nAppliance

mISAE Server 2006 Enterprise Edition Users Guide

For use with mISAE Appliances

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Contents

nAppliance mISAE Server is an advanced application layer firewall, virtual private network (VPN), and Web cache solution that enables you to maximize existing IT investments by improving network security and performance. The nAppliance mISAE Server firewall is preinstalled and hardened to provide secure connections to the Internet and enable a similar level of security for remote access connections to resources on the protected network.

The nAppliance mISAE Server Users Guide focuses on important issues that you should consider. However, this Users Guide is not a comprehensive guide to configuring all of the firewall features of nAppliance mISAE Server. You can find in-depth coverage about nAppliance mISAE Server firewall and Web caching configuration in the Help file included with the product and on the mISAE Server 2006 website (http://www.microsoft.com/mmISAEEserver/2006/default.mspx).

This guide contains basic information about network configuration and setup. If you are an experienced firewall or network administrator, you will already be familiar with most of the concepts and procedures contained in this guide. However, we recommend that you briefly review the subjects covered in this guide as some of the subjects may be new or of specific interest to you.

Hardware Setup

This section includes the following topics concerning the hardware:

- Package Contents
- Connect nAppliance mISAE Server
- Power On the Appliance
- Connecting to the nAppliance mISAE Server Web-Management

The topic “Connecting to the nAppliance mISAE Server Web-Management” specifies how to connect to the Web-Management of the nAppliance mISAE Server. It is a flexible and simple configuration method to fit the server to your requirements, the full functionality is described in the later chapter “nAppliance mISAE Server Web-Management”.

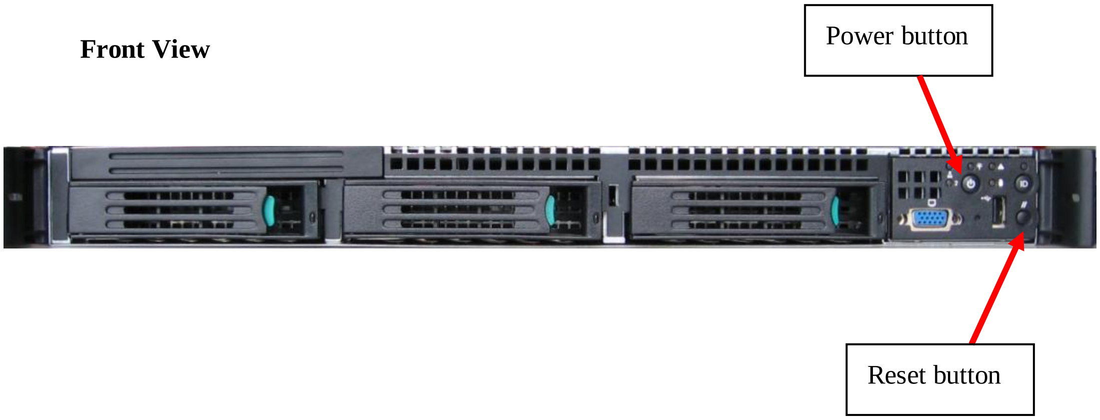
Package Contents

The package contains the following items:

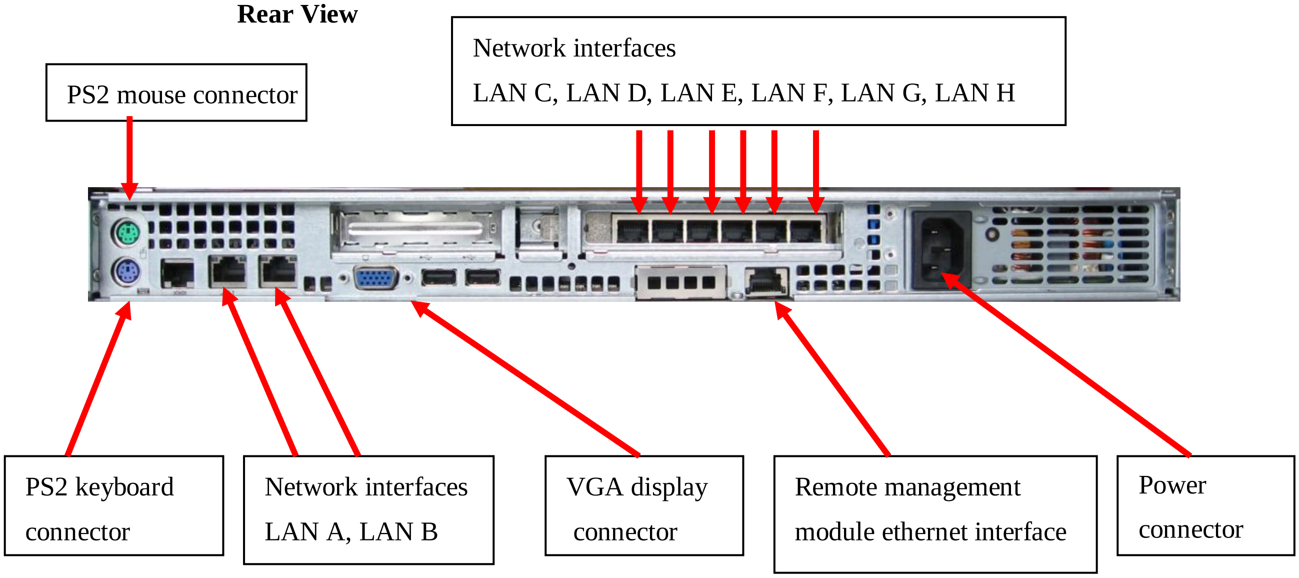
- nAppliance mISAE Server, power cabling
- nAppliance Appliance Installation DVD
- nAppliance mISAE Server Users Guide
- nAppliance mISAE Server Quick Start Guide

Connect nAppliance mISAE Server

Front View



Rear View


PS2 mouse connector
Network interfaces
LAN C, LAN D, LAN E, LAN F, LAN G, LAN H
PS2 keyboard connector
Network interfaces LAN A, LAN B
VGA display connector
Remote management module ethernet interface
Power connector

As you see in the picture you have eight network ports: LAN A through LAN H, all ports are able to handle 1000/100/10 Mb/s connections. The default configuration of the interfaces is as follows:

LAN A:

- IP Address: 192.168.73.254
- Netmask: 255.255.255.0

LAN B – LAN H:

- DHCP

Action

1. To connect the nAppliance mISAE Server to your network use either LAN A if you prefer using static IP addresses or LAN B through LAN H to obtain an IP address automatically from your DHCP server.
2. Connect a monitor to the VGA display connector on the nAppliance mISAE Server computer.
3. Connect a mouse and keyboard to the PS2 connectors
4. Plug the computer end of the power cord into the nAppliance mISAE Server computer power connector, and plug the other end into an appropriate power source.

Power On the Appliance

Action

1. Change the power switch to “ON” and press the power button on your nAppliance mISAE Server computer.

When powering on the appliance for the first time the server checks the file systems and reboots the machine. Afterwards an automatic windows setup will start which does not require any user interaction.

After the setup process has finished, the server will reboot and automatically log on to the system as the administrator and execute important post installation scripts. Finally the computer will reboot and display the logon screen. Now you have the possibility to connect you to the server over the Web-Management.

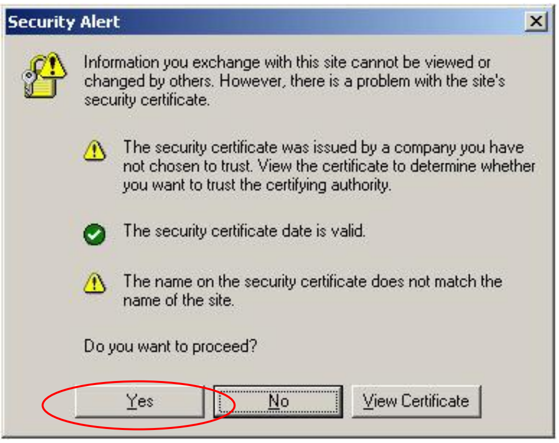
> **Important**
>
> The initial setup of the appliance is completely unattended and must not be interrupted by the user. Note that the appliance will reboot 3 times before it is fully functional and ready for operation.

Connecting to the nAppliance mISAE Server Web-Management

Action

1. Start a Microsoft Internet Explorer.
2. Enter **https://192.168.73.254:8098** in the address field if you use the pre-configured IP Address given by LAN A**.** If you have changed the server’s IP-address or you use LAN B or LAN C, please enter the new address instead of entering the pre-set IP Address 192.168.73.254 in the given format here.

Should the following browser warning appear on your screen, please confirm the message with **YES**.



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

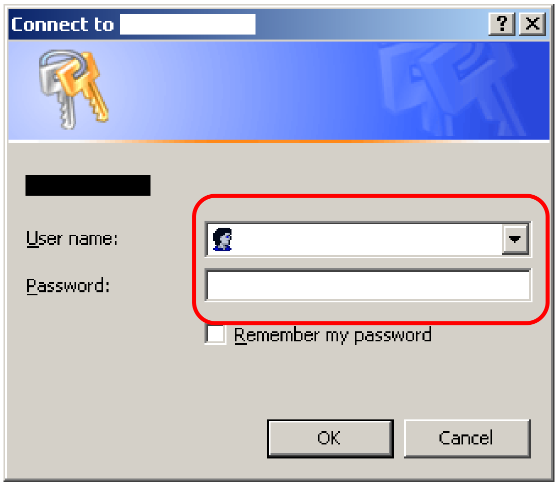
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The name on the security certificate does not match the name of the site.

Do you want to proceed?

3. In the next screen you have to input the user name and the password. By default the user name is **Administrator** and the password is **nappliance13.**



4. Choose **OK**.

> **Important**
>
> To enable the full functionality of the Web-Management you have to add the internal IP address to the trusted sites in the Microsoft Internet Explorer.

Add the internal IP address to the trusted sites

1. To do this open the Microsoft Internet Explorer and select the menu item **Tools.**

2. Choose **Internet Options**.

3. Select the tab **Security**.
4. Click on the Icon **Trusted sites**.
5. Press the button **Sites…**.
6. Enter **https://192.168.73.254** in the text box. If you don't use the standard IP address add the server's IP address in the given format.
7. Press **Add**.
8. Press **OK** in the window **Trusted sites**.
9. Press **OK** in the window **Internet Options**.

Initial Setup Considerations

You need to address a number of issues and questions before beginning the nAppliance mISAE Server firewall setup. The nAppliance mISAE Server firewall will be able to provide you the best level of security and accessibility if you consider these subjects before you begin.

Note

All configuration steps described in this chapter can be done through the mISAE Server Web-Management interface. For a detailed description of the Web-Interface see Chapter "nAppliance mISAE Web-Management interface".

Firewall Lockdown Mode

Important

Your mISAE 2006 Enterprise Edition Appliance defends itself out of the box by running in lockdown mode. Please follow the upcoming chapters carefully in order to leave firewall lockdown mode.

A critical function of a firewall is to react to an attack. When an attack occurs, it may seem that the first line of defense is to disconnect from the Internet, isolating the compromised network from malicious outsiders. However, this is not the recommended approach. Although the attack must be handled, normal network connectivity must be resumed as quickly as possible, and the source of the attack must be identified.

The lockdown feature introduced with mISAE Server 2006 combines the need for isolation with the need to stay connected. Whenever the Microsoft Firewall service is down, mISAE Server enters the lockdown mode. This occurs when:

- The server is starting up and the Firewall service has not started yet.
- The first time configuration has not been done, Appliance needs to be initialized.
- An event triggers the Firewall service to shut down. When you configure alert definitions, you decide which events will cause the Firewall service to shut down. Essentially, you configure when mISAE Server enters lockdown mode.
- The Firewall service is manually shut down. If you become aware of malicious attacks, you can shut down the Firewall service, while configuring the mISAE Server computer and the network to handle the attacks.

Affected functionality

When in lockdown mode, the following functionality applies:

- The Firewall Packet Filter Engine (fweng) applies the firewall policy.
- The following system policy rules are still applicable:
    - Allow ICMP from trusted servers to the local host.
    - Allow remote management of the firewall using MMC (RPC through port 3847).
    - Allow remote management of the firewall using RDP.
    - Allow remote Management using the Web-Interface.
- Outgoing traffic from the Local Host network to all networks is allowed. If an outgoing connection is established, that connection can be used to respond to incoming traffic. For example, a DNS query can receive a DNS response, on the same connection.
- No incoming traffic is allowed, unless a system policy rule (listed previously) that specifically allows the traffic is enabled. The one exception is DHCP traffic, which is always allowed. That is, the UDP Send protocol on port 68 is allowed from all networks to the Local Host network. The corresponding UDP Receive protocol on port 67 is allowed.
- VPN remote access clients cannot access mISAE Server. Similarly, access is denied to remote site networks in site-to-site VPN scenarios.

υ Any changes to the network configuration while in lockdown mode are applied only after the Firewall service restarts and mISAE Server exits lockdown mode. For example, if you physically move a network segment and reconfigure mISAE Server to match the physical changes, the new topology is in effect only after mISAE Server exits lockdown mode.

υ mISAE Server does not trigger any alerts.

Leaving lockdown mode

After setting up all system and network specific parameters like network interfaces, DNS client and active directory membership, you will learn how to initialize the mISAE 2006 Enterprise Edition Appliance at the end of this chapter. Initializing the server will automatically leave lockdown mode.

Internal Network Overview

The Internal network consists of addresses on the protected network that are not associated with a perimeter or external network interface. Addresses on the LAN are typically part of the Internal network. The nAppliance mISAE Server depends on the correct configuration of the Internal network adapter so that nAppliance mISAE Server firewall system policy is applied correctly. Network infrastructure services such as Active Directory directory service domain controllers, internal DNS servers, DHCP servers, Windows Internet Name Service (WINS) servers, Terminal Services, Internet Control Message Protocol (ICMP), Common Internet File System (CIFS), and others depend on the correct configuration of the Internal network.

Incorrect configuration of the Internal network addresses could lead to a compromise of the nAppliance mISAE Server firewall.

The Internal network consists of a collection of addresses representing a portion of a network ID, an entire network ID, or several network IDs. The Internal network can represent all addresses accessible from one or more network adapters.

Computer Name and Administrator Password

The nAppliance mISAE Server firewall computer name must be different from any other computer on your network. No two computers on your network can have the same name. The computer name must be 15 characters or less in length and include only letters and numbers (spaces are not allowed).

Action

υ Choose a computer name for the nAppliance mISAE Server firewall computer. Make sure that this name is not already in use on the network. The name must be 15 characters or less in length and contain only letters and numbers (spaces are not allowed). Refer to your computer name database if you are installing the nAppliance mISAE Server firewall on a larger network.

The Administrator account has complete access to all components of your nAppliance mISAE Server firewall. Any person connecting to the nAppliance mISAE Server firewall with the Administrator account can take control of the firewall, and from there attack your network. You must use a complex and difficult to guess password for the Administrator account. This helps to prevent attackers from easily guessing the password.

> **Note**
>
> It is important that the password should be at least 7 characters
> in length and should include capital letters, small letters and numbers.
> Otherwise you would get a reference that the password does not fulfill
> the requirements.

Action

υ Write down the administrator password that you will use for your nAppliance mISAE Server firewall and then memorize this password. Put this paper in a protected location after the nAppliance mISAE Server firewall installation is completed. Note that if the nAppliance mISAE Server firewall will be joined to a domain, be sure to comply with existing domain-wide password policy.

Workgroup and Domain Name Considerations

The nAppliance mISAE Server firewall can be joined to a workgroup, a Microsoft Windows Server 2003 or Windows 2000 Active Directory domain, or a Windows NT 4.0 domain. You may want to join the nAppliance mISAE Server firewall to your Windows domain if you already have a Windows Server 2003 or Windows 2000 Active Directory domain, or a Windows NT 4.0 domain on your network.

An advantage of joining the nAppliance mISAE Server firewall to your domain includes:

υ The ability to assign permissions for Internet access on a domain user or group basis and centralized management of the firewall computer through Group Policy.

A dmmISAEEdvantage of joining the nAppliance mISAE Server firewall to your domain includes:

Many firewall experts believe that joining the nAppliance mISAE Server firewall to your domain may reduce the overall level of protection that the firewall can provide to your network.

Note that when you join the nAppliance mISAE Server firewall to a Windows domain, the domain Group Policy may be applied to the firewall computer. This may change the level of security on the nAppliance mISAE Server firewall computer. You may want to join the nAppliance mISAE Server firewall to a workgroup and later join a Windows domain after you have a better understanding of how Group Policy can potentially change the firewall's security configuration.

You will join the nAppliance mISAE Server firewall to a Windows workgroup if you do not have a Windows domain or if you choose not to join the nAppliance mISAE Server firewall to an already existing domain.

Actions

1. Decide on whether you want to join the nAppliance mISAE Server firewall to your Windows domain before installing the nAppliance mISAE Server firewall onto your network.
2. Write down the name of your domain and the user name and password of a user that has permissions to add a computer to the domain.
3. If you do not have a Windows domain, or if you do not want to join your nAppliance mISAE Server firewall to your Windows domain, write down the name of the workgroup already in use on your LAN.
4. If you do not already have a workgroup name for your LAN, you can use the workgroup name, WORKGROUP.

If you chose to join the nAppliance mISAE Server firewall to your domain, perform the following procedure.

1. Connect you to the nAppliance mISAE Server using the **Web-Management** from a remote computer.
2. On the primary navigation bar, choose **Network**.
3. Choose **Identification**.
4. Select that the server will be part of a **domain**.
5. Type the **user name** and **password** of the person who has permission to add client computers to the domain.
6. Choose **OK**.
7. When prompted to reboot the server, click **Yes**.

The nAppliance mISAE Server firewall is now a member of the Internal network Active Directory domain and can access user accounts contained in the Active Directory or Windows NT 4.0 domain and domains trusted by that domain.

The nAppliance mISAE Server Firewall Internal IP Address

The IP address assigned to the internal interface of the nAppliance mISAE Server firewall must be a valid IP address for the network to which the firewall is directly connected. This address must meet the following requirements:

- The Internal IP address must be on the same network ID as other computers connected to the same network segment.
- The Internal IP address must not already be in use on the network.
- The Internal IP address, in most cases, is statically assigned. Do not use DHCP to assign an address to the internal interface unless you have a specific requirement to do so. This helps prevent name resolution issues for the Firewall and Web Proxy clients.
- Examples of network IDs commonly used on LANs include:
- 192.168.1.0 with a subnet mask of 255.255.255.0
- 10.1.0.0 with a subnet mask of 255.255.0.0
- 172.16.0.0 with a subnet mask of 255.255.0.0

Note

The nAppliance mISAE Server firewall uses a default internal IP address of 192.168.73.254. You should change this to meet your network’s unique addressing requirements.

After changing the internal IP address you have to use the entered IP address to connect to your server over Web-Management.

For example, consider the network depicted in the following figure 1. All of the computers on the network have the same subnet mask, which is 255.255.255.0. The three computers on the LAN have the IP addresses:

- 192.168.2.2
- 192.168.2.3
- 192.168.2.4

The internal interface must be placed in the same network as these computers. In this example, this is accomplished by assigning the internal interface the IP address of 192.168.2.1. By the way the address to connect over Web-Management from another internal computer would be https://192.168.2.1:8098 now. The external interface of the nAppliance mISAE Server firewall is assigned an Internet IP address that is determined by your Internet service provider (ISP).

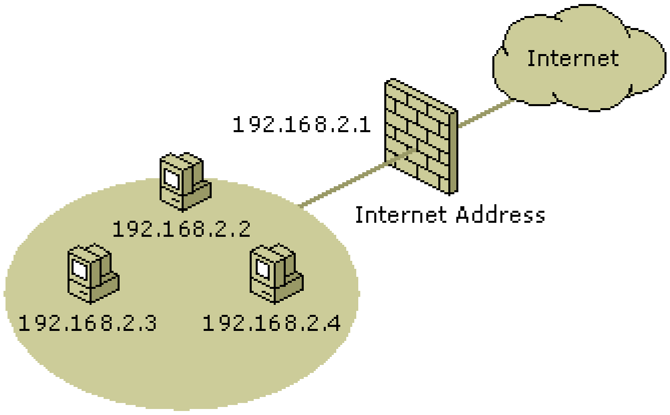


Figure 1: Sample network setup

Note

IP addressing can be a complex issue. If you do not understand how the IP addresses were assigned to computers on your LAN, consult with a networking professional who can assist you with network IP addressing issues.

Actions

1. Before you install the nAppliance mISAE Server firewall, determine the network ID used on the network directly connected to its internal interface.
2. Assign the internal interface of the nAppliance mISAE Server firewall an IP address on the same network ID as the other computers on the internal interface's directly connected network.
3. If you are not sure what IP address to assign to the internal interface of the nAppliance mISAE Server firewall, consult with a network professional who can help you with IP addressing issues.

DNS Server Address on the Internal Interface

Your nAppliance mISAE Server firewall needs to resolve names to IP addresses. For example, each time you use your Web browser to connect to a website on the Internet, such as www.microsoft.com, that name is sent to a Domain Name System (DNS) server to match (or resolve) that name to the IP address of the website. After your Web browser has the IP address of the website, it connects to the website using the IP address.

The nAppliance mISAE Server firewall must be configured to use a DNS server that resolves Internet computer names to IP addresses. There are several ways to do this:

υ Install a DNS server on the LAN, configure that DNS server to resolve Internet host names, and configure the nAppliance mISAE Server firewall to use that DNS server.

υ Use the IP address of your ISP DNS server. The DNS server at your ISP will be able to resolve Internet computer names, but it will not be able to resolve computer names on your LAN.

υ Install and configure a DNS server on the nAppliance mISAE Server firewall computer. This DNS server would be able to resolve both Internet computer names and computer names on your LAN.

Note

Any network services and client applications installed on the firewall can potentially increase the security risk.

If you are already familiar with the installation and configuration of DNS servers, or if you already have a DNS server on your LAN, the best option is to configure that DNS server to resolve Internet host names, and then create an access rule on the firewall enabling that DNS server to use the DNS protocol to connect to the Internet.

If you are not familiar with DNS server installation and configuration, or if you do not want to install and configure a DNS server, you can use your ISP DNS server. The main limitation of this option is that your ISP DNS server cannot resolve names of computers on your LAN.

Action

1. Determine if you already have a DNS server on your LAN.
2. If you have a DNS server on your LAN, configure that DNS server to resolve Internet host names, and then create a firewall rule allowing this DNS server access to the DNS protocol to all sites on the Internet.
3. If you do not have a DNS server on your LAN, you can install a DNS server on the nAppliance mISAE Server firewall computer. For details on DNS setup and configuration, see the Windows Server 2003 Help and Support Center.
4. If you do not have a DNS server on your LAN and do not want to install a DNS server on the nAppliance mISAE Server firewall, configure the internal interface to use the IP address of your ISP DNS server. You may need to consult your ISP website or call them to determine the correct IP address of their DNS server.

Custom Network Adapter Configurations

Your nAppliance mISAE Server firewall may be equipped with additional network interfaces. In addition to the internal and external interfaces, you may have additional LAN, partner access, and perimeter network (also known as DMZ, demilitarized zone, and screened subnet) interfaces. These interfaces can be used for:

υ Additional LAN interfaces can connect several Internal networks to the firewall. The nAppliance mISAE Server firewall can control what network traffic moves among the LANs and between the LANs and the Internet.

υ Perimeter network interfaces can be used to connect perimeter networks hosting publicly accessible servers and services. For example, you may want to host your own e-mail or Web servers on the perimeter network.

υ Partner networks allow business partners to connect to resources on a network segment outside of the LAN and perimeter networks. These are not public networks because only the partners are able to connect to them. Partner networks are sometimes referred to as extranets.

IP addresses assigned to additional LAN interfaces, perimeter network interfaces, and extranet interfaces are specific to the requirements or your unique network configuration. The only requirement from the standpoint of the nAppliance mISAE Server firewall is that each of these interfaces is configured with IP addresses on different network IDs.

Actions

1. Before configuring the nAppliance mISAE Server firewall, determine what IP addresses and subnet masks should be configured on the additional, perimeter network or extranet interfaces. Write these down prior to configuring your nAppliance mISAE Server firewall.
2. If you need to configure a perimeter network, additional LAN networks, or an extranet, but do not know what IP addresses to assign the nAppliance mISAE Server firewall interfaces, consult with a network professional who can help you determine the correct configuration.

External IP Address Configuration

Your ISP determines the IP address of the external interface of the nAppliance mISAE Server firewall. The address can be a statically assigned IP address or a dynamically assigned IP address. Statically assigned IP addresses do not change over time. Dynamic IP addresses change over the course of hours, days, or weeks. How frequently the address changes is determined by your ISP.

The type of address you use is based on how much you are able to spend on the Internet connection and the level of service you require. If you will use the nAppliance mISAE Server firewall only for connection your network computers to the Internet, a dynamically assigned address will fulfill that requirement. However, if you want to publish servers on the Internal network to the Internet, or if you want to take advantage of the nAppliance mISAE Server firewall virtual private network (VPN) server features, you will benefit from having a permanent IP address on the firewall external interface.

You must have a valid IP address assigned to the external interface of the nAppliance mISAE Server firewall before you can connect to the Internet. You can assign either a static or dynamic address to the external interface.

Actions

1. Determine if you have a statically or dynamically assigned external IP address before installing your nAppliance mISAE Server firewall.
2. If you have a statically assigned IP address, write it down for future reference.
3. If you have a dynamically assigned IP address, you will configure the external interface to automatically obtain an IP address.

Initializing mISAE 2006 Enterprise Edition

As mentioned in the previous chapter, your mISAE 2006 Enterprise Edition Appliance will be fully operational after the mISAE initialization. This chapter will guide you through this task with the help of the "mISAE Initialization wizard" of the nAppliance mISAE Web-Management interface.

Actions

1. Connect to the nAppliance mISAE Web-Management Interface as described before, you will see the WebUI page.
2. If you have completed all the tasks from the previous chapters, you can continue directly with "Configure mISAE2006EE". Be sure that you have set up all IP-Addresses, DNS Client and Active directory membership before.
3. Depending on the desired area of operation you will be asked for several parameters which will be described now.

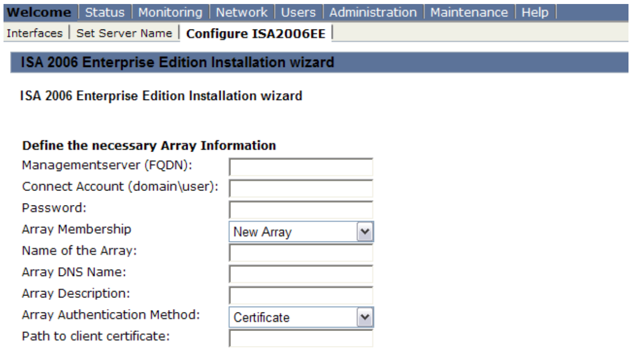
mISAE Initialization Procedure

First of all, you will be asked for the CSS type. The CSS is the Configuration Storage Server which stores all mISAE specific settings (access rules, VPN configurations etc.) for your mISAE2006 Enterprise Edition firewalls. If you already have an CSS on your local (or remote) network, answer the question by checking the *"remote"* button.

If the CSS is on your local network, select *"The mISAE Server is permanently connected to the management server"*, else choose *"The mISAE Server is connected to the management server through a VPN tunnel"*.

For a permanently connected CSS you will have to enter the following information:

- Managementserver (FQDN of your CSS)
- Account name and password which you want to use to add the mISAE Appliance to your CSS
- Either if you want to create a new array or join an existing array
- Array information (DNS name and description may be left blank when joining an existing array)
- Authentication method
- Path to client certificate (must be left blank when "Windows Authentication" is selected)



ISA 2006 Enterprise Edition Installation wizard

ISA 2006 Enterprise Edition Installation wizard

Define the necessary Array Information

Managementserver (FQDN):	
Connect Account (domain\user):	
Password:	
Array Membership	New Array
Name of the Array:	
Array DNS Name:	
Array Description:	
Array Authentication Method:	Certificate
Path to client certificate:	

If the CSS is on a remote site, the following information is additionally needed:

- VPN protocol type
- Depending on the selection (IPSec or L2TP), several VPN specific parameters have to be entered (i.e. pre-shared secret, Username and Password etc.)

If you do not have a CSS yet

you have answered the first question with *"local"*, a new array will be automatically created and both CSS and firewall services will be initialized on the mISAE Appliance. Note that the new arrays name is mandatory, DNS name and description are optional.

Note

A dedicated CSS server is recommended. Do not use a perimeter firewall as a CSS for your network.

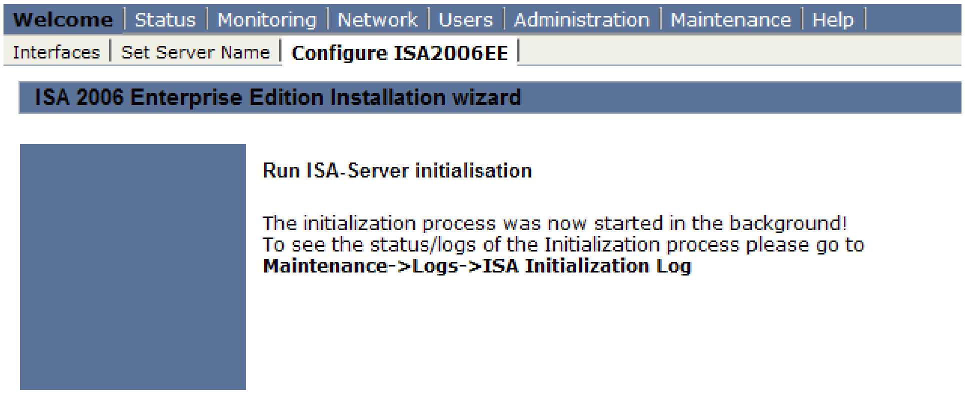
When you have entered all necessary data, press the "Next" button to continue. All configuration information has been written to a temporary configuration file, which is now used to initialize your mISAE 2006 EE Appliance.

ter pressing the "Next" button once again, the initialization process will run unattended in the background.

Important

While the initialization process is running, the Appliance ewill be reoobted once or twice, depending on your selections. Note that the whole proccess can take up to 10 minutes! No user interaction is required as soon as the initialization has been started.

To see the status of initialization process verify the log output in Maintenance → Logs → mISAE Initialization Log.

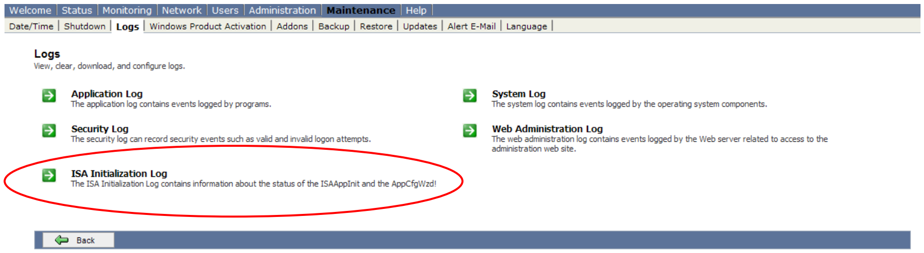

Welcome | Status | Monitoring | Network | Users | Administration | Maintenance | Help |
Interfaces | Set Server Name | Configure ISA2006EE |

ISA 2006 Enterprise Edition Installation wizard

Run ISA-Server initialisation

The initialization process was now started in the background!
To see the status/logs of the Initialization process please go to **Maintenance->Logs->ISA Initialization Log**

Note that log files will become available as soon as certain parts of the initialization process have been finished.


Welcome | Status | Monitoring | Network | Users | Administration | Maintenance | Help |
Date/Time | Shutdown | Logs | Windows Product Activation | Addons | Backup | Restore | Updates | Alert E-Mail | Language |
Back

Logs
View, clear, download, and configure logs.

Application Log
The application log contains events logged by programs.

System Log
The system log contains events logged by the operating system components.

Security Log
The security log can record security events such as valid and invalid logon attempts.

Web Administration Log
The web administration log contains events logged by the Web server related to access to the administration web site.

ISA Initialization Log
The ISA Initialization Log contains information about the status of the ISAAppInit and the AppCfgWzd!

nAppliance mISAE Server Firewall Setup

There are several basic configuration tasks you should carry out. These include:

- Enabling the Web listener
- Enabling the Firewall client listener
- Creating an Internet access rule

Enabling the Web Listener

A Web listener is software that accepts connections from Web browsers on the LAN configured to use the nAppliance mISAE Server firewall as a Web Proxy server. The Web browser sends requests to connect to the Internet directly to the IP address on the nAppliance mISAE Server firewall listening for outbound Web requests. Some advantages of configuring the Web browser to use the nAppliance mISAE Server firewall as a Web Proxy include:

- The client computer connecting to the nAppliance mISAE Server firewall does not rely on its default gateway configuration to connect to the Web. The client computer only needs to know the route to the internal IP address of the nAppliance mISAE Server firewall.
- Non-Microsoft operating systems can authenticate with the nAppliance mISAE Server firewall.
- You can use Remote Authentication Dial-In User Service (RADIUS) to authenticate Web browsers connecting through the Web Proxy. Microsoft implements RADIUS as part of its Internet Authentication Service (IAS) servers, which is a service available on Windows Server 2003 and Windows 2000 Server family products.
- A connection time-out for Web browsers connected to the nAppliance mISAE Server firewall can be configured.
- A limit on the number of simultaneous connections can be configured.

To enable and configure the Web Proxy listener, perform the following steps.

4. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand your server name, expand the **Configuration** node, and then click the **Networks** node.
5. In the details pane, on the **Networks** page, click the **Networks** tab. In the list of networks, right-click the **Internal** network and click **Properties**.
6. In the **Internal Properties** dialog box, click the **Web Proxy** tab.
7. On the **Web Proxy** tab, select the **Enable Web Proxy clients** check box. Select the **Enable HTTP** check box and verify that the default port number in the **HTTP port** text box is **8080**.
8. Click the **Authentication** button.
9. In the **Authentication** dialog box, verify that the **Integrated** check box is selected. Select the **Basic** check box. Click **Yes** in the **mISAE Server Configuration** dialog box warning you that passwords are transmitted in clear text when sent by means of Basic authentication. Note that clear text communications can be captured and read by network analyzers because they are not encrypted. However, Basic authentication is supported by all browsers.
10. In the **Authentication** dialog box, click **OK**.
11. In the **Internal Properties** dialog box, click **Apply**, and then click **OK**.
12. Click the **Apply** button at the top of the details pane to save the changes and update the firewall policy.

Enabling the Firewall Client Listener

The Firewall Client is an optional client-side software component that you can install to enhance the level of security and accessibility for those host systems. The Firewall Client software can be installed on all 32-bit Windows operating systems. The Firewall Client software provides the following benefits:

- User credentials are transparently sent to the nAppliance mISAE Server firewall which enables user level authentication for access control.
- All Winsock applications are supported, including those requiring complex protocols (such as FTP, games, and voice or video applications).
- The Firewall client computer is independent of the default gateway configuration because it forwards Internet connection requests directly to the internal IP address of the nAppliance mISAE Server firewall.

The Firewall Client software is not required and is an optional component. However, you should consider enabling the Firewall client listener so that your nAppliance mISAE Server firewall is ready to accept incoming connection requests from Firewall clients when you decide to use the Firewall Client software on your network.

To enable the Firewall client listener on your nAppliance mISAE Server firewall computer, perform the following steps.

1. In the scope pane of the **Internet Security and Acceleration Server 2006** console, expand the server name, and then expand the **Configuration** node. Click the **Networks** node.
2. In the details pane, click the **Networks** tab. In the list of networks, right-click the **Internal** network and click **Properties**.
3. In the **Internal Properties** dialog box, click the **Firewall Client** tab.
4. On the **Firewall Client** tab, select the **Enable Firewall client support for this network** check box. In **mISAE Server name or IP address**, do not change the default setting. You may need to change this setting later depending on whether you have a DNS server on your LAN.
5. Click **Apply**, and then in the **Internal Properties** dialog box, click **OK**.
6. Click **Apply** at the top of the details pane to save the changes and update the firewall policy.

Creating an Internet Access Rule

By default nAppliance mISAE Server firewall, all traffic from internal network clients to the Internet is blocked. This default configuration provides a high level of security and prevents both internal and external users from accessing content through the nAppliance mISAE Server firewall.

You may want to connect to the Internet through your nAppliance mISAE Server firewall immediately. The simplest client configuration is the SecureNAT client. To connect internal network clients to the Internet as quickly as possible, but still remain secure from external threats, you will need confirm the following:

υ The default gateway setting on your LAN computers is set to the IP address of the internal interface of the nAppliance mISAE Server computer.

υ Your LAN computers are configured with a DNS server address that can resolve Internet host names. If you do not have a DNS server on your LAN capable of resolving Internet host names, you can configure your LAN computers to use the IP address of your ISP DNS server. For more details, see the DNS discussion later in this document (look forward to the pages 36).

υ There must be a firewall rule allowing access to the Internet protocols that you require.

The default gateway address and the DNS server address used by the computer on the LAN can be changed in **Control Panel**. The remaining step is to create an access rule on the nAppliance mISAE Server firewall computer. The access rule can be configured to allow a limited number of protocols outbound access to the Internet, and limited to a selected group of users to a selected group of websites, or you can create a firewall rule that allows all the users on your LAN access to all sites, at all times, using virtually any protocol.

The following example demonstrates how to create a firewall rule that allows everyone access to all protocols to all sites at all times. Perform the following steps to create the firewall rule.

7. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand your computer name, right-click the **Firewall Policy** node, point to **New**, and then click **Access Rule**.
8. On the Welcome to the New Access Rule Wizard page, type the name of the rule in the Access rule name text box. In this example, type All IP Traffic Outbound from Internal and click Next.
9. On the **Rule Action** page, select the **Allow** option and click **Next**.
10. On the **Protocols** page, select the **All outbound protocols** option and click **Next**.
11. On the **Access Rule Sources** page, click the **Add** button. In the **Add Network Entities** dialog box, click the **Networks** folder. Double-click the **Internal** network, and then click **Close**.
12. The Internal network should appear in the This rule applies to traffic from these sources list. Click Next.
13. On the **Access Rule Destinations** page, click the **Add** button. In the **Add Network Entities** dialog box, click the **Networks** folder. Double-click the **External** network, and then click **Close**.
14. The External network should appear in the This rule applies to traffic sent to these destinations list. Click Next.
15. On the User Sets page, confirm that All Users appears in the This rule applies to requests from the following user sets and click Next.
16. On the Completing the New Access Rule Wizard page, click Finish.
17. Click the **Apply** button at the top of the scope pane to save the changes and update the firewall policy.

You can now access the Internet from computers on your LAN. You should consider strengthening security for outbound connections after you have confirmed that your nAppliance mISAE Server firewall is successfully allowing access to the Internet. One effective method for creating a secure access policy is to use the network templates included with mISAE Server 2006. For detailed information about the network templates, see the mISAE Server 2006 Help file.

Managing and Maintaining the Firewall

The nAppliance mISAE Server firewall, like any other network device, must be managed and maintained. Common management and maintenance tasks include:

- Using Windows Update to keep the software updated.
- Using Remote Desktop to manage the nAppliance mISAE Server firewall from computers on the LAN.
- Using Remote Management Console to manage the nAppliance mISAE Server firewall from a management station on the LAN.
- Using Remote Assistance to obtain help with nAppliance mISAE Server firewall troubleshooting.
- Configuring nAppliance mISAE Server logs and monitoring.
- Setting up Client installation Share to allow Firewall Client software to be installed on network client systems.
- Creating a Web Proxy Automatic Discovery (WPAD) entry to support Web browser and Firewall client automatic configuration.
- Configuring Time Synchronization to use the nAppliance mISAE Server server as a time server for your LAN.
- Using a Remote Access virtual private network (VPN) for remote management and network connectivity.

Windows Update

You can use the Microsoft Windows Update website to update the operating system with the latest service packs and hot fixes. The process can be configured to download system updates and install them automatically, or it can be configured to wait for nAppliance mISAE Server administrator approval. You can configure the Automatic Updates tab with one of the following options:

- Notify me before downloading any updates and notify me again before installing them on my computer.
- Download the updates automatically and notify me when they are ready to be installed.
- Automatically download the updates, and install them on the schedule that I specify.

Perform the following steps to configure the automatic update feature of the nAppliance mISAE Server firewall.

1. Click **Start**, click **Control Panel**, and then click **System**.
2. In the **System Properties** dialog box, click the **Automatic Updates** tab.
3. On the Automatic Updates tab, select the Keep my computer up to date check box.
4. Select one of the options in the **Settings** frame that best meets your requirements.

Remote Desktop

The nAppliance mISAE Server firewall is preconfigured to allow a single concurrent Remote Desktop Connection to the server. You can use this connection to perform remote management. The Remote Desktop Protocol (RDP) is used to connect to the nAppliance mISAE Server firewall Remote Desktop, where you can access the **Microsoft Internet Security and Acceleration Server 2006** management console to manage the firewall.

You can access the nAppliance mISAE Server firewall through an internal network computer or a computer located anywhere on the Internet. This can be done by adjusting a system policy rule.

⇨ To enable external users access to the Remote Desktop Service on the nAppliance mISAE Server firewall, perform the following steps.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand the server name, right-click the **Firewall Policy** node, and then click **Edit System Policy**.
2. In the **System Policy Editor** dialog box, locate the **Remote Management** group, and then click the **Terminal Server** entry.
3. On the **General** tab, confirm that the **Enable** check box is selected.
4. Click the **From** tab and click the **Add** button to the right of the **This rule applies to traffic from these sources** list.
5. In the **Add Network Entities** dialog box, click the **Networks** folder, double-click **External**, and then click **Close**.
6. In the **System Policy Editor** dialog box, click **OK**.
7. Click **Apply** to save the changes and update firewall policy.

External computers will now be able to connect to the RDP service on the nAppliance mISAE Server firewall.

Remote nAppliance mISAE Server Management Console

You can manage the nAppliance mISAE Server firewall from a management station on the LAN by installing the **Microsoft Internet Security and Acceleration Server 2006** management console on the management station. The **Microsoft Internet Security and Acceleration Server 2006** management console on the management station can manage virtually any aspect of the nAppliance mISAE Server firewall configuration.

The nAppliance mISAE Server Management Console can be installed by placing the nAppliance Appliance Installation DVD into the management station’s DVD-ROM drive, and then selecting the option to install the Management Console from the Autorun page. The management station will be able to connect to the nAppliance mISAE Server firewall because there is a system policy rule in place that allows internal network hosts to connect using the nAppliance mISAE Server Management Console.

Configuring Monitoring, Reporting and Logging

The nAppliance mISAE Server firewall has a comprehensive logging and reporting facility. There are some logging and reporting options that you should configure immediately to get the most from the nAppliance mISAE Server logging and reporting feature set. These options include:

υ Configure Firewall logging

υ Configure Web Proxy logging

The nAppliance mISAE Server automatically stores log files in the folder “D:\logs\”.

Configure Firewall Logging

The Firewall log records connections from SecureNAT and Firewall clients on the Internal network and External network. Firewall logging can be configured to use one of several storage methods. Each storage method has its own advantages and dmmISAEEdvantages. Firewall logging storage methods include:

υ File logging

υ SQL database logging

υ MSDE database logging

Perform the following steps to configure the Microsoft Firewall service

basic logging properties.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand your server name, and then click the **Monitoring** node.
2. In the details pane, click the **Logging** tab.
3. In the task pane, click the **Tasks** tab, and then click **Configure Firewall Logging**.
4. The **Log** tab appears in the **Firewall Logging Properties** dialog box. Select the Log storage format that best meets your needs. The **File** format option is best when you need to copy log file information to a third-party application on another computer. The **SQL database** format option is best when you have an SQL database on the Internal network and have the expertise to manage an SQL database. The **MSDE database** format option is an excellent option when do not want to use SQL text-based logging.
5. Select the **File** format option. From the **Format** list, select the **mISAE Server file format**. This format will save log file entries using the local time configured on the nAppliance mISAE Server firewall to stamp the log entries. Note that when you use file-based logging, you will not be able to perform queries on the log file in real time.
6. Click **Apply**, and then click **OK**.
7. Click the **Apply** button at the top of the details pane to save the changes and update firewall policy.

Configure Web Proxy Logging

The Web Proxy logs contain information about connections from Web Proxy clients. Web Proxy logging can be configured to use a number of different storage methods. Each storage method has its own advantages and dmmISAEEdvantages. Web Proxy storage methods include:

- File logging
- SQL database logging
- MSDE database logging

Perform the following steps to configure the Web Proxy basic logging properties.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand your server name, and then click the **Monitoring** node.
2. In the details pane, click the **Logging** tab.
3. In the task pane, click the **Tasks** tab, and then click **Configure Web Proxy Logging**.
4. The **Log** tab appears in the **Web Proxy Properties** dialog box. Select the Log storage format that best meets your needs. The **File** format option is best when you need to copy log file information to a third-party application on another computer on the Internal network. The **SQL database** format option is best when you have an SQL database on the Internal

network and have the expertise to manage an SQL database. The **MDSE database** format option is an excellent option when do not want to use SQL or text-based logging.

5. Select the **File** format option. From the **Format** list, select the **mISAE Server file format**. This format will save log file entries using the local time configured on the nAppliance mISAE Server firewall to stamp the log entries. Note that when you use file-based logging, you will not be able to perform queries on the log file in real time.
6. Click **Apply**, and then click **OK**.
7. Click the **Apply** button at the top of the details pane to save the changes and update firewall policy.

Setting Up Client Installation Share

The Client Installation Share contains the Firewall Client installation files. The Firewall Client software can be installed on network client systems by having the clients connect to the Client Installation Share located on the nAppliance mISAE Server firewall computer, or on another internal network computer.

In the current nAppliance mISAE Server release, the Client Installation Share is installed on the nAppliance mISAE Server firewall computer. However, network clients will not be able to access the installation files because the Server service is dmmISAEEbled. The Server service must be manually enabled before network client computers can connect to the share. However, enabling the Server service on the firewall is not recommended.

Another option is to use the nAppliance Appliance Installation DVD and install the Client Installation Share on a secure file server on the LAN. You can install the Client Installation Share on a computer other than the nAppliance mISAE Server firewall by inserting the nAppliance Appliance Installation DVD into the server’s DVD-ROM drive and selecting the Install Client Installation Share option from the Autorun menu.

Supporting Web-Proxy and Firewall Client Automatic Discovery

The Firewall and Web Proxy client computers can be configured to automatically obtain configuration information from the nAppliance mISAE Server firewall computer. Automatic discovery enables the Web Proxy and Firewall client computers on the LAN to automatically discover the location of the nAppliance mISAE Server firewall and obtain configuration information. The entire process is transparent to users, and it allows mobile users to move to and from the LAN and automatically obtain connection and configuration information required to connect to the Internet through the nAppliance mISAE Server firewall.

There are two methods that support the Web Proxy and Firewall client automatic discovery mechanism:

- DNS Wpad entry
- DHCP Option 252

DNS Wpad Entry

A wpad alias entry is placed on the DNS server on your LAN. The entry maps the name *wpad* to the DNS Host (A) record for the nAppliance mISAE Server firewall's internal interface. Requirements for the DNS wpad alias entry include:

- A DNS server on the LAN.
- A Host (A) entry for the nAppliance mISAE Server firewall's internal interface.
- An alias (CNAME) record for the name wpad that maps to the Host (A) record for the nAppliance mISAE Server firewall's entry in DNS.
- Computers on the LAN must be able to correctly qualify the unqualified name *wpad*. The best way to do this is to join the LAN computers to the same domain as the wpad entry.

If you already have a Windows DNS server on your LAN, perform the following steps to create the DNS wpad entry.

1. On the DNS server, from the **Administrative Tools** menu, open the **DNS** console.
2. In the left pane of the **DNS** management console, expand the server name, and then expand the **Forward Lookup Zones** node. Click your domain name.
3. Right-click your domain name and click the **New Alias (CNAME)** command.
4. In the Alias name (uses parent domain if left blank) text box, enter the name wpad.
5. Click the **Browse** button. In the **Browse** dialog box, double-click your server name in the **Records** list. Then double-click the **Forward Lookup Zones** entry in the records list. Next, double-click your domain name in the **Records** list. Find the resource record for the nAppliance mISAE Server firewall in the **Records** list and click it, and then click **OK**.
6. The name of the nAppliance mISAE Server firewall now appears in the **Fully qualified domain name (FQDN) for target host** text box. Click **OK**.
7. The wpad alias entry now appears in the resource record list in the results pane of the **DNS** console.

DHCP Option 252

You can use the DHCP option 252 wpad method for computers using DHCP to obtain IP addressing information. Requirements for this option include:

- A DHCP server on the LAN.

υ Computers on the LAN use DHCP to obtain IP addressing information.

υ Web Proxy client users must be logged on as local administrators or as members of the Power Users group.

Perform the following steps if you have a DHCP server on your LAN.

1. From the **Administrative Tools** menu on the DHCP computer on the LAN, open the **DHCP** console.
2. In the scope pane of the **DHCP** console, right-click the server name and click the **Set Predefined Options** command.
3. In the **Predefined Options and Values** dialog box, click the **Add** button.
4. In the **Option Type** dialog box, in the **Name** text box, enter **WPAD**. Select the **String** option in the **Data type** list. Type **252** in the **Code** text box and type **DHCP wpad entry** in the **Description** text box.
5. In the **Predefined Options and Values** text box, type the following information in the **String** text box.

   http://<Computer_Name>:<AutoDiscoveryPortNumber>/Wpad.dat
6. Where the *Computer_Name* entry is the DNS name (fully qualified domain name) of the nAppliance mISAE Server computer and the *AutoDiscovveryPortNumber* is the port number that the nAppliance mISAE Server firewall uses to publish automatic discovery information. This is TCP
   port 80 by default. For example, if the computer name is firewall.*domain.com*, the value would look as follows:

   http://firewall.domain.com:80/wpad.dat
7. In the Predefined Options and Values dialog box, click OK.

> **Note**
>
> The user must be logged on as an Administrator or Power User in Windows 2000 or as an Administrator, a Power User, or a member of the Network Configuration Operators group in Windows XP for the DHCP automatic discovery method to work. For more information, see Automatic Proxy Discovery in Internet Explorer with DHCP Requires Specific Permissions (http://go.microsoft.com/fwlink/?LinkID=27334).

Configuring Time Synchronization

You may want to use the firewall as a time server for your LAN. A time server is a computer that provides accurate time to other computers on the LAN. This increases security on your network by providing accurate time to all hosts on the network so that auditing and logging entries have the correct time. In addition, many network protocols require accurate time to function properly.

To obtain the most accurate time possible, the nAppliance mISAE Server firewall needs to access a time server on the Internet. Even if you do not want the nAppliance mISAE Server firewall to be a time server for your LAN, you can configure the nAppliance mISAE Server firewall to allow computers on your LAN to contact their own Internet time servers.

For example, if you have a Windows domain on the Internal network, you can configure the PDC emulator to use the nAppliance mISAE Server firewall as its time server. If you do not have a Windows domain, you can configure the individual clients to synchronize with nAppliance mISAE Server time server.

You can create an access policy enabling both the nAppliance mISAE Server firewall and the computers on the LAN to contact Internet time servers.

Perform the following steps on the nAppliance mISAE Server firewall to create this access policy.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, expand your server name, right-click the **Firewall Policy** node, point to **New**, and then click **Access Rule**.
2. On the Welcome to the New Access Rule Wizard page, type the name for the rule in the Access rule name text box. In this example, type Network Time requested by Local Host and Internal and click Next.
3. On the **Rule Action** page, select the **Allow** option and click **Next**.
4. On the **Protocols** page, in the **This rule applies to** list, select the **Selected protocols** option. Click the **Add** button. In the **Add Protocols** text box, click the **Infrastructure** folder, and then double-click the **NTP (UDP)** entry. On the **Add Protocols** dialog box, click **Close**.
5. On the **Protocols** page, click **Next**.
6. On the **Access Rule Sources** page, click the **Add** button. In the **Add Network Entities** dialog box, click the **Networks** folder. Double-click the **Local Host** entry, double-click the **Internal** entry, and then click **Close**.
7. On the Access Rule Sources page, click Next.
8. On the **Access Rule Destinations** page, click the **Add** button. Click the **Networks** folder, double-click the **External** entry, and then click **Close**.
9. On the Access Rule Destinations page, click Next.
10. On the **User Sets** page, click **Next**.
11. On the Completing the New Access Rule Wizard page, click Finish.

The nAppliance mISAE Server firewall is now able to perform time synchronization with Internet based time servers. If you want the Internal network clients to synchronize with the nAppliance mISAE Server firewall, you will need to create an access rule allowing the Internal network access to the Local Host network using the Network Time Protocol. In addition, the clients will need to be configured to use the correct time server. In Windows XP, the time server configuration is performed in the **Date and Time** properties dialog box on the **Internet Time** tab.

It is also possible to configure a time server with the Web-Interface, but this is explained at the pages 53/54.

Remote Access VPN

A Remote Access virtual private network (VPN) allows computers located virtually anywhere in the world to connect to computers in the Internal network through the nAppliance mISAE Server firewall using a VPN connection. The only requirement is that the client computer has an Internet connection. You can manage your nAppliance mISAE Server firewall from home or any other location by creating a VPN connection to the nAppliance mISAE Server firewall computer. In addition, you can access other computers on the Internal network protected by the nAppliance mISAE Server firewall computer. For comprehensive documentation on how to create and configure site-to-site VPN connections, see the nAppliance mISAE Server Help file and the Microsoft mISAE Server 2006 website (http://www.microsoft.com/mmISAEEserver/2006/default.mspx).

Disaster Recovery and Change Management

There are a number of tasks you can perform that address dmmISAEEster recovery and change management issues. These tasks include:

- nAppliance mISAE Server firewall settings backup and restore
- System backup and restore
- Back to factory settings

nAppliance mISAE Server Firewall Settings Backup and Restore

Firewall change management can be accomplished by backing up the nAppliance mISAE Server firewall configuration settings before making changes. The backed up settings can be restored in the event subsequent changes made to the firewall configuration have unexpected or undesirable results. The nAppliance mISAE Server firewall has an integrated backup feature that saves almost all of its configuration settings.

To back up the nAppliance mISAE Server firewall configuration, perform the following steps.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, right-click the server name, and then click **Back Up**.
2. In the **Backup Configuration** dialog box, select a location for the backup file in the **Save in** list. Type a name for the backup file in the **File name** text box, and then click **Backup**.
3. In the **Set Password** dialog box, in the **Password** text box, type a password to protect the backup file. In the **Confirm password** text box, confirm the password and click **OK**.
4. In the Exporting dialog box, when it informs you that The array data has been successfully backed up, click OK.

After the backup is complete, copy the file to a safe location separate from the nAppliance mISAE Server firewall computer.

To restore the nAppliance mISAE Server firewall to the settings contained in the backup file, perform the following steps.

1. In the scope pane of the **Microsoft Internet Security and Acceleration Server 2006** management console, right-click the server name, and then click **Restore**.
2. In the Restore Configuration dialog box, locate the backup file, and then click Restore.
3. In the **Type Password to Open File** dialog box, type the password that you assigned to the file and click **OK**.
4. In the **Importing** dialog box, after you are informed that **The array data has been successfully restored**, click **OK**.
5. Click the **Apply** button to save the changes and update the firewall policy to the settings contained in the backup file.
6. In the **mISAE Server Warning** dialog box, select the **Save the changes and restart the service(s)** option and click **OK**.

System Backup and Restore

It is a good security policy to backup the entire contents of the nAppliance mISAE Server firewall hard disk, including the nAppliance mISAE Server firewall software and underlying operating system. The Windows Backup utility can be used to accomplish this task.

To perform a backup or a restore over the Web-Management read Chapter “nAppliance mISAE Server Web-Management” → “Maintenance” → “Backup” and “Restore”.

The Web-Management can also be used to configure scheduled backup tasks.

Alternative Backup method: Full Harddisk Backup

You have the possibility to create a full hard disk image of the appliance through the built-in flash device. This backup writes an installation source file to a Windows- or SSH-share, please follow the steps below to create an hard disk image.

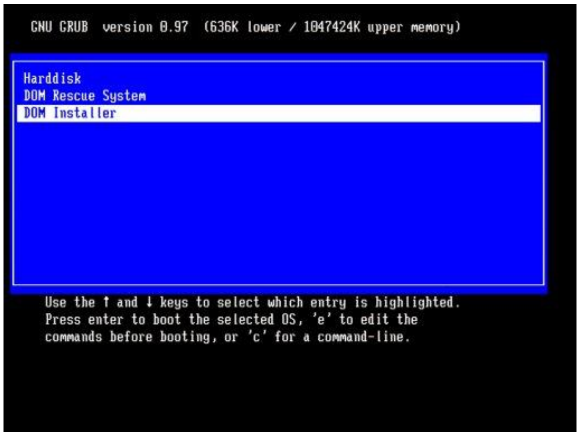
Important

You will need to reboot the Appliance into the DOM Installer! The Appliance will be offline during the backup process, which will take several hours, depending on the amount of data contained on the hard disk.

To back up the nAppliance mISAE Appliance hard disk, perform the following steps.

Step 1:

Reboot the Appliance and select "DOM Installer" from the GRUB boot loader menu:



```
GNU GRUB  version 0.97  (636K lower / 1047424K upper memory)

 Harddisk
 DOM Rescue System
 DOM Installer

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, or 'c' for a command-line.
```

Step 2:

When asked to start the installation on the active console, hit return. You will be forwarded to the installers main menu.

Step 3:

Select the option "HDBKP"

Step 4:

Choose the network interface which you want to use to connect to the network share.

Step 5:

Select the type of network share which should be used to connect to the server:

(1) CIFS:

Use this option if you are using a Windows share to back up the appliance.In the next dialog you have to configure the network interface. The IP-Address can be gained via DHCP or manual configuration. If you are using DHCP you can ignore the dialog elements “Netmask”, “Domain Name Server” and “Default Gateway”. The Windows share must be specified in the form “//HOSTNAME/SHARENAME” in the “Installation Host” field (the field “Installation Directory” will be ignored). Additionally you have to provide a username and password which will be used to connect to the share.

(2) SSHFS:

Select this option, if you have a running SSH server with the required install files. All steps are analog to the “Install from Windows share” method in the paragraph above except the interactive password request, which means that you are asked for the password after you entered the configuration information. Note that you have to enter a only a valid hostname or IP-Address into the “Installation Host” field and an absolute path to the installation source file (.img file located in the files\sources\ directory of the DVD/CD-ROM). If your SSH server is running on an non-default port (22), please enter the correct port in the "SSH Port" field.

Important

Make sure that you have write permissions on the share which you use for backing up the hard disk! Depending on the amount of data stored on the Appliance, you will need at least 5 gigabytes of free space.

Step 6:

After entering the network data, the backup process will start automatically.

Step 7:

A dialog box will inform you as soon as the backup has been finished. Hit enter to return to the main menu, and select "Reboot" to restart the Appliance into Windows to return to normal operation.

Important

The resulting IMG file located in the network share can be used as a data source for the Appliance Installer. Please follow the instructions in the next chapter to restore the hard disk from this installation source.

Back to Factory Settings

The Back to Factory Settings option enables you to return your nAppliance Appliance back to its original out of box factory settings. The following steps are required to return the computer to its original factory settings.

Note that you have 2 possibilities to reinstall the Appliance: you can start the installer using the Flash device which is built in the Appliance and fetching the main installation sources from a Windows share or via SSHFS, or you can set up by using an USB DVD-ROM to boot from the nAppliance Appliance DVD.

If you are planning to install through a Windows share or the Secure Shell Filesystem (SSHFS), please be sure copy the installation source from the nAppliance Appliance Installation DVD contents into the shared directory. The Installation source can be found in the files\sources subdirectory of the DVD (file with extension “img”).

Important

A new installation leads to a complete loss of all data and programs which are installed on the nAppliance Appliance. After you complete the Back to Factory Settings routine, you can restore system settings from previously created backups.

To reinstall the Appliance with the help of an **USB DVD-ROM drive**, follow these instructions:

Step 1:

Plug in the DVD-ROM drive into one of the USB ports located on the front. Reboot the nAppliance Appliance and boot from the Appliance DVD.

Step 2:

Follow the prompts generated by the nAppliance Appliance installation routine given by the next steps.

Step 3:

The first dialog serves to choose the output interface:

1) VGA:	Output installation dialogs to the monitor (recommended)
2) Serial:	Output installation dialogs to COM-1 (use a null modem cable to connect to the appliance, serial settings: 19200bps, 8N1, no flow control)

Step 4:

Choose a language, which will be used during the installation progress. German and English are available.

Step 5:

The data source can be chosen in this dialog:

(1) DVD-ROM:

Appliance software image can be found on the DVD or CD-ROM disc.

(2) CIFS:

Use this option if you are using a Windows share to set up the appliance server. Select a network interface, where the machine is connected to the network. In the next dialog you have to configure the network interface. The IP-Address can be gained via DHCP or manual configuration. If you are using DHCP you can ignore the dialog elements “Netmask”, “Domain Name Server” and “Default Gateway”. The Windows share must be specified in the form “//HOSTNAME/SHARENAME” in the “Installation Host” field (the field “Installation Directory” will be ignored). Additionally you have to provide a username and password which will be used to connect to the share.

(3) SSHFS:

Select this option, if you have a running SSHFS server with the required install files. All steps are analog to the “Install from Windows share” method in the paragraph above except the interactive password request, which means that you are asked for the password after you entered the configuration information. Note that you have to enter a only a valid hostname or IP-Address into the “Installation Host” field and an absolute path to the installation source file (.img file located in the files\sources\ directory of the DVD/CD-ROM).

(4) HDD:

The Appliance contains a partition with the Installation source, providing you with the possibility to re-install the Appliance without the need of a CD-ROM or Network support. This option is only available when booting from the Flash device.

Note

After selecting the CIFS or SSHFS installation method, networking will be started on the machine. You have to provide at least an IP address plus network mask and the IP-address of your CIFS/SSHFS-server and/or a valid DNS server to the installer and a username/password combination to access the share. Please use the connector assignment picture below to select the correct network interface for installation.

Make sure that you have copied the installation source file (IMG file located in the files\sources directory of the Appliance Installation DVD, or the backup file which has been created with the previous chapter) to the network share before connecting to the share.

Although no data will be written to the share in this step, make sure that you have **write permissions** and that the **"read only" flag is not set** on the installation source file!

Step 6:

If more than one valid image is available the installer will give you a list of installable images from the directory which you’ve selected in the previous step. Please select the image which you want to install by pressing the appropriate number. If only one image is available the installer automatically selects this image.

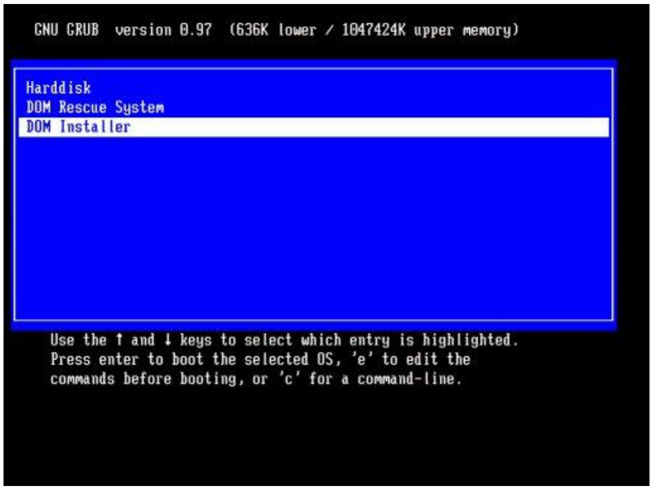
Step 7:

Confirm the installation to start the deployment of the selected package.

The hard drive will be re-partitioned now and the images will be deployed. This step may take some minutes.

After the installation has been deployed, reboot your computer and follow the instructions in the chapter *“Maintenance / Restore”* to restore a backup file, or *“Power on the Appliance”* to configure the nAppliance Appliance from scratch.

If you prefer a network based reinstallation of the Appliance, reboot the Appliance and select **"DOM Installer"** from the GRUB boot loader menu as shown in the picture below. Afterwards, follow the instructions beginning with **Step 4** of the previous guide.



```
GNU GRUB  version 0.97  (636K lower / 1047424K upper memory)

Harddisk
DOM Rescue System
DOM Installer

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, or 'c' for a command-line.
```

Connector Assignment for Network Installations

nAppliance mISAE Server Firewall Network Services Support

There are two network services that provide important infrastructure support for the nAppliance mISAE Server firewall computer and network hosts that make connections through the nAppliance mISAE Server firewall. These network services are:

- The DNS server service.
- The DHCP server service.

DNS Server

The nAppliance mISAE Server firewall depends on a DNS server to resolve Internet host names. There are a number of ways that you can provide DNS server support for the nAppliance mISAE Server firewall:

- Use your ISP DNS server.
- Use your own DNS server on the Internal network.
- Use a caching-only DNS server on the nAppliance mISAE Server firewall.
- Use a caching-only DNS server on a perimeter network segment.

The simplest approach is to use your ISP DNS server. The drawback of using only your ISP DNS server is that you will not be able to use DNS to resolve computer names on your Internal network.

If you already have a DNS server on the Internal network, you can use it to resolve Internet host names. All Active Directory domains require at least one DNS server, and you can use that DNS server to resolve Internet host names for your Internal network clients. Configure the Internal interface of the nAppliance mISAE Server firewall to use this DNS server after configuring the Internal network DNS server to resolve Internet names.

A caching-only DNS server does not contain DNS zone or domain information. Instead, it queries other DNS servers on the Internet for the IP address of a given host, and then caches the result before forwarding the answer to the computer requesting the name resolution. You can install a caching-only DNS server on the nAppliance mISAE Server firewall, and then configure the nAppliance mISAE Server firewall to use itself as its DNS server.

Another caching-only DNS server solution takes advantage of a perimeter network configuration. If your nAppliance mISAE Server firewall has three or more network interfaces, one of the network interfaces can be connected to a perimeter network. You can then install and configure a caching-only DNS server on the perimeter network. If you have a DNS server on the Internal network, you can configure that DNS server to use the perimeter network DNS server as a forwarder.

For more information on DNS setup and configuration, see the Windows Server 2003 Help and Support Center or the Windows 2000 Help.

DHCP Server

A DHCP server assigns IP addresses to computers configured as DHCP clients. In a typical nAppliance mISAE Server firewall configuration, the DHCP server assigns addresses to computers on the Internal network and the VPN Clients network. The DHCP server itself can be located on:

- The nAppliance mISAE Server firewall computer.
- A computer on the Internal network.

The DHCP server can be installed on the nAppliance mISAE Server firewall computer if there are no other server computers on the Internal network on which you can install a DHCP server. The reason that installing the DHCP server on your nAppliance mISAE Server firewall is a second choice is that VPN clients will not be able to obtain an IP address from the DHCP server on the nAppliance mISAE Server firewall itself. You must configure a static address pool of IP addresses to assign to VPN clients when the DHCP server is installed on the nAppliance mISAE Server firewall. Another reason to keep the DHCP server off the firewall is to reduce the number of applications running on the firewall, all of which create potential portals for attack.

Placing the DHCP server on a computer located on the Internal network enables the VPN clients to obtain IP addressing information from the DHCP server. In addition, the nAppliance mISAE Server firewall is able to automatically define the VPN Clients network based on the IP addresses it obtains from the DHCP server. Another advantage is that you can optionally install the DHCP Relay Agent routing service on the nAppliance mISAE Server firewall and assign DHCP options to the VPN Clients network, such as a primary domain name.

nAppliance mISAE Server Web-Management

A simple and flexible web interface is provided by your nAppliance mISAE Server. Connecting to the nAppliance mISAE Server is described in the first chapter.

Navigation in the Web Interface

The top of each page of the Web UI is composed of a status area, as well as primary and secondary navigation bars. The body of each page of the Web UI is composed of the content area

Following is a description of these sections:

Status Area: The top band of the window, the status area displays the server host name and status. There are four possible Status displays (Normal, Information, Warning, Critical)

You can click **Status: <status type>** to get detailed information about the status of the server.

Navigation Bars: Immediately below the status area are the navigation bars. The above illustration shows the primary (blue) and secondary (gray) navigation bars. The primary navigation bar lists the available Web UI tasks by type. The secondary navigation bar lists the related subtasks available for the selected primary task.

Content Area: This section of the Web UI describes the management activities you can perform on that page. This text may also provide instructions about tools available to perform the selected tasks.

Many of the task pages include an **Object/Task** Selector. The Object/Task Selector is simply a table listing the objects you can manage or configure, their descriptions, and the tasks you can perform. The leftmost column of the Object/Task Selector contains a radio button you click to select a given object. In the event that multiple objects in the Object/Task Selector, can be selected, the leftmost column will contain a check box rather than a radio button. The rightmost column lists the tasks you can perform.

To navigate through the Web UI

1. On the primary navigation bar, click the general type of task you want to perform.
2. On the secondary navigation bar or in the list of tasks in the content area of the page, click the specific type of task you want to perform.
3. In the content area of the subsequent page: If an Object/Task Selector is available, select the object you want to manage or configure by clicking the radio button to the left of the object

name. Then select the task you want to perform from the Tasks list on the right. Depending on the page, the Object/Task Selector may provide search capabilities, as well as the ability to page though the information contained in the table.

4. If an Object/Task Selector is not available, enter the data in the fields indicated to accomplish the chosen task.
5. When you are finished with each task, choose **OK** to confirm your changes, or **Cancel** to retain the previous settings.
6. Once the change or cancellation has processed, the previous page will display.
7. If you are on a property page and select another navigation bar item, a pop-up window displays with the message **Click OK to discard any changes**. This gives you the chance to either commit to or reject the changes before moving to the next selected page.

Welcome

If you choose Welcome in the primary bar you have the possibility to perform following actions:

- **Set Server Name**: Here you can change the computer name of the nAppliance mISAE Server
- **Set Administrator Password**: Here you can set the Administrator name or the Administrator password.
- **Set Default Page**: You can set the default page of the Web-Management. This will be the page that displays each time you access the server.

Set server name

1. On the primary navigation bar, choose **Welcome**.
2. Choose **Set Server Name**.
3. In the boxes provided, type the appropriate **Server name** and Domain Name System suffix (**DNS suffix**). The optional DNS suffix is appended to the host name to create the fully qualified machine name.
4. Select whether the server will be part of a **workgroup** or a **domain**.
5. If the server will be part of a domain, type the **User** name and **Password** of the person who has permission to add client computers to the domain.
6. Choose **OK**.
7. When prompted to reboot the server, you may either accept or cancel the reboot.
8. If you choose **OK**, the server will reboot and the Restarting page will appear.
9. If you choose **Cancel**, the changes to the server identity will not take effect until the next reboot.

Set administrator password

1. Log on to the server as **Administrator**.
2. On the primary navigation bar, choose **Welcome**.
3. Choose Set Administrator Password.
4. Type the new name for the administrator account in the **User name** box.
5. Type the current administrator password in the **Current password** box.
6. Type the new administrator password in the **New password** box.
7. Retype the new administrator password in the **Confirm new password** box.

8. Choose **OK**.

Setting the default page

1. From the primary navigation bar, choose **Welcome**.
2. From the **Welcome** page, choose **Set Default Page**.
3. On the **Set Default Page**, choose whether the Welcome page or the Status page become the default page.
4. Choose **OK**.

Status

From the Status page, you can view status alerts, system resources, and system information. The upper left quadrant displays system alerts and the upper right quadrant displays status information about system resources. After selecting an alert or system resource, detailed information about the selection is displayed in the bottom half of the screen.

There are four possible Status displays:

- **Normal** (green text): The **Alert** page will indicate that there are no messages
- **Information** (grey text): The **Alert** page will list the issues as hyperlinks, with an information icon next to each issue the system has encountered.
- **Warning** (yellow text): The **Alert** page will list the errors as hyperlinks, with a warning icon next to each error that the system has encountered.
- **Critical** (red text): The **Alert** page will list the errors as hyperlinks, with a critical icon next to each error the system has encountered.

You can click **Status: <status type>** to get detailed information about the status of the server.

Clear an alert

1. To clear an alert, choose Status from the primary navigation bar.
2. Choose the alert you want to clear.
3. Choose the action you want to address the alert conditions, or choose **Clear Message** to clear the alert message without changing the configuration of your server.

Show system information

1. From the primary navigation bar, choose **Status**.
2. From the secondary navigation bar, choose **System Information**.

Network

From the Network page, you can choose which of the following network-related properties of the server to configure:

- **Identification**: Set the name and domain membership of the server.
- **Global Settings**: Configure network settings that apply to all network adapters on the server.
- **Interfaces**: Configure the properties of each network adapter on the server.
- **Administrator**: Change the password of the user account you are using to access the server administration Web site.
- **Administration Web Site**: Specify which IP address(es) and port are used to access the administration Web site.

Identification

The server must be given a name. Client computers use this name to access the file shares that reside on this server.

The server can be configured as a member of one of the following groups:

- Microsoft Windows NT 4 domain
- Microsoft Active Directory domain
- Workgroup

Set the name and domain membership of the server

1. On the primary navigation bar, choose **Network**.
2. Choose **Identification**.
3. In the boxes provided, type the appropriate **Server name** and Domain Name System suffix (**DNS suffix**). The optional DNS suffix is appended to the host name to create the fully qualified machine name.
4. Select whether the server will be part of a **workgroup** or a **domain** and type the workgroup or the domain name in the appropriate box.
5. If the server will be part of a domain, type the **User** name and **Password** of the person who has permission to add client computers to the domain.
6. Choose **OK**.
7. When prompted to reboot the server, you may either accept or cancel the reboot.

8. If you choose **OK**, the server will reboot and the Restarting page will appear.
9. If you choose **Cancel**, the changes to the server identity will not take effect until the next reboot.

> **Note**
> This configuration is actually the same as the Option **Set Server Name** in the **Welcome** tab

Global Settings

From this page, you can change the overall network settings for your server by configuring the IP settings as well as specifying the DNS suffixes and the LMHOSTS and HOSTS file to use. These files can be used to resolve the names of any computer or device. Note that the DNS suffix used here applies when the server is trying to resolve a host or domain name. You can also add routes for all of your network adapters.

Automatically set or change DNS suffixes

1. On the primary navigation bar, choose **Network**.
2. Choose **Global Settings**.
3. Select the **DNS Resolution** tab.
4. Select the **Append primary DNS suffix** button.
5. Optional: you may choose to **Append parent suffixes of the primary DNS suffix** by selecting the check box.
6. Choose **OK**.

Manually modify specific DNS suffixes

1. On the **Network** page, choose **Global Settings**.
2. Select the **DNS Resolution** tab.
3. Select the **Append the following DNS suffixes, in order of use** button.
4. To add a domain suffix, type the DNS suffix you want to add in the **Domain suffix** box, and then choose **Add**.
5. To remove a domain suffix, use the **Up** and **Down** buttons to scroll through the list of domain suffixes. Select the suffix you want to delete, and then choose **Remove**.
6. Choose **OK**.

Edit the Hosts file

1. On the **Network** page, choose **Global Settings**.
2. Select the **TCP/IP Hosts** tab. By default, the **Hosts file** box contains the current Hosts file configuration.
3. Change the Hosts file by clicking in the box and editing the information.
4. Choose **OK**.

Edit the LMHOSTS file

1. From the primary navigation bar, choose **Network**.
2. Choose **Global Settings**.
3. Select the **NetBIOS LMHOSTS** tab.
4. Select the **Enable LMHOSTS lookup** check box. By default, the box below contains the current LMHOSTS file configuration; however, if there are no entries to be seen, the box will be empty.
5. Edit the LMHOSTS file by clicking in the box and changing the information.
6. Choose **OK**.

Add a route

1. On the **Network** page, choose **Global Settings**.
2. Select the **Routing** task.
3. To add an active route select the **Add active network route** from the **Tasks** list at the **IPv4 Active Routing Table**.
4. To add a persistent route select the **Add persistent route** from the **Tasks** list at the **IPv4 Persistent Routing Table**.
5. Choose the network interface.
6. Insert the network destination, the subnetmask and the gateway for your new route.
7. Click **OK** to add the new route.

Remove a route

1. On the **Network** page, choose **Global Settings**.
2. Select the **Routing** task.
3. To remove an active route choose a route in the **IPv4 Active Routing Table** and select the **Delete active network route** task.
4. To remove a persistent route, choose a route in the **IPv4 Persistent Routing Table** and select the **Delete persistent network route** task.
5. Click **OK** to remove the route.

Interfaces

A network adapter provides the physical interface, or connector, and the hardware to let a computer access a network.

From the **Interfaces** page, you can perform one of the following tasks:

- Change the name of the connection.
- Set or change the Internet Protocol (IP) addresses, gateway addresses, subnet masks, and metrics.
- Set or change how the server resolves DNS names.
- Set or change the configuration of the Windows Internet Naming Service (WINS) clients.

Rename an interface connection

1. From the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the interface connection you want to rename.
4. In the **Tasks** list, choose **Rename**.
5. In the **New connection name** box, type the new name of the interface connection.
6. Choose **OK.**

Set or change the IP settings on the General tab

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **IP**.

5. Select the **General** tab.
6. Select whether to obtain the configuration automatically from the DHCP server, or to statically configure the IP address(es).
7. If you choose to obtain the configuration from the DHCP server, choose **OK**.
8. If you have chosen to use static IP settings, enter the IP address, Subnet mask, and Default gateway in the boxes provided, choose **OK**.

Set or change the IP settings and the gateway settings on the Advanced tab

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **IP**.
5. Select the **Advanced** tab.
6. In the **IP address** box on the right, type the IP address, and then choose **Add**.
7. Type the appropriate mask information in the **Subnet mask** box.
8. If necessary, update the **IP Connection Metric**.
9. Repeat steps 1–8 for any other IP addresses you wish to add.
10. In the **Gateway** and **Metric** boxes, type the IP address of both the default gateway and the metric, and then choose **Add**.
11. Repeat step 10 for each default gateway you want to add.
12. When you are finished modifying the configurations on this screen, choose **OK**.

> **Note**
> Changing the IP address may cause clients to lose their connection with the server. To reconnect clients must either use the new IP address or wait until the DNS server is updated.

Set DNS settings

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **DNS**.

5. To obtain DNS server information from a DHCP server, select the **Obtain configuration from DHCP server** button and choose **OK**.
6. To manually configure the DNS server settings, select the **Configure manually** button.
7. Type the appropriate IP address in the box next to the **Add** button, and then choose **Add**.
8. To add another DNS server, repeat step 7.
9. When you are finished adding DNS servers, choose **OK**.

Change the WINS settings of the server

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. Select the network connection you want to modify.
4. In the **Tasks** list, choose **WINS**.
5. To remove a WINS server, select the IP address of the WINS server you want to delete in the **WINS servers** list, and then choose **Remove**.
6. To add a WINS server, type the IP address of the WINS server in the **WINS server address** box, and then choose **Add**.
7. Repeat steps 5 and 6 for each WINS server IP address you want to remove or add.
8. Choose **OK**.

Add a VLAN

1. On the primary navigation bar, choose **Network**.
2. Choose **Interfaces**.
3. On the task table, choose **Create VLAN**.
4. Select the network adapter to add a new VLAN on it.
5. Choose an ID for the VLAN.
6. Click **OK**.

Delete an existing VLAN

1. On the **Network** page, choose **Global Settings**.
2. Choose **Interfaces**.
3. On the interfaces table, choose the VLAN you want to delete.
4. On the task table, choose **Remove VLAN**.

> **Note**
>
> Do not rename a VLAN which you attached to one of your existing LAN's, because otherwise, if you would like to delete it, your computer would recognize it as a physical LAN and you would not be able to delete this VLAN.

5. Click **OK**.

Administrator

The Windows server software comes with a set of default accounts. Only the administrator account has administrative privileges.

Change the administrator account for the server

1. Log on to the server as **Administrator**.
2. On the primary navigation bar, choose **Network**.
3. Choose Administrator.
4. Type the new name for the administrator account in the **User name** box.
5. Type the current administrator password in the **Current password** box.
6. Type the new administrator password in the **New password** box.
7. Retype the new administrator password in the **Confirm new password** box.
8. Choose **OK**.

Administration Web Site

This feature allows you to change the IP address(es) and port that can be used to access the administration Web site on the server.

Change the Administration Web Site Properties

1. On the primary navigation bar, choose **Network**.
2. Choose **Administration Web Site**.
3. On the Administration Site Properties page:
   υ Specify whether to use **All IP addresses** or **Just this IP address**.

- If you choose to use **Just this IP address**, use the list to select the IP address you want to use.
- If you are changing the port for non-encrypted access, type the new port number in the **Port for non-encrypted access** box.
- If changing the port for encrypted access, type the new port number in the **Port for encrypted (SSL) access** box.

4. Choose **OK**.

> **Note**
>
> By default, non-encrypted access to the administration Web site is dmmISAEEbled. To enable non-encrypted access to the administration Web site, use Internet Information Services Manager.

Users

From this page you can create, edit, and delete local users and groups on the server. You can also change the members of each group. If the server is a member of a domain, you will not want to create any users on the server itself. The primary purpose of this page is to add one or more domain members to the local group.

You may also want to use domain user and group accounts to control access to resources on the server. You may also want to use domain management tools to manage domain users and domain groups.

Local Users

A local user or group account is an account that exists on the server itself and grants users or groups access to its resources. The server can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft Windows NT 4 or Microsoft Active Directory domain. You can add local users, domain users, and domain groups to local groups.

Users and groups are important in Microsoft Windows security because you can assign *permissions* to limit the ability of users and groups to perform certain actions.

Any local or domain user who is a member of the local Administrators group on the server has administrative credentials for the server.

This section describes following actions:

- Adding a user account
- Removing a user account
- Setting a user password

υ Modifying user properties

Add a user account

1. From the primary navigation bar, choose **Users**.
2. Choose **Local Users**.
3. In the **Tasks** list, choose **New**.
4. Type the information for the new user account.
5. The **Home Directory** field specifies a new directory which will be created, and to which the user will have exclusive access permission. The directory name is the same as user name defined above, and will be located in the path specified.
6. If you want to dmmISAEEble the user account, select the **DmmISAEEble this user account** checkbox.
7. If you want to prevent the password from expiring, select the **Password never expires** checkbox.
8. Choose **OK**.

> **Note**
> It is important that the password should be at least 7 characters in length and should include capital letters, small letters and numbers. Otherwise you would get a reference that the password does not fulfill the requirements.

Removing a user account

1. On the primary navigation bar, choose **Users**.
2. Choose **Local Users**.
3. Select one or more user accounts to remove.
4. In the **Tasks** list, choose **Delete**.
5. Verify you want to delete the indicated user account(s), and then choose **OK**.

> **Note**
>
> Built-in users cannot be deleted.
>
> A deleted user cannot be recovered.

Setting a user password

1. From the primary navigation bar, choose **Users**.
2. Choose **Local Users**.
3. Select the user account for which you want to change the password.
4. In the **Tasks** List, choose **Set a Password**.
5. Type the new password, and then confirm it in the boxes provided. The new password must conform to any password policy in force on the server or domain.
6. Choose **OK**.

Modifying user properties

1. On the primary navigation bar, choose **Users**.
2. Choose **Local Users**.
3. Select one or more user accounts you want to modify.
4. In the **Tasks** list, choose **Properties**.
5. Make your changes to the user properties. If you choose multiple accounts, the only change you can make is to enable or dmmISAEEble all selected accounts.
6. Choose **OK**.

Local Groups

A local user or group account is an account that exists on the server itself and grants users or groups access to its resources. If the server is part of a domain, it can also be configured to grant access to domain users and groups. Domain users and groups are those that exist in a Microsoft Windows NT 4 or Microsoft Active Directory domain. You can add local users, domain users, and domain groups to local groups.

Here you can organize such a group and add or remove member e.g., following topics will be handled:

υ Adding a group account

- Removing a group account
- Modifying group properties

Add a group account

1. On the primary navigation bar, choose **Users**.
2. Choose **Local Groups**.
3. In the **Tasks** list, choose **New**.
4. On the **General** tab, type the name and description of the group you want to add.
5. On the **Members** tab:
   - To add members to the group, select a user or group to add from the **Add user or group** box, and then choose **Add**.
   - Only local users are displayed in the list. To enter a domain user account, type the domain and user name (<domain\user name>) in the box below.
6. To remove members from the group, select a member or group from the **Members** box, and then choose **Remove**.
7. Choose **OK**.

Remove a group account

1. From the primary navigation bar, choose **Users**.
2. Choose **Local Groups**.
3. Select one or more group accounts to remove.
4. In the **Tasks** list, choose **Delete**.
5. Verify that the group identified is the group account you want to delete, and then choose **OK**.

Set or modify a group name or description

1. On the primary navigation bar, choose **Users**.
2. Choose **Local Groups**.
3. Select the group account you want to modify.

4. In the **Tasks** list, Choose **Properties**.
5. On the **General** tab, type a new name and description.
6. Choose **OK**.

Set or modify group membership

1. On the primary navigation bar, choose **Users**.
2. Choose **Local Groups**.
3. Select the group account you want to modify.
4. In the **Task** list, choose **Properties**, and then select the **Members** tab.
5. To add a member:
   - In the **Add user or group** box, select a local user or group from the list, and then choose the **Add** button.
   - To add a domain user or group to this group, enter a name in the format *domain\user*, then choose **Add**. If you are logged on with an account that is not part of this domain, you will also need to enter a username and password that has credentials to add the group.
6. To remove a member, select a user name from the **Members** list, and then choose **Remove**.
7. Choose **OK**.

Maintenance

From the main **Maintenance** page, users can perform the following general server maintenance tasks:

- **Date and Time**: Set the date and time on the server.
- **Shutdown**: Shut down or restart the server.
- **Logs**: View, download, configure, and clear event logs.
- **Windows Product Activation**: Activate your Windows Server.
- **Addons**: Installation of additional Packages.
- **Backup**: Back up or restore the server's operating system.
- **Restore**: Restore the server operating system.
- **Alert E-Mail**: Set alert e-mail on the server.

Date/Time

Here you can set the date, time and time zone used by the server.

Set the date, time and time zone of the server

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Date/Time**.
3. Type the date and time in the indicated format.
4. Select the appropriate time zone from the list.
5. You can also automatically adjust the server for daylight saving changes, which is recommended. To do this, check the **Automatically adjust clock for daylight saving changes** check box.
6. Choose **OK**.

At this page you are also able to adjust a timeserver.

Configure a timeserver

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Date/Time**.
3. Type your chosen timeserver (e.g. time.windows.com), which you want to use for the time synchronmmISAEEtion, into the text field below the text “Time server attitudes”.
4. Select the checkbox beside the text field.
5. Choose **OK.**

Shutdown

Use this page to shut down, restart, or to schedule a shutdown or restart of the server. The page identifies any shutdown-related alerts and whether any shared files are open.

Shut down or restart the server

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Shutdown**.
3. Choose the task you want to perform.
4. Choose **OK** to confirm your decision.
5. If you have chosen to restart the server appliance, the **Restarting** page will display.

> **Note**
>
> The Restarting page checks periodically to determine whether the server is back online. If the Restarting page detects that the server is online, it automatically returns to the default page.

Schedule a shutdown or restart of the server appliance

1. From the primary navigation bar, choose **Maintenance**.
2. Choose **Shutdown**.
3. Choose **Scheduled Shutdown**.
4. Choose the scheduled shutdown settings you want.
5. Choose **OK**.

> **Note**
>
> To cancel a currently-scheduled event, select the No scheduled shutdown or restart button.

Logs

A log file is a file that stores messages, or event logs generated by an application, service, or Microsoft Windows. These messages are used to track the operations performed on the server.

You can use the **Logs** feature to view, clear, download, and configure the following types of event logs provided by the system:

υ Managing **Application Logs**: The application log contains events logged by applications and services running on the server. The events that are recorded are dependent upon the application.

υ Managing **Security Logs**: The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files.

- Managing **System Logs**: The system log contains events logged by the Microsoft Windows operating system components
- Managing **Web Administration Logs**: The Web administration log contains events logged by the Web server related to accessing the administration web site.
- Clearing Log Files
- Downloading Log Files
- Modifying Log Properties
- Viewing Log Details

Clear application, security or system logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select the type of log you want to clear.
4. Select **Clear Log**.
5. Choose **OK**.

Clear Web administration logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select **Web Administration Log**.
4. Select one or more log files to clear.
5. Choose **Clear Log**.
6. Choose **OK**.

Download application, security or system logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the type of log you wish to download.
4. Choose **Download Log….**
5. At the **Download System Log** page select the log format you want.
6. Click **Download Log…** to download the file.
7. Select Save this file to disk.

8. Choose **OK.**

Download Web administration logs

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Select the **Web Administration Logs**.
4. Select the log file to download.
5. Choose **Download Log**.
6. Select Save this file to disk.
7. Choose **OK**.

Modify the properties of a log file

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the **Application**, **System** or **Security log** you want to configure.
4. Choose **Log Properties**.
5. In the **Maximum log size** box, type the maximum size of the log, in kilobytes.
6. Select the button that best represents how you want to handle log entries once the maximum log size is reached.

View the details of a log file

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Logs**.
3. Choose the type of log you wish to view.
4. Select the log or log entry you want to view.
5. Choose Event Details or View Log.

> **Note**
>
> If you are viewing the application, security, or system log, you can navigate between log entries using the Up and Down buttons.
>
> The HTTP protocols log events in multiple log files. After selecting a log file, you can choose to view, clear, or download the contents of the log file.

Addons

Additional software can be installed to increase the security level or ease the manageability of your appliance.

Install an additional software

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Addons**.
3. Choose **Next**.
4. Select the desired software you want to install and choose **Next**.
5. After selecting the favoured software, the setup process will be started in a remote desktop session. Please follow the instructions of the setup program.
6. After the installation has completed, choose **Next**.
7. Choose **Finish**.

> **Note**
>
> It is recommended to install the program to its default location to ensure that it is included in the backups.
>
> Extra licenses need to be purchased for additional software packages. Most packages contain a 3 days trial license, to be able to use the software after this period; licenses which satisfy your LAN environment have to be purchased. Please contact your reseller for more information.

Backup

Allows you to backup the mISAE Server appliance. In every backup process the following files and settings are backed up:

system state (contains registry, boot files and COM-settings)	
c:\	(the whole system drive)
d:\logs	(mISAE server log files)
d:\reports	(reports from mISAE)

There are 2 possibilities to choose from:

- **Full backup**: Always backs up all files, depending on your configuration and the amount of log files, this backup file will be greater than 2.5GB in size.

- **Differential backup**: Only backs up files which archive-attribute has been reset, that means: all files that have changed since the last backup. Note that this backup type does note set the archive flag again, you will notice that every differential backup file is larger than the one before. However, there is a large advantage when it comes to dmmISAEEster recovery: you will only need to restore the last full backup file and one (the latest) differential backup file. Depending on the amount of log files and reports, the Backup file will be at least 700MB large. The reason for this is that a differential backup also contains a full system state, which is by default about 650MB.

> **Important**
>
> After the appliance is initially configured it is highly recommended to make a full backup. All backup files should be moved to a secure location after the backup has finished. Note that it is not possible to restore backups to a different appliance type, i.e. backups from an mISAE110 appliance cannot be restored to a mISAE760 appliance!

It is also possible to choose the storage where the backup should be written. You can choose between a **Local Store**, **Windows Share** and **Linux Share**.

- Local

  Stores the Backup Local at **D:\Backups**.

- Windows Share

  Enter the UNC path to the share where you want to store the backup files in the "Server" field. Note that you can enter domain users in the form "DOMAIN\user" in the "User" field, an optional subdirectory can be provided in the "Directory" field.

υ Linux Share

If you want to use an SSH connection to a linux machine to backup your Appliance, please provide a valid DNS name or IP address in the "Server field", as well as the TCP port number where the SSH daemon is listening. In the "Directory"filed provide the absolute path where you want to store the file. The first time when you use the server, a pop-up opens and you will have to commit the servers SSH-key.

You can also export and import the mISAE configuration, which contains rule base, network objects and VPN configurations.

Backup the system immediately

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Backup**.
3. Choose **Back up the system immediately**.
4. Choose **OK**.
5. After a message has appeared on the screen, the system will start the backup in background 2 minutes later.

Add a scheduled backup task

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Backup**.
3. Choose **Add a scheduled backup task**.
4. Configure the time you want to start a backup
5. Choose **OK**.

Remove a scheduled backup task

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Backup**.
3. Choose the scheduled backup task you want to remove.
4. Choose **OK**.

Export current configuration

1. On the primary navigation bar, choose **Maintenance**.

2. Choose **Backup**.
3. Choose **Export current configuration**.
4. Choose **OK**.
5. Follow the instructions on the screen and save the file to a favoured path.

Import uploaded configuration

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Backup**.
3. Choose **Upload a file**
4. Choose **Browse**, select an mISAE Server configuration file, click **Upload** and wait until a message indicates that the file was uploaded successfully.
5. Close the Upload window.
6. Choose **Import uploaded configuration**.
7. Choose **OK**.

View backup log

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Backup**.
3. Choose View Backup Log and the last 50 lines of the log-file are shown.

> **Important**
>
> The import process will start by a scheduled task 2 minutes after the OK button has been pressed. During the import process the server will close all open connections, including the connection to the web-management interface.

Restore

In case of misconfiguration or dmmISAEEster recovery you may revert the nAppliance mISAE Server to a previous state using the restore function.

> **Important**
>
> If the appliance is a member server of an Active Directory or Windows NT4 domain, it may be necessary to re-add the computer to the domain after the restore process has finished. If you perform a dmmISAEEster recovery, you have to copy your backup files to the new appliance first. Your may use a remote desktop connection to fetch the files from your secure location.

To generally start the restore wizard perform the actions below.

Start the Backup or Restore Wizard

1. On the primary navigation bar, choose **Maintenance**.
2. Choose **Restore**.
3. Please follow the instructions of the Restore wizard in the remote session to revert the appliance to a previous state.

The following instructions will guide you through the whole recovery process, assuming that the Appliance is freshly installed (either new hardware or a fresh install from the Appliance Installation DVD) and you have copied all necessary backup files to the Folder d:\Backups.

Recovery Process

1. Restore the full backup using the **Backup and Restore Wizard**. It is recommended, to select **always overwrite files** from the advanced settings when performing this restore.
2. Reboot the machine and restore the latest differential backup if necessary.
3. Re-add the machine to your NT 4 Domain or Active Directory domain if necessary.

Alert E-Mail

Your server can be configured to generate an automatic e-mail notification when an alert is raised. You can choose to be notified when any type of alert is raised or only for specific alert types, such as informational, warning, or critical alerts.

This feature uses the SMTP service to send e-mail. In a normal Internet environment, you do not need to configure an SMTP gateway. However, to send e-mail to Microsoft Exchange Server or Lotus Notes, you need to provide the name of the specific SMTP gateway. You must put the SMTP gateway server name, or IP address, in the SMTP server field in the Web-Management. Contact your Microsoft Exchange administrator for the server name of the SMTP gateway.

Enable the alert e-mail feature

1. From the primary navigation bar, choose **Maintenance**.
2. Choose **Alert E-Mail**.
3. Select the **Enable alert e-mail** button, and then select the check boxes for the circumstances under which you want alert e-mail to be sent.
4. In the **To** box, type the system administrator's e-mail address.
5. You may have alert e-mail sent to multiple addresses, simply type the addresses into the **To** box, separated by a comma.
6. In the **From** box, type the user name of the e-mail account from which the mail will be sent.
7. In the **With** box, type the SMTP gateway name or IP address of the SMTP server.
8. To test the settings, choose **Test**.
   - After clicking the **Test** button, test e-mail is sent. If the SMTP service is not installed on your computer, or there is no network cable, you will receive the error message "Test e-mail cannot be sent out."
   - If you do not receive the test e-mail at all, even though the message "Test e-mail has been sent out. Please check administrator's mailbox" has been displayed in the Web UI, the error has most likely been caused by the SMTP server. To clear this error, reset the SMTP server name.
9. Choose **OK**.

DmmISAEEble the alert e-mail feature

1. From the primary navigation bar, choose **Maintenance**.
2. Choose **Alert E-Mail**.
3. Select the **DmmISAEEble sending alert e-mail** button.

Administration

From the main **Administration** page, users can perform the following general server maintenance tasks:

- **File upload:** upload and, if you want, execute a file in you folder
- **mISAE Management Console**: Start the mISAE Management Console to configure your system.
- **Resources**: View actual server resources.
- **Sniffer**: Ability to sniff the network traffic.
- **Remote Desktop**: Manage all aspects of the server by connecting to it using Remote Desktop.
- **Harden System Policy:** Restrict access to web UI and remote desktop

File Upload

Upload a file

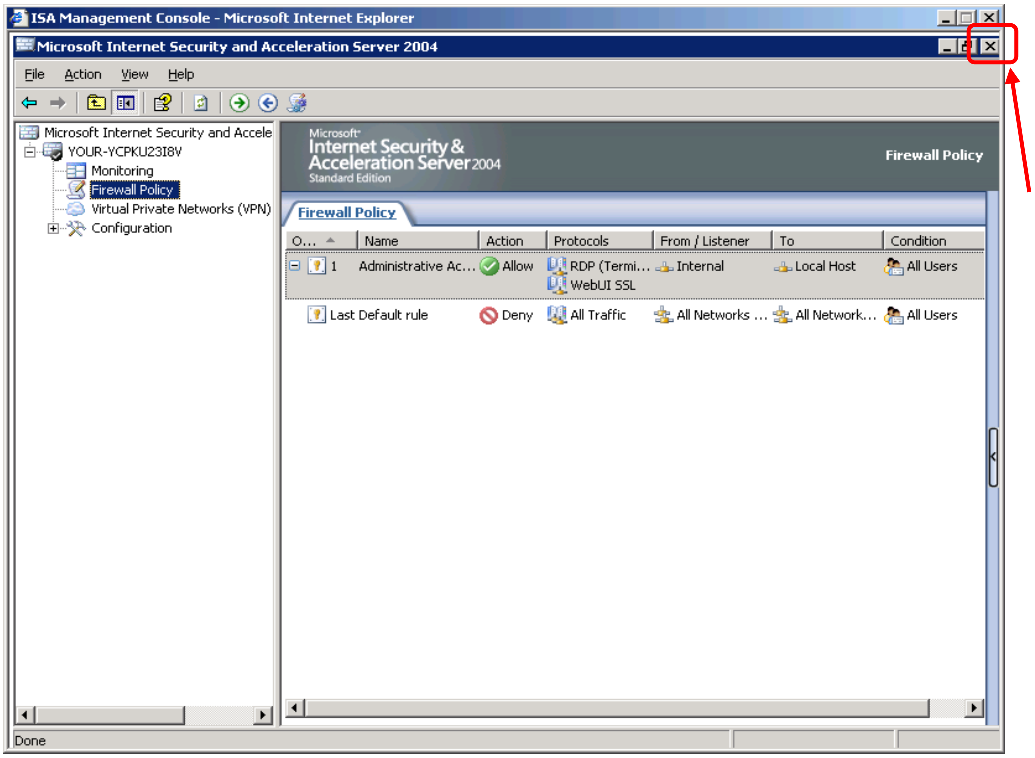
1. On the primary navigation bar, choose **Administration**.
2. Choose **File upload**.
3. Fill in the directory where you want to store your uploaded file (e.g. D:\Uploads)
4. **Browse** for the file which you want to upload.
5. If you want to execute the file after uploading, activate the checkbox "Execute after upload".
6. Click File upload.

mISAE Management Console

Start the mISAE Management Console to configure your system.

Start the mISAE Management Console

1. On the primary navigation bar, choose **Administration**.
2. Choose **mISAE Management Console**.


ISA Management Console - Microsoft Internet Explorer
Microsoft Internet Security and Acceleration Server 2004
File
Action
View
Help
Microsoft Internet Security and Accele
YOUR-YCPKU23I8V
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Microsoft
Internet Security & Acceleration Server 2004
Standard Edition
Firewall Policy
Firewall Policy
Done

O...	Name	Action	Protocols	From / Listener	To	Condition
1	Administrative Ac...	Allow	RDP (Termi... WebUI SSL	Internal	Local Host	All Users
	Last Default rule	Deny	All Traffic	All Networks ...	All Network...	All Users

Important

Close the application inside the mISAE Management Console as shown in the picture above to shut down the session correctly.

Resources

Views actual system parameters like:

υ Memory size

υ Memory usage

υ Processor usage

υ Running time

The CPU usage is averaged over 1 minute to get a more accurate value.

Show resources

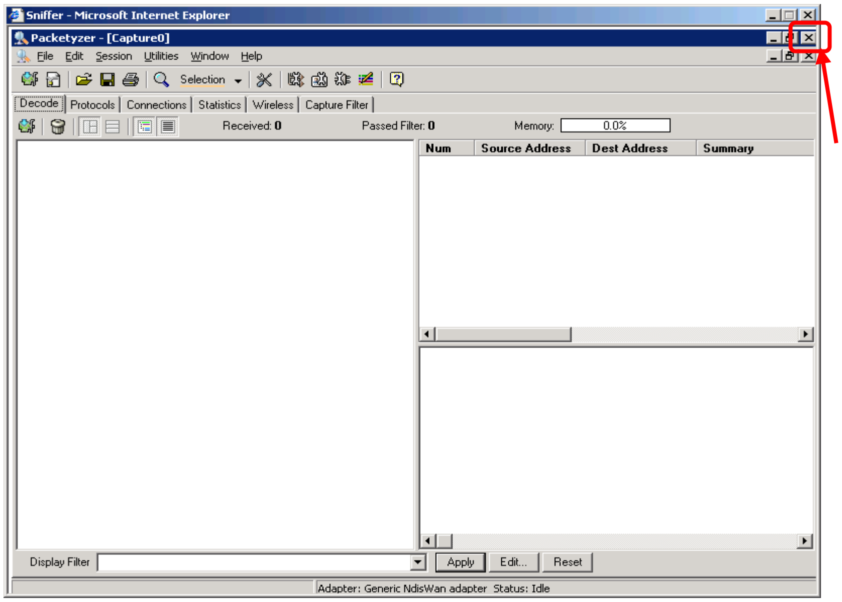
1. On the primary navigation bar, choose **Administration**.
2. Choose **Resources**.

Sniffer

This opens the network packet analyser which is installed on the mISAE server appliance. This program is useful to debug network issues and should only be used by network professionals.

Start the Sniffer Application

1. On the primary navigation bar, choose **Administration**.
2. Choose **Sniffer**.



Received: 0 Passed Filter: 0 Memory: 0.0%

Adapter: Generic NdisWan adapter Status: Idle

Important

Close the application inside the Sniffer Console as shown in the picture above to shut down the session correctly.

Remote Desktop

Remote Desktop provides the ability for you to log onto and remotely administer your server, giving you a method of managing it from any client. Installed for remote administration, Remote Desktop allows only two concurrent sessions. Leaving a session running takes up one license and can affect other users. If two sessions are running, new users will be denied access.

Access Remote Desktop

1. On the primary navigation bar, choose **Administration**.
2. Choose **Remote Desktop**.
3. Log on.

> **Important**
>
> Log off Remote Desktop when you have finished your work to shut down the session correctly.

Harden System Policy

This wizard helps you to limit the access to the Web UI and via remote desktop to certain computers or networks. Per default, all hosts in the internal network can access the remote desktop and Web UI.

Add Hostinformation

1. On the primary navigation bar, choose **Administration**.
2. Choose **Harden System Policy**.
3. Click **Next**.
4. Choose whether if you want to **Add a single host**, to **Add address range** or to **Add subnet**.
5. If you have chosen **Add a single host**, then you have to fill in the IP-address of the host. Fill in the start address and the end address if you haven chosen **Add address range**. Otherwise if you want to **Add a subnet**, enter the network address and the Netmask.
6. Click **Next**.
7. Operation will be completed, click **Finish**.

Help

You can locate information in **Help** by using any of the following procedures:

υ To browse through topics by category

  υ To browse through the topics, click the topic title in the **Table of Contents** list.

υ To invoke context-sensitive Help

  υ From the page for which you want assistance, click the **?** icon at the right end of the primary navigation bar.