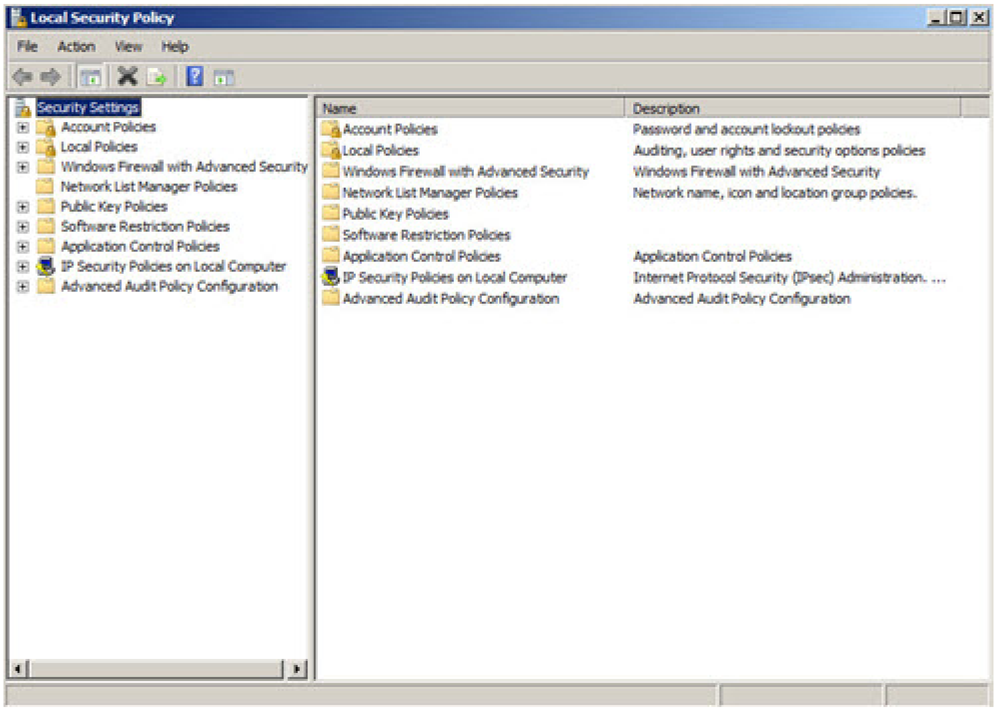
1.1.2 User Accounts

In the procedures in this document, the user names listed below are used. 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** — NetSight server administrator with full Remote Desktop privileges
- **netsightadmin** — NetSight administrator with only NetSight Remote Desktop privileges
- **netsightuser** — NetSight user with only NetSight Remote Desktop privileges
- **xadministrator** — non-default server administrator
- **xguest** — non-default guest account

1.2 Configuring Server Account Settings to be STIG-Compliant

Figure 1-1 Local Security Policy Security Settings Window



- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administration. ...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

1.2.1 Set the Password Policy

1. Start > Administrative Tools > Local Security Policy > Account Policies > Password Policy
2. In the right column, double click **Enforce password history**. In the pop-up window, set the **Password Remembered:** field to 10 passwords remembered, then click OK.
3. In the right column, double click **Maximum password age**. In the pop-up window, set the **Password expiration:** to 90 days, then click OK.
4. In the right column, double click **Minimum password age**. In the pop-up window, set the **Password can be changed after:** field to 1 days, then click OK.
5. In the right column, double click **Minimum password length**. In the pop-up window, set the **Password must be at least:** field to 14 characters, then click OK.
6. In the right column, double click **Password must meet complexity requirements**. In the pop-up window, select **Enabled**, then click OK.
7. In the right column, double click **Store passwords using reversible encryption**. In the pop-up window, select **Disabled**, then click OK.

1.2.2 Set the Account Lockout Policy

1. Start > Administrative Tools > Local Security Policy > Account Policies > Account Lockout Policy

2. In the right column, double click **Account lockout duration.** In the pop-up window, set the **Account is locked out for:** field to 1 minute, then click OK.
3. In the right column, double click **Account lockout threshold**. In the pop-up window, set the **Account will lock out after:** field to 3 invalid logon attempts, then click OK.
4. In the right column, double click **Reset account lockout counter after**. In the pop-up window, set the **Reset account lockout counter after:** field to 1 minute, then click OK.

1.2.3 Set the Audit Policy

1. Start > Administrative Tools > Local Security Policy > Local Policies > Audit Policy
2. In the right column, double click **Audit account logon events**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
3. In the right column, double click **Audit account management**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
4. In the right column, double click **Audit directory service access**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
5. In the right column double click **Audit logon events**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
6. In the right column double click **Audit object access**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
7. On the right column double click **Audit policy change**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
8. In the right column double click **Audit privilege user**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
9. In the right column double click **Audit process tracking.** In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.
10. In the right column double click **Audit system events**. In the pop-up window, enable **Success** and enable **Failure** under **Audit these attempts**, then click OK.

1.2.4 Set the Security Options

1. Start > Administrative Tools > Local Security Policy > Local Policies > Security Options
2. In the right column, double click **Accounts: Rename administrator account**. In the pop-up window, set the field to “xadministrator,” then click OK.
3. In the right column, double click **Accounts: Rename guest account.** In the pop-up window, set the field to “xguest,” then click OK.
4. In the right column, double click **Interactive logon: Message text for users attempting to log on**. In the pop-up window, set the field to the following text:

   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 interests--not 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.

5. In the right column, double click **Interactive logon: Message title for users attempting to log on**. In the pop-up window, set the field to the following text:

   U.S. Government (USG) Information System (IS) that is provided for USG authorized use only.

6. In the right column, double click **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing**. In the pop-up window, select **Enable**.

1.3 Configuring Windows Users and Groups

1.3.1 Create a NetSight Users Group

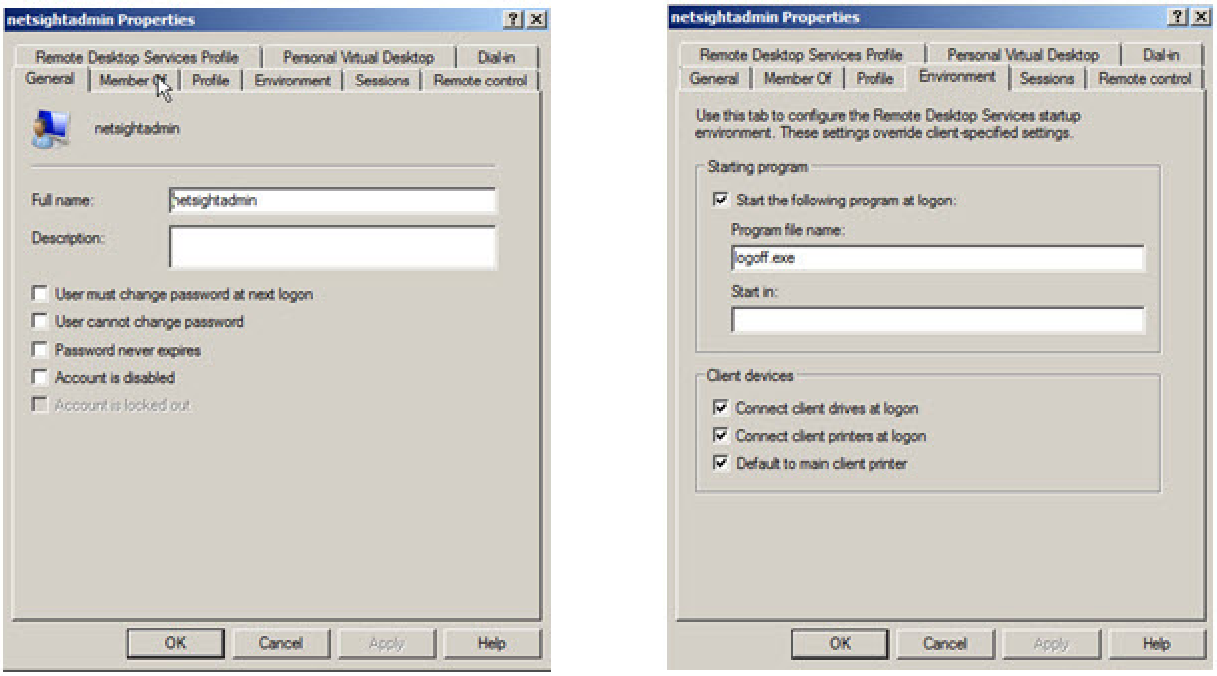
1. Start > Administrative Tools > Server Manager > Local users and Groups > Groups
2. In the right column, right click and select **New Group**, then fill out the following fields as shown:
   a. Group name: netsightusers
   b. Description: Users that are capable of using Netsight
3. Click Create.

1.3.2 Configure NetSight Users

1. Start > Administrative Tools > Server Manager > Local users and Groups > Users
2. In the right column, right click and select **New User,** then fill out the following fields as shown:
   a. User name: netsightadmin
   b. Password: [User defined password]
   c. Confirm password: [User defined password]
3. Click Create.
4. In the right column, double click **netsightadmin**.
5. Select the **Member of** tab, then click **Add** to add the following groups
   a. netsightusers
   b. Users
   c. Remote Desktop Users
6. Remove all other groups by selecting the group, then click **Remove.**
7. Select the **Environment** tab.

8. Enable **Start the following program at logon,** then fill out the following fields:
    a. Program file name: logoff.exe
9. Click OK.
10. In the right column, right click and select **New User**, then fill out the following fields as shown:
    a. User name: netsightuser
    b. Password: [User defined password]
    c. Confirm password: [User defined password]
11. Click Create.
12. In the right column, double click **netsightuser.**
13. Select the **Member of** tab, then click **Add** to add the following groups:
    a. netsightusers
    b. users
    c. Remote Desktop Users
14. Remove all other groups by selecting the group, then click **Remove.**
15. Select the **Environment** tab.
16. Enable **Start the following program at logon,** then fill out the following fields:
    a. Program file name: logoff.exe
17. Click OK.
18. In the right column, right click and select **New User**, then fill out the following fields as shown:
    a. User name: netsightsrv
    b. Password: [User defined password]
    c. Confirm password: [User defined password]
19. Click Create
20. In the Right Column, double click **netsightsrv**
21. Select the **Member of** tab, then click **Add** to add the following groups:
    a. netsightusers
    b. Administrators
22. Remove all other groups by selecting the group, then click **Remove**
23. Click OK.

Figure 1-2 Configuring New Users Properties



netsightadmin Properties

Remote Desktop Services Profile | Personal Virtual Desktop | Dial-in
General | Member Of | Profile | Environment | Sessions | Remote control

netsightadmin

Full name: netsightadmin

Description:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled
□ Account is locked out

netsightadmin Properties

Remote Desktop Services Profile | Personal Virtual Desktop | Dial-in
General | Member Of | Profile | Environment | Sessions | Remote control

Use this tab to configure the Remote Desktop Services startup environment. These settings override client-specified settings.

Starting program

☑ Start the following program at logon:

Program file name: logoff.exe

Start in:

Client devices

☑ Connect client drives at logon
☑ Connect client printers at logon
☑ Default to main client printer

1.4 Installing NetSight

Note: To do the following steps, you must be logged in as "netsightsrv."

1. Initiate the NetSight install by double clicking the install package via the EXE file or install via DVD Media.
2. In the Install GUI Welcome Screen, click **Next**.
3. Select **I accept the terms of the License Agreement**, then click Next.
4. Enter your NetSight Product License, then click Next.
5. Click Next.
6. Unselect TFTP and BOOTP.
7. Click Next.
8. Change the Install Folder to the following: C:\Enterasys Networks\NetSight
9. Click Next.
10. If the folder does not exist, click OK to create folder when prompted.
11. Wait until the following status is shown:

    Server is ready for connections
12. Click Finish.

1.5 Creating NetSight Users and Groups

1. Start > All Programs > Enterasys Networks > NetSight > Clients > Console

2. When prompted to login, use the following credentials:
    a. Server: localhost
    b. Username: netsightsrv
    c. Password: [User defined password]
3. Click OK.
4. Go to Tools > Authorization/Device Access.
5. Click **Add Group** and fill out the following fields:
    a. Authorization Group name: netsightuser
    b. Membership Criteria: basic netsight capabilities
6. Select the **Capabilities** tab.
7. Select or unselect the user's capabilities depending on the user's privileges.
8. Click **Apply.**
9. Click **Add Group** and fill out the following fields:
    a. Authorization Group name: netsightadmin
    b. Membership Criteria: admin netsight capabilities
10. Select the **Capabilities** tab.
11. Select or unselect the user's capabilities depending on the user's privileges.
12. Click **Apply.**
13. Click **Close.**
14. Click **Add User** and fill out the following fields:
    a. User name: netsightuser
    b. Domain/Host name: localhost
    c. Authorization group: netsightuser
15. Click **Apply.**
16. Click **Add User** and fill out the following fields:
    a. User name: netsightadmin
    b. Domain/Host name: localhost
    c. Authorization group: netsightadmin
17. Click **Apply.**
18. Click **Close.**
19. Exit out of Netsight Console Program.

1.6 Configuring NetSight Services

1. Start > Administrative Tools > Server Manager > Configuration > Services
2. In the right column, double click NetSight BootP Service

3. Under the General tab, change the Startup type field to Disabled.
4. Select the Log On tab.
5. Enable This account.
6. Click Browse.
7. Fill in the following field as shown:

   Enter the object name to select: netsightsrv
8. Click Check Names.
9. Click OK.
10. Fill in the following fields as shown:
    a. Password: [User defined password]
    b. Confirm password: [User defined password]
11. Click OK.
12. In the right column, double click NetSight Database Service.
13. Under the General tab, change the Startup type field to Automatic.
14. Select the Log On tab.
15. Enable This account.
16. Click Browse.
17. Fill in the following field as shown:

    Enter the object name to select: netsightsrv
18. Click Check Names.
19. Click OK.
20. Fill in the following fields as shown:
    a. Password: [User defined password]
    b. Confirm password: [User defined password]
21. Click OK.
22. In the right column, double click NetSight Server Service.
23. Under the General tab, change the Startup type field to Automatic.
24. Select the Log On tab.
25. Enable This account.
26. Click Browse.
27. Fill in the following field as shown:

    Enter the object name to select: netsightsrv
28. Click Check Names.
29. Click OK.
30. Fill in the following fields as shown:

    a. Password: [User defined password]
    b. Confirm password: [User defined password]

31. Click OK.
32. In the right column, double click NetSight SNMP Trap Service.
33. Under the General tab, change the Startup type field to Automatic.
34. Select the Log On tab.
35. Enable This account.
36. Click Browse.
37. Fill in the following field as shown:

    Enter the object name to select: netsightsrv

38. Click Check Names.
39. Click OK.
40. Fill in the following fields as shown:
    a. Password: [User defined password]
    b. Confirm password: [User defined password]
41. Click OK.
42. In the right column, double click NetSight Syslog Service.
43. Under the General tab, change the Startup type field to Automatic.
44. Select the Log On tab.
45. Enable This account.
46. Click Browse.
47. Fill in the following field as shown:

    Enter the object name to select: netsightsrv

48. Click Check Names.
49. Click OK.
50. Fill in the following fields as shown:
    a. Password: [User defined password]
    b. Confirm password: [User defined password]
51. Click OK.
52. In the right column, double click NetSight TFTP Service.
53. Under the General tab, change the Startup type field to Disabled.
54. Select the Log On tab.
55. Enable This account.
56. Click Browse.
57. Fill in the following field as shown:

Enter the object name to select: netsightsrv

58. Click Check Names.

59. Click OK.

60. Fill in the following fields as shown:

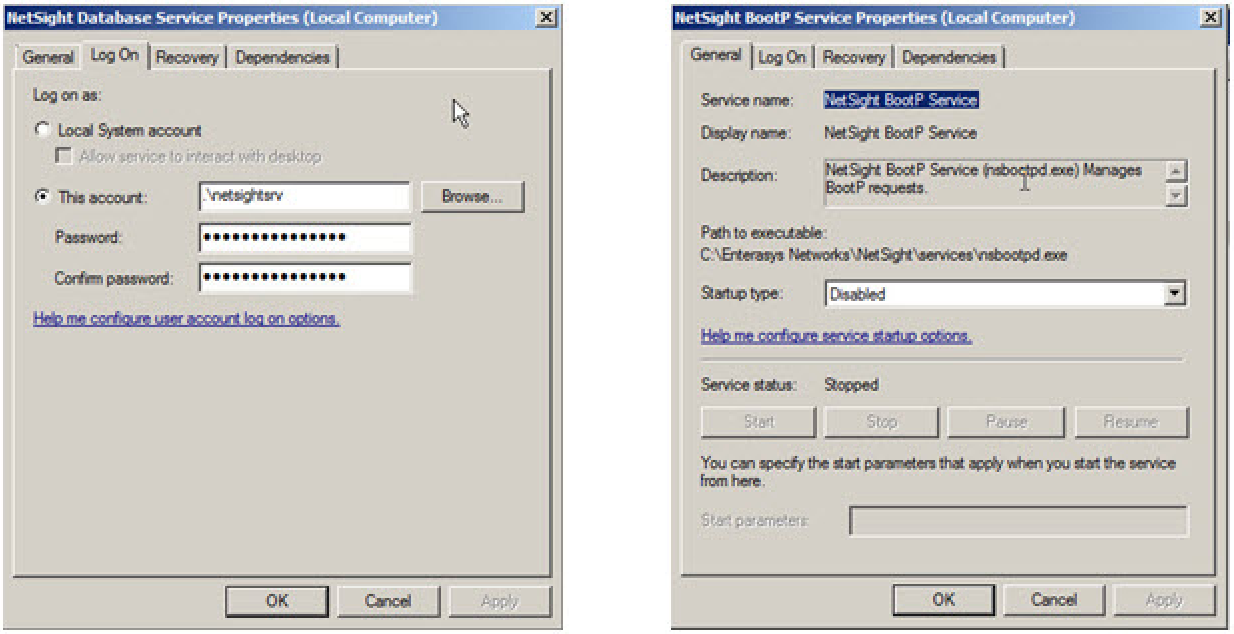
    a. Password: [User defined password]

    b. Confirm password: [User defined password]

61. Click OK.

62. Restart the computer and re-login as netsightsrv.

Figure 1-3 Configuring NetSight Services



NetSight Database Service Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: .\netsightsrv

Password: •••••••••••••••

Confirm password: •••••••••••••••

Help me configure user account log on options.

NetSight BootP Service Properties (Local Computer)

Service name: NetSight BootP Service

Display name: NetSight BootP Service

Description: NetSight BootP Service (nsbootpd.exe) Manages BootP requests.

Path to executable:
C:\Enterasys Networks\NetSight\services\nsbootpd.exe

Startup type: Disabled

Help me configure service startup options.

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

1.7 Configuring Access Control of NetSight Directory

1. Start > Computer
2. Go into the following directory, C:\
3. Right click the directory named Enterasys Networks.
4. Select Properties.
5. Select Security Tab.
6. Select Advanced.
7. Select Change Permissions.
8. Unselect Include inheritable permissions from this object's parent.
9. Click Add.
10. Select Replace all child object permissions with inheritable permissions from this object.

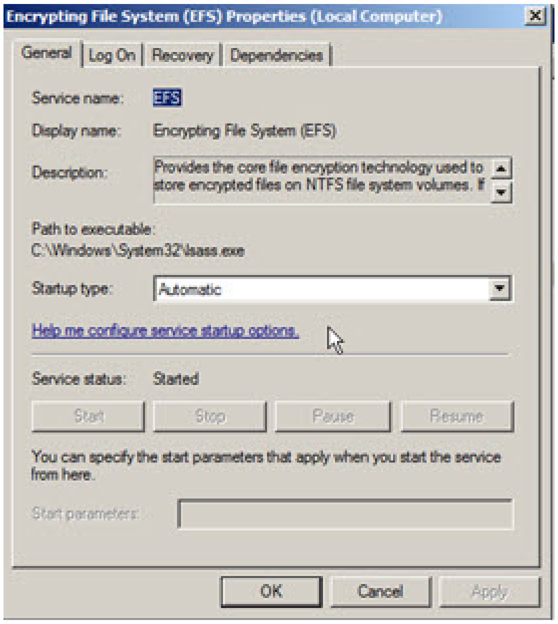
11. Click Add.
12. Fill in the following field as shown:

    Enter the object name to select: netsightusers
13. Click Check Names.
14. Click OK.
15. Select Allow for the following permissions:
    a. Traverse folder / execute file
    b. List folder / read data
    c. Read attributes
    d. Read extended attributes
    e. Create files / write data
    f. Create folders / append data
    g. Write attributes
    h. Write extended attributes
    i. Read permissions
16. Select Apply these permissions to objects and/or containers within this container only.
17. Click OK.
18. Click on Users (NETSIGHT-1\Users).
19. Select Remove.
20. Click on Users (NETSIGHT-1\Users).
21. Click Remove.
22. Click OK.
23. Click Yes.
24. Click OK.
25. Click OK.

1.8 Encrypting the File System Service

1. Start > Administrative Tools > Server Manager > Configuration > Services
2. In the right column, double click Encrypting File System (EFS).
3. Under the General tab, change the Startup type field to Automatic.
4. Click Start.
5. Once the service has started, click OK.

Figure 1-4 Encrypting the File System Service


Encrypting File System (EFS) Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
Start parameters:
OK
Cancel
Apply

Service name: EFS

Display name: Encrypting File System (EFS)

Description: Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If

Path to executable:
C:\Windows\System32\lsass.exe

Startup type: Automatic

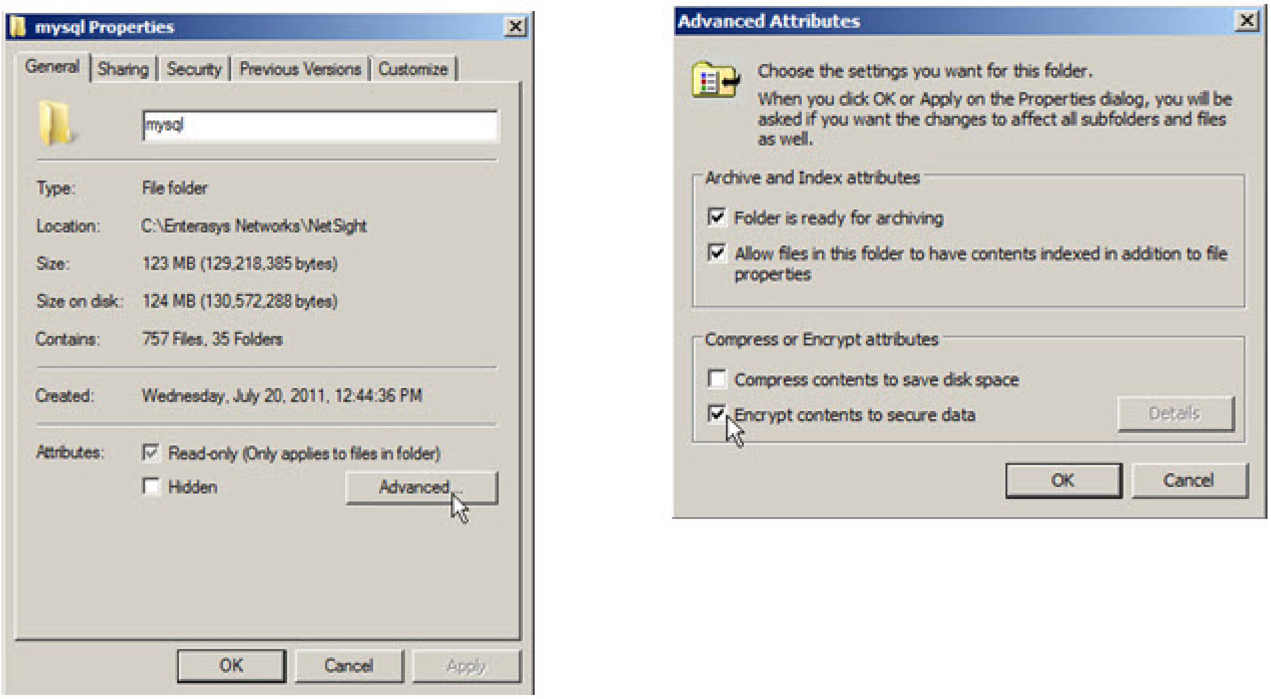
Service status: Started

You can specify the start parameters that apply when you start the service from here.

1.9 Encrypting the File System of the NetSight mysql Directory

1. Start > Administrative Tools > Server Manager > Configuration > Services
2. In the right column, double click NetSight Database Service.
3. Under the General tab, click Stop.
4. Once the Service has stopped, click OK.
5. Start > Computer
6. Go to the following directory, C:\Enterasys Networks\NetSight.
7. Right click on the directory called mysql.
8. Select Properties.
9. Click Advanced.
10. Select Encrypt contents to secure data.
11. Click Apply.
12. Upon prompt, select Apply changes to this folder, subfolders and files.
13. Click OK.
14. Click OK.
15. Start > Administrative Tools > Server Manager > Configuration > Services
16. In the right column, double click NetSight Database Service.
17. Under the General tab, click Start.
18. Once the Service has started, click OK.

Figure 1-5 Encrypting the NetSight mysql Directory File System



mysql Properties

General | Sharing | Security | Previous Versions | Customize

mysql

Type: File folder

Location: C:\Enterasys Networks\NetSight

Size: 123 MB (129,218,385 bytes)

Size on disk: 124 MB (130,572,288 bytes)

Contains: 757 Files, 35 Folders

Created: Wednesday, July 20, 2011, 12:44:36 PM

Attributes: ☑ Read-only (Only applies to files in folder)

☐ Hidden

Advanced...

OK Cancel Apply

Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☑ Folder is ready for archiving

☑ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

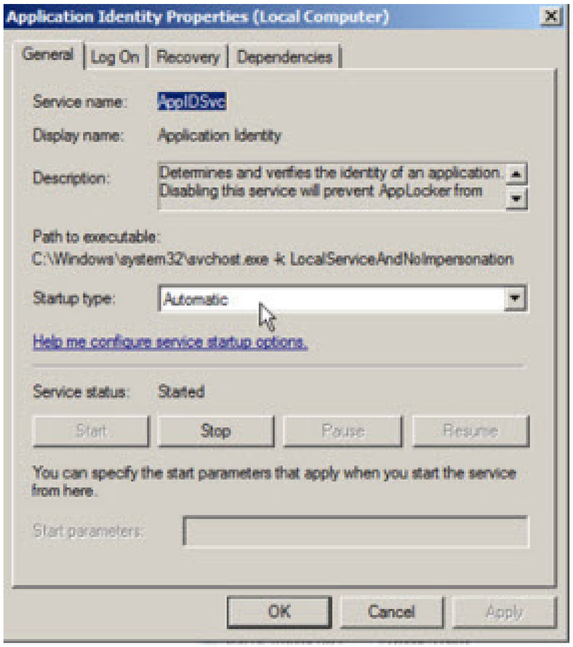
Details

OK Cancel

1.10 Configuring the Application Identity Service

1. Start > Administrative Tools > Server Manager > Configuration > Services
2. In the right column, double click Application Identity.
3. Under the General tab, change the Startup type field to Automatic.
4. Click Start.
5. Once the service has started, click OK.

Figure 1-6 Configuring the Application Identity Service



Application Identity Properties (Local Computer)

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

Startup type: Automatic

Help me configure service startup options.

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

1.11 Configuring Application Control Policies

1. Start > Administrative Tools > Local Security Policy > Application Control Policies -> AppLocker
2. Right click AppLocker.
3. Select Properties.
4. Select Configured under the following sections
   a. Executable rules
   b. Windows Installer rules
   c. Script rules
5. Click OK.

1.11.1 Configuring AppLocker Executable Rules

1. Start > Administrative Tools > Local Security Policy > Application Control Policies -> AppLocker -> Executable Rules
2. In the right column, right click.
3. Select Create New Rule.
4. Click Next.
5. Select Allow.
6. Click Select.
7. Fill in the following field

   Enter the object name to select: netsightusers

8. Click Check Names.
9. Click OK.
10. Click Next.
11. Select Path.
12. Click Next.
13. Click Browse folders.
14. Select the following path: C:\Enterasys Networks
15. Click OK.
16. Click Next.
17. Click Next.
18. Fill in the following field

    Name: Netsight
19. In the right column, right click.
20. Select Create New Rule.
21. Click Next.
22. Select Allow.
23. Click Select.
24. Fill in the following field

    Enter the object name to select: netsightsrv
25. Click Check Names.
26. Click OK.
27. Click Next.
28. Select Path.
29. Click Next.
30. Click Browse folders.
31. Select the following path: C:\Users\netsightsrv
32. Click OK.
33. Click Next.
34. Click Next.
35. Fill in the following field

    Name: netsightsrv
36. Click Create.
37. In the right column, right click.
38. Select Create New Rule.
39. Click Next.

40. Select Allow.
41. Click Select.
42. Fill in the following field

    Enter the object name to select: netsightadmin
43. Click Create.
44. Click Check Names.
45. Click OK.
46. Click Next.
47. Select Path.
48. Click Next.
49. Click Browse folders.
50. Select the following path: C:\Users\netsightadmin
51. Click OK.
52. Click Next.
53. Click Next.
54. Fill in the following field

    Name: netsightadmin
55. Click Create.
56. In the right column, right click.
57. Select Create New Rule.
58. Click Next.
59. Select Allow.
60. Click Select.
61. Fill in the following field

    Enter the object name to select: netsightuser
62. Click Check Names.
63. Click OK.
64. Click Next.
65. Select Path.
66. Click Next.
67. Click Browse folders.
68. Select the following path: C:\Users\netsightuser
69. Click OK.
70. Click Next.
71. Click Next.

72. Fill in the following field

    Name: netsightuser

73. Click Create.

1.11.2 Configuring AppLocker Script rules

1. Start > Administrative Tools > Local Security Policy > Application Control Policies -> AppLocker -> Script Rules
2. In the right column, right click.
3. Select Create New Rule.
4. Click Next.
5. Select Allow.
6. Click Select.
7. Fill in the following field

    Enter the object name to select: netsightusers

8. Click Check Names.
9. Click OK.
10. Click Next.
11. Select Path.
12. Click Next.
13. Click Browse folders.
14. Select the following path: C:\Enterasys Networks
15. Click OK.
16. Click Next.
17. Click Next.
18. Fill in the following field

    Name: Netsight

19. Click Create.
20. In the right column, right click.
21. Select Create New Rule.
22. Click Next.
23. Select Allow.
24. Click Select.
25. Fill in the following field

    Enter the object name to select: netsightsrv

26. Click Check Names.
27. Click OK.

28. Click Next.
29. Select Path.
30. Click Next.
31. Click Browse folders.
32. Select the following path: C:\Users\netsightsrv
33. Click OK.
34. Click Next.
35. Click Next.
36. Fill in the following field

    Name: netsightsrv
37. Click Create.
38. In the right column, right click.
39. Select Create New Rule.
40. Click Next.
41. Select Allow.
42. Click Select.
43. Fill in the following field

    Enter the object name to select: netsightadmin
44. Click Check Names.
45. Click OK.
46. Click Next.
47. Select Path.
48. Click Next.
49. Click Browse folders.
50. Select the following path: C:\Users\netsightadmin
51. Click OK.
52. Click Next.
53. Click Next.
54. Fill in the following field

    Name: netsightadmin
55. Click Create.
56. In the right column, right click.
57. Select Create New Rule.
58. Click Next.
59. Select Allow.

60. Click Select.

61. Fill in the following field

    Enter the object name to select: netsightuser

62. Click Check Names.

63. Click OK.

64. Click Next.

65. Select Path.

66. Click Next.

67. Click Browse folders.

68. Select the following path: C:\Users\netsightuser

69. Click OK.

70. Click Next.

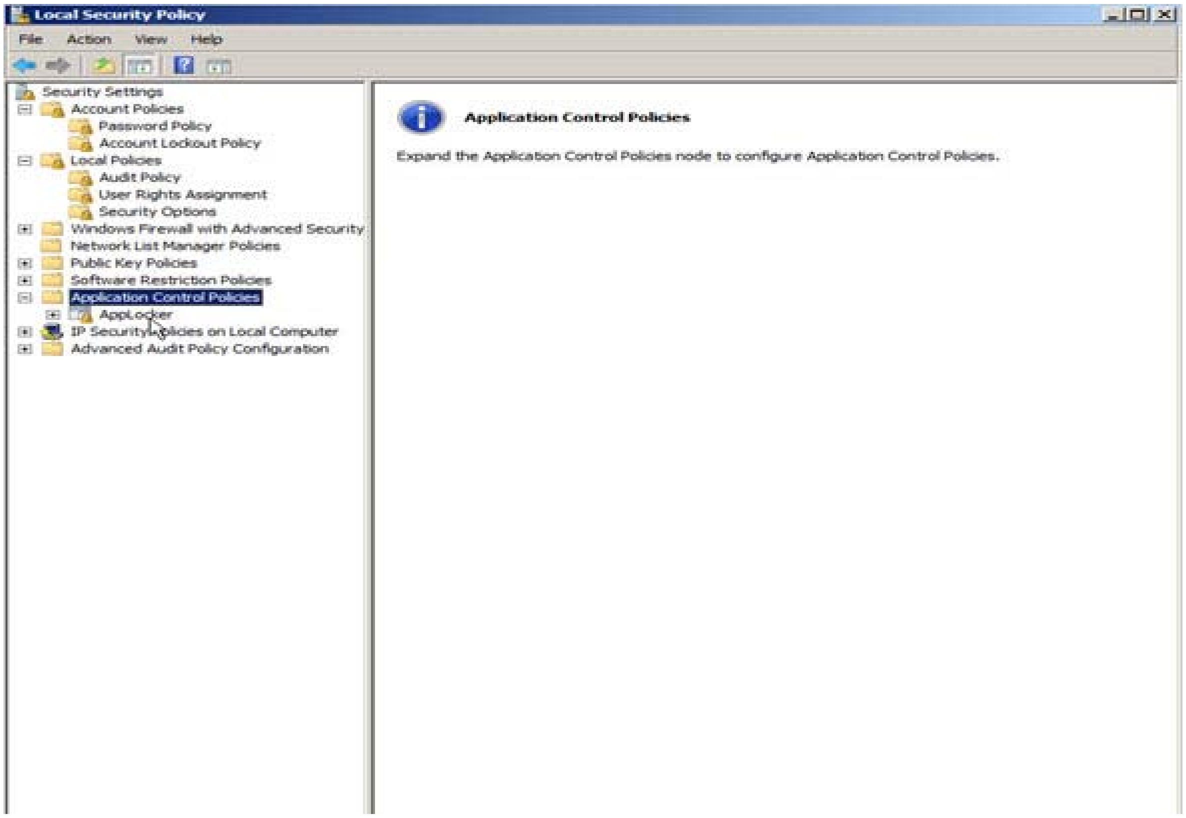
71. Click Next.

72. Fill in the following field

    Name: netsightuser

73. Click Create.

Figure 1-7 Configuring Application Control Policies



Application Control Policies

Expand the Application Control Policies node to configure Application Control Policies.

1.12 Configuring RemoteApp Manager

1. Start > Administrative Tools > Server Manager > Roles > RemoteApp Manager
2. Right click RemoteApp Manager.
3. Select Add RemoteApp Programs.
4. Click Next.
5. Select the following Apps:
    a. Automated Security Manager
    b. Console
    c. Inventory Manager
    d. NAC Manager
    e. Policy Manager
6. Click Next.
7. Click Finish.
8. In the right column under RemoteApp Programs, do the following steps for each NetSight program:
    a. Right click the program
    b. Select Create Windows Installer Package
    c. Click Next
    d. Click Next
    e. Click Next
    f. Click Finish
    g. Repeat for next NetSight program
9. Start > Computer
10. Go into the following directory, C:\Program Files\Packaged Programs
11. Copy MSI packages just created onto USB stick or other type of media.
12. Transfer and install MSI packages onto NetSight client computer.

1.13 Windows Firewall Configuration

1. Start > Administrative Tools > Local Security Policy > Windows Firewall and Advanced Security. Expand folder.
2. Click on Inbound Rules.
3. In the right column, right click and select New Rule.
4. Select Port and click Next.
5. Select TCP.
6. Select Specific local ports and type 135, then click Next.
7. Select Allow the Connection if it is secure, then click Customize.

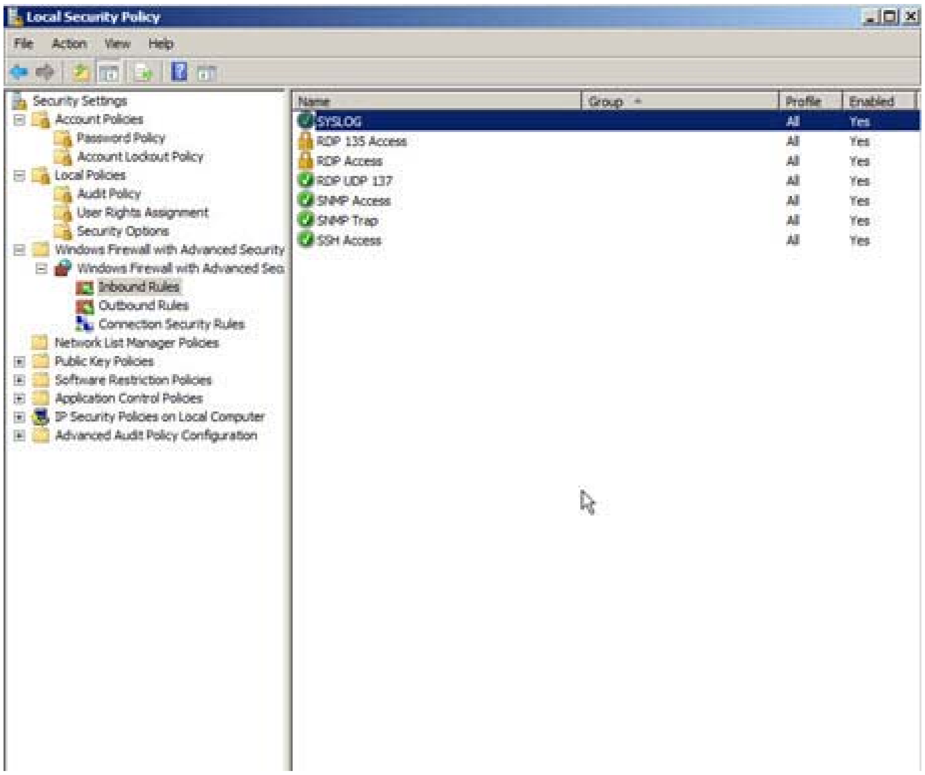
8. Select Allow the connection if it is authenticated and integrity-protected.
9. Click OK then click Next.
10. Leave Domain, Private, and Public checked then click Next.
11. Enter Rule {RDP 135 Access} then click Finish.
12. In the Right Column, right click and select New Rule.
13. Select Port and click Next.
14. Select TCP.
15. Select Specific local ports and type 3389 then click Next.
16. Select Allow the Connection if it is secure then click Customize.
17. Select Allow the connection if it is authenticated and integrity-protected.
18. Click OK then click Next.
19. Leave Domain, Private, and Public checked then click Next.
20. Enter Rule {RDP 3389 Access} then click Finish.
21. In the Right Column, Right Click and select New Rule.
22. Select Port and click Next.
23. Select UDP.
24. Select Specific local ports and type 137 then click Next.
25. Select Allow the Connection then click Next.
26. Leave Domain, Private, and Public checked then click Next.
27. Enter Rule {RDP UDP 137 Access} then click Finish.
28. In the Right Column, right click and select New Rule.
29. Select Custom then click Next.
30. Select All programs then click Next.
31. In the Protocol type, select UDP.
32. In the Local port select Specific Ports.
33. Type 161 then click Next.
34. Under Which local IP addresses does this rule apply to, choose These IP addresses and click Add button.
35. Choose This IP address or subnet. Enter IP address of Netsight server. [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
36. Under Which remote IP addresses does this rule apply to, choose These IP addresses and click Add button.
37. Choose This IP address or subnet. Enter Management IP address and 64 bit mask of Management Subnet for Router/Switch. [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
38. Click Next.
39. Select Allow the Connection then click Next.
40. Leave Domain, Private, and Public checked then click Next.
41. Enter Rule {SNMP Access} then click Finish.

42. In the Right Column, right click and select New Rule.
43. Select Custom then click Next.
44. Select All programs then click Next.
45. In the Protocol type, select UDP.
46. In the Local port select Specific Ports.
47. Type 162 then click Next.
48. Under Which local IP addresses does this rule apply to, choose These IP addresses and click Add button.
49. Choose This IP address or subnet. Enter IP address of Netsight server.
    [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
50. Under Which remote IP addresses does this rule apply to, choose These IP addresses and click Add button.
51. Choose This IP address or subnet. Enter Management IP address and 64 bit mask of Management Subnet for Router/Switch. [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
52. Click Next.
53. Select Allow the Connection then click Next.
54. Leave Domain, Private, and Public checked then click Next.
55. Enter Rule {SNMP Trap} then click Finish.
56. In the Right Column, Right Click and select New Rule.
57. Select Custom then click Next.
58. Select All programs then click Next.
59. In the Protocol type, select TCP.
60. In the Local port select Specific Ports.
61. Type 22 then click Next.
62. Under Which local IP addresses does this rule apply to, choose These IP addresses and click Add button.
63. Choose This IP address or subnet. Enter IP address of Netsight server.
    [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
64. Under Which remote IP addresses does this rule apply to, choose These IP addresses and click Add button.
65. Choose This IP address or subnet. Enter Management IP address and 64 bit mask of Management Subnet for Router/Switch. [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]. Click OK.
66. Click Next.
67. Select Allow the Connection then click Next.
68. Leave Domain, Private, and Public checked then click Next.
69. Enter Rule {SSH Access} then click Finish.
70. In the Right Column, right click and select New Rule.
71. Select Port and click Next.
72. Select UDP.
73. Select Specific local ports and type 514 then click Next.
74. Select Allow the Connection then click Next.

75. Leave Domain, Private, and Public checked then click Next.

76. Enter Rule {Syslog UDP 514 Access}, then click Finish.

Figure 1-8 Configuring RemoteApp Manager



Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Sec
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Name	Group	Profile	Enabled
SYSLOG		All	Yes
RDP 135 Access		All	Yes
RDP Access		All	Yes
RDP UDP 137		All	Yes
SNMP Access		All	Yes
SNMP Trap		All	Yes
SSH Access		All	Yes

1.14 Configuring IPsec

1. Start > Administrative Tools > Local Security Policy > Windows Firewall and Advanced Security. Expand folder.
2. Right click on Windows Firewall with Advanced Security - Local Group Policy Object. Select properties.
3. Select the domain profile tab.
4. In the firewall state drop down menu, select On.
5. In the Inbound connections drop down menu, select Block.
6. In the Outbound connections drop down menu, select Allow.
7. Select the private profile tab.
8. In the firewall state drop down menu, select On.
9. In the Inbound connections drop down menu, select Block.
10. In the Outbound connections drop down menu, select Allow.
11. Select the public profile tab.
12. In the firewall state drop down menu, select On.
13. In the Inbound connections drop down menu, select Block.

14. In the Outbound connections drop down menu, select Allow.
15. Select IPsec Settings tab.
16. Under IPSec Defaults, select Customize.
17. Under Key Exchange (Main Mode) section, select advanced button and click Customize. Click Add button.
18. In Integrity algorithm drop down, choose SHA-1.
19. In Encryption Algorithm drop down, choose AES-CBC 128.
20. In Key exchange algorithm drop down, choose Diffie-Hellman Group 14. Click OK.
21. Under key lifetimes, enter 480 for minutes and 0 for sessions.
22. Under key exchange options, check Use Diffie-Hellman for enhanced security. Click OK.
23. Under Data protection (Quick Mode), select advanced and click Customize button.
24. Check Require encryption for all connection security rules that use these settings.
25. Under data integrity and encryption, click Add button.
26. Under protocol, choose ESP.
27. In Encryption algorithm drop down, choose AES-CBC 128.
28. In Integrity algorithm drop down, choose SHA-1.
29. Under key lifetimes, enter 60 for minutes and 100,000 for KB. Click OK.
30. Click OK.
31. Under Authentication method, select advanced and click Customize.
32. Click Add button.
33. Select Preshared key. Enter key in box. Click OK.
34. Uncheck First authentication is optional. Click OK.
35. Click OK.
36. In IPsec tunnel authorization area, select none. Click OK.
37. In left menu pane, click Connection Security Rules.
38. On right of screen under Actions, click New rule.
39. Select Custom. Click Next button.
40. Under Which computers are in Endpoint 1, choose These IP addresses and click Add button.
41. Choose This IP address or subnet. Enter IP address of Netsight server. Xxxx.xxxx.xxxx.xxxx. Click OK.
42. Under Which computers are in Endpoint 2, choose These IP addresses and click Add button.
43. Choose This IP address or subnet. Enter IP address and 64 bit mask of Netsight client(s). [xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx/64] or [xxx.xxx.xxx.xxx/24]
44. Click OK.
45. Click Next.
46. Choose require authentication for inbound and outbound connections. Click Next.
47. Choose Advanced. Click Customize button.
48. Under First authentication methods, click Add.

49. Select Preshared key. Enter key. Click OK.

50. Uncheck, First authentication is optional. Click OK.

51. Click Next.

52. In Protocol type drop-down, choose Any.

53. In Endpoint 1 port drop-down, choose All Ports.

54. In Endpoint 2 drop-down, choose All Ports.

55. Click Next.

56. Check Domain, Private, and Public.

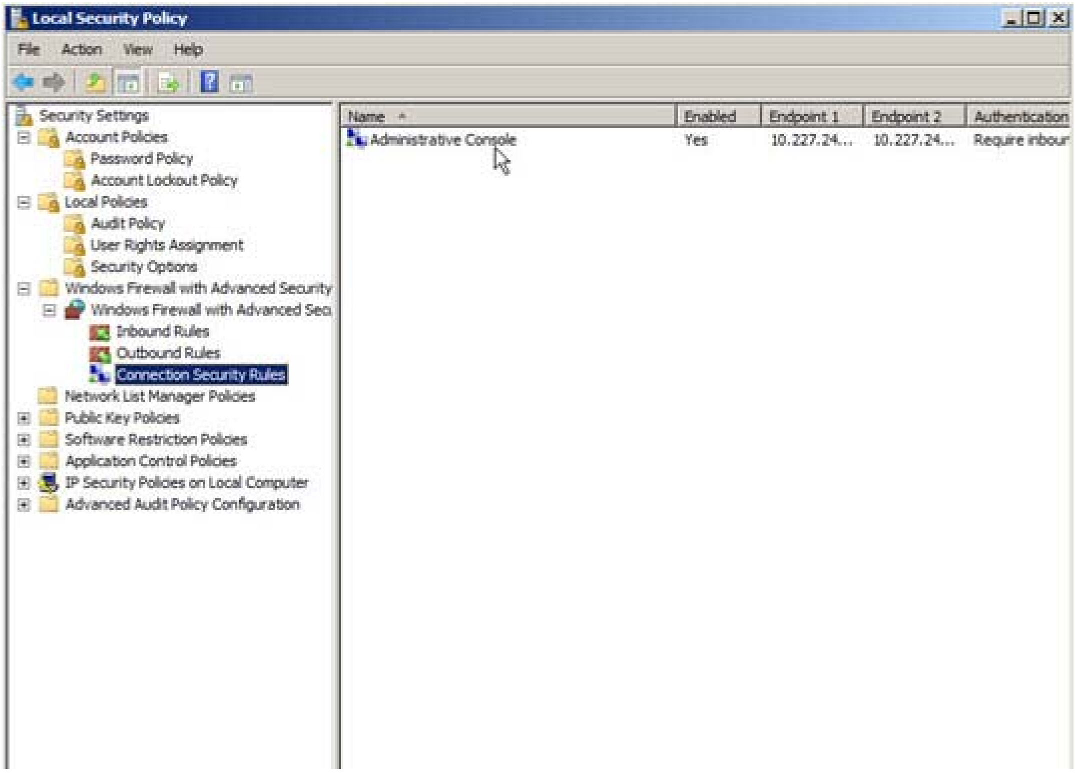
57. Enter <rule name>.

58. Click Finish.

59. If new rule is not enabled, right click rule, then select Enable rule.

60. Setup the Netsight Client IPSEC configuration the same way except in steps 40–43 reverse the IP addresses.

Figure 1-9 Configuring IPsec



Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Windows Firewall with Advanced Secu
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Name	Enabled	Endpoint 1	Endpoint 2	Authentication
Administrative Console	Yes	10.227.24...	10.227.24...	Require inbour