



Setup Guide

April 2007 Edition
© 2007 eIQnetworks

Clavister AB
Torggatan 10,
SE-891 28 ÖRNSKÖLDSVIK,
SWEDEN
www.clavister.com

Copyright and Trademarks

Clavister InSight End User License Agreement

Important - BEFORE OPENING OR INSTALLING THE SOFTWARE PACKAGE(S), CAREFULLY READ THE TERMS AND CONDITIONS OF THE FOLLOWING Clavister Insight LICENSE AGREEMENT. OPENING OR INSTALLING THE SOFTWARE PACKAGE(S) INDICATES YOUR ACCEPTANCE OF THE TERMS AND CONDITIONS OF THE AGREEMENT. THIS IS A LEGAL AGREEMENT BETWEEN YOU, AS LICENSEE, AND EIQNETWORKS, INC. ("EIQNETWORKS") AS OWNER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THE AGREEMENT, RETURN THE UNOPENED AND UNINSTALLED SOFTWARE PRODUCTS AND THE ACCOMPANYING ITEMS TO THE PLACE YOU OBTAINED THEM. PROMPTLY RETURN THE UNOPENED AND OR UNINSTALLED SOFTWARE PACKAGE(S) AND ALL OTHER MATERIALS WITH PROOF OF PAYMENT TO YOUR PLACE OF PURCHASE, AND YOUR LICENSE FEE WILL BE REFUNDED.

SOFTWARE LICENSE

1) GRANT OF LICENSE. This License Agreement ("License") gives you a nonexclusive, nontransferable license to install one copy of the software per contained in the sealed software package or electronic package and may include electronic documentation or paper documentation, (the "SOFTWARE") on one (1) workstation, or server ("HOST"). Base license allows the user to collect, analyze and report on log / event / activity data from ten(10) licensed devices. An additional license is needed for each additional device beyond the base license to collect, analyze and report on log / event / activity data from licensed network device or licensed host. A Base License is required before additional licenses can be purchased. A device is defined as any supported network switch, router, firewall, IDS / IPS / Proxy / Anti Virus Server / any network device or appliance. A host is defined as any Windows or Linux/Solaris or Unix node.

The SOFTWARE is in "use" on a computer when it is loaded into the temporary memory (RAM) or installed into the permanent memory (HARD DISK /CD ROM, or other storage device) of that computer. A separate license is required for each physical device on which the licensed software will be used to collect, analyze, monitor and report.

Clavister Insight is licensed based on Device IP address, Device ID, and or Device Name. Customers who wish to purchase Clavister Insight license are required to provide the Systems Identifier (System ID of the system on which Clavister Insight will be installed) so that eIQnetworks can generate the appropriate license key. Customers who subsequently change their System are required to submit a written letter (on your company letterhead) requesting eIQnetworks to issue a new license key. eIQnetworks at its sole discretion will determine if it will issue a new license key.

2) UPGRADES. If the SOFTWARE is a valid upgrade you may use or transfer the SOFTWARE only in conjunction with the prior version(s) of the SOFTWARE.

3) COPYRIGHT. The SOFTWARE (including any images, photographs and text incorporated into the SOFTWARE) is owned by eIQnetworks, and is protected by United States, Canadian and international copyright laws and international treaty provisions. No title to the Software shall be transferred to you. Therefore you must treat the SOFTWARE like any other copyrighted material and not reproduce it except that you either (a) make one copy of the SOFTWARE solely for backup or archival purposes, or (b) transfer the SOFTWARE to a single hard disk provided you keep the original solely for backup or archival purposes, and the copy contains

all of eIQnetworks' proprietary notices. You may not copy the printed materials accompanying the SOFTWARE.

4) TITLE. Clavister Insight and the information it contains, any updates and all copies are eIQnetworks property and title to such Software Program remains with eIQnetworks.

5) Other Restrictions. You may not reverse engineer, decompile, disassemble, or translate the SOFTWARE, except to the extent such foregoing restriction is expressly prohibited by applicable law. You may not permit other individuals to use the Software Program except pursuant to the terms and conditions herein, reverse assemble, decompile, modify or create derivative works based on the Software Program, copy the Software Program except as provided above, rent, lease, assign or otherwise transfer any rights with respect to the Software Program or remove any proprietary notices on such Software Program. It is illegal to copy or distribute Clavister Insight software or its accompanying documentation, including programs, applications, data, codes, and manuals, or to run a copyrighted software program on two or more computers simultaneously unless this is specifically allowed by the license agreement, without permission or a license from eIQnetworks.

6) Dual-media Software. You may receive the SOFTWARE in more than one medium. Regardless of the type or size of medium you receive, you may use only the medium appropriate for your single-user computer. You may not use the other medium on another computer or loan, rent, lease, or transfer the disks to another user except as part of the permanent transfer (as provided above) of all SOFTWARE and printed materials, nor print copies of any user documentation provided in "online" or electronic form.

7) EXPORT CONTROLS. The Software Program and/or any underlying information or technology may not be exported or re-exported into or to a national or resident of Cuba, Libya, North Korea, Iran, Syria or any other country to which the United States has effected an embargo, or to anyone on the U.S. list of Specially Designated Nationals.

8) TERMINATION. eIQnetworks may terminate the license granted you hereunder at any time if you fail to comply with any terms and conditions of this Agreement. Upon termination of the license, you must destroy or dispose of the Software, any copies of the Software and manual and other materials provided with the Software.

9) THIRDPARTY SOFTWARE. The Software Program uses certain third-party libraries/software. The license agreements of the same are provided with *THIRDPARTYLICENSEREADME.txt* under application install path.

LIMITED WARRANTY. eIQnetworks warrants that the SOFTWARE will perform substantially in accordance with the accompanying written materials for a period of thirty (30) days from the date of receipt. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. This warranty may not be assigned.

CUSTOMER REMEDIES. eIQnetworks and its suppliers' entire liability and your exclusive remedy shall be, at eIQnetworks option, either (a) return of the price paid, or (b) repair or replacement of the SOFTWARE that does not meet eIQnetworks Limited Warranty and which is returned to eIQnetworks with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period or twenty-one (21) days, whichever is longer.

NO OTHER WARRANTIES. To the maximum extent permitted by applicable law, eIQnetworks and its suppliers disclaim all other warranties, either or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with regard to the SOFTWARE and the accompanying printed materials. This limited warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES. To the maximum extent permitted by applicable laws, in no event shall eIQnetworks or its suppliers be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of information, or other pecuniary loss) arising out of the use of or inability to use Clavister Insight, even if eIQnetworks has been advised of the possibility of such damages. Because some states/jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

Should you have questions concerning this Agreement, or if you desire to contact eIQnetworks please visit our Web site: www.eIQnetworks.com

I have read and agree to the terms and conditions above.

Network Security Analyzer[™], eIQnetworks[™], The Power of Security Intelligence, Security Analysis Center[™] and Instant Reports[™] are trademarks and or Service marks of eIQnetworks, Inc.

Contents

ICONS IN THE DOCUMENTATION	7
INSTALLATION OVERVIEW	8
GETTING STARTED	8
PRE-INSTALLATION CHECKLIST	9
<i>Minimum System Requirements</i>	9
<i>Recommended Requirements</i>	9
<i>Preparing the Installation</i>	10
INSTALLATION	11
LICENSE REQUIREMENTS	12
<i>Uninstall Program</i>	12
<i>Support</i>	12
<i>Sales</i>	12
<i>Technical Support</i>	12
<i>Upgrades and New Products</i>	12
THE SETUP PROCEDURE.....	13
<i>Welcome</i>	14
<i>Product Upgrade</i>	15
<i>The End User License Agreement</i>	15
<i>Choosing Installation Type</i>	17
<i>Enter Product Registration Details</i>	19
<i>Destination Directory</i>	20
<i>Install Clavister InSight as Website on IIS</i>	20
<i>Installation as a Virtual Directory on IIS</i>	22
<i>Install Clavister InSight on Apache Server</i>	23
<i>Summary</i>	24
<i>The Finish Screen</i>	25
CHOOSING INSTALLATION TYPE	26
CHOOSING AN INSTALLATION OPTION	27
<i>Scenario for a Standalone Installation</i>	27
<i>Scenario for Distributed Installation</i>	28
INSTALLING SYSLOG SERVER	30
CIS ARCHITECTURE	31
SYSTEM REQUIREMENTS	32
THE WELCOME SCREEN	33

CLAVISTER INSIGHT SERVER LOCATION-----34

PRE-INSTALL CHECKER -----35

INSTALLATION PATH -----36

THE SUMMARY SCREEN -----37

UNINSTALLING SYSLOG SERVER -----38

THE CONFIGURATION SCREEN-----38

The General Screen -----38

Syslog Ports Screen -----41

LEA Firewalls -----43

The Anti-Virus Screen-----46

The ISA Device -----48

The ISS Device-----50

RDEP -----52

The Advanced Tab -----54

APPENDIX A-----56

 STEPS SPECIFIC TO THE WINDOWS 2003 PLATFORM -----56

Adding ISAPI Filter -----57

Enabling SSL Port on IIS -----59

 CONFIGURING IIS 6.0 FOR CLAVISTER INSIGHT-----66

 CONFIGURING WINDOWS 2003 TO ALLOW CGI EXTENSIONS -----71

 CONFIGURING MIME TYPE EXTENSION FOR IIS ON WINDOWS 2003 -----76

 ADDING IIS TO USE THE IUSR ACCOUNT -----79

 CONFIGURING THE IUSR ACCOUNT TO HAVE THE NECESSARY PERMISSIONS-----82

 CONFIGURING IIS TO REMOVE APPLICATION MAPPING FOR .EXT FILES -----82

 ENABLE ACTIVE X CONTROLS AND PLUG-INS -----84

 CONFIGURING IIS FOR ACCESSING THE APPLICATION USING REMOTE DESKTOP -----86

APPENDIX B -----87

 ADMINISTERING SERVICES RUNNING ON SERVICES WINDOW -----87

 PROPERTIES WINDOW -----87

 GRANTING PRIVILEGE-----89

 VERIFYING GRANTED PRIVILEGES -----90

Icons in the Documentation

There are three icons used to call your attention to additional helpful information.



The "Important!" icon points out important information regarding data and system security.



The "Note" has information that should be considered.



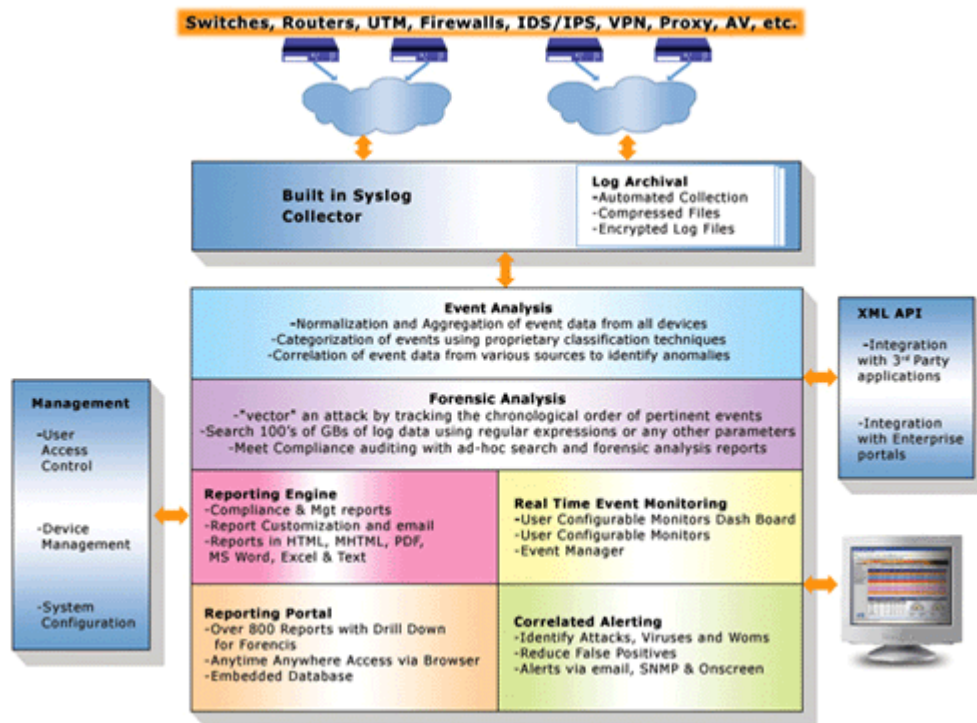
The "Tip" has information that may aid in performing a procedure or in solving a problem.

Installation Overview

Getting Started

This chapter provides you with general information on the pre-installation hardware and software requirements that you will need to install and run Clavister InSight (also referred to as CIS). The Clavister InSight installer will guide you through the installation process as it performs tasks such as gathering user input, checking for required disk space and components for installation, information on environment variables, and the launching of configuration assistants to configure the components.

Clavister InSight Network Architecture



Pre-installation Checklist

This section outlines all the pre-installation tasks that must be completed before installing Clavister InSight.

Minimum System Requirements

- ❖ **Processor** - Pentium 4 – 2.4 GHz
- ❖ **Disk Space** – 20 GB
- ❖ **RAM** – 2 GB
- ❖ **Operating System** - Windows® NT/2000/XP/2003
- ❖ IIS, Netscape or Apache
- ❖ Java 2 Runtime Environment JRE
- ❖ Internet Explorer 6.0 or any DOM compatible web browser with Shockwave Flash plug-in.

Recommended Requirements

- ❖ **Processor** - Pentium 4 – 2.8 GHz or higher
- ❖ **Disk Space** – 100GB or higher
- ❖ **RAM** - 2 GB or higher
- ❖ **Operating System** - Windows Server 2000 or 2003
- ❖ Fast IO
- ❖ Java 2 Runtime Environment JRE v1.5 and above
- ❖ Internet Explorer 6.0 with Shockwave Flash plug-in
- ❖ IIS (for increased security)

Additional Requirements

- ❖ MS-Office must be installed before you try to generate reports in WORD or EXCEL formats.
- ❖ Adobe Acrobat Reader to view reports in PDF format.

Preparing the Installation

You can find important installation tips in the file: readme.txt. We strongly recommend that you read this file because it may contain information that became available after this guide was printed.



The installation process can be stopped at any time by clicking the **Cancel** button. If you stop installation, you will not be able to run Clavister InSight or the syslog server. You can have the installation directory and all files contained therein automatically removed after you cancel the installation.

Installation

Insert the included CD-ROM into the CD-ROM drive of the Windows PC. If the installation software does not start automatically, select Run from the Start Menu and enter D:\launch.exe (where D: is the letter of your CD-ROM drive).

You will be presented with a list of options. Select the option to install the Clavister InSight server software.

If you are installing the program from the downloaded file from the Internet, run the executable setup file. This launches the Setup program and guides you through the setup process. In setup, select the directory in which you want to install Clavister InSight. The setup program installs the required system components and registers them with the operating system. Alternatively, you can use the Windows Run screen to launch the setup program. Follow the on-screen instructions to install Clavister InSight. The sections below explain the installation procedure in detail.



If you have already installed a previous version of Clavister InSight, you must first uninstall it.



To install Clavister InSight, you must be a user with administrator rights.

License Requirements

You can download a trial copy of Clavister InSight from <http://www.clavister.com>. Clavister InSight automatically creates a 21-day trial license for 10 devices. The trial-license and any permanent license are machine specific and are hence not portable. You must provide your machine's MAC-address and the number of devices you want to report on for us to generate a permanent-license.

Uninstall Program

To remove Clavister InSight from your system, uninstall it using the **Add/Remove** utility from the Control Panel. Locate *Clavister InSight v4.6* among the programs listed, select it, and click **Add/Remove**. This will remove the program and the services it has installed on your system.

Support

This section provides information about sales, technical support, upgrades and new products.

Sales

For sales support, please contact us by e-mail at sales@Clavister.com.

Technical Support

We provide technical support for all trials and with the purchase of eCare, we provide continuous support for product purchases. Please contact us at support@clavister.com.

Upgrades and New Products

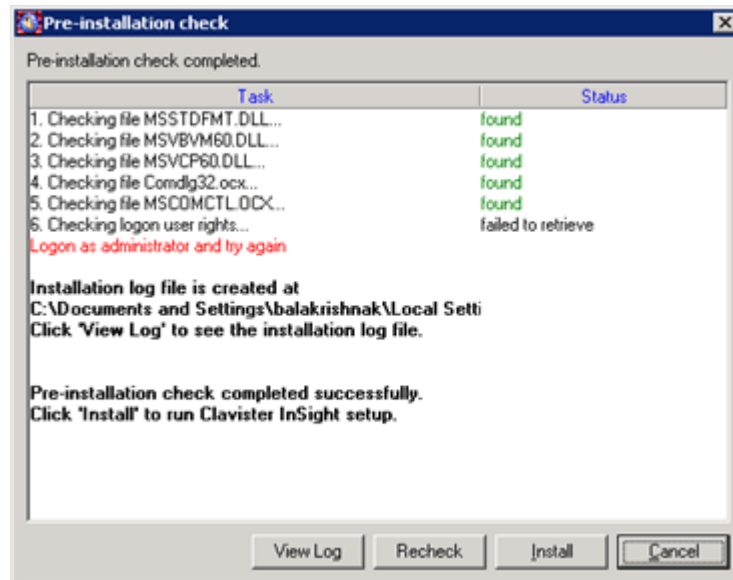
Please check our website from time to time for information about upgrades, service packs and utilities that you can download at <http://www.Clavister.com/>.

If you register Clavister InSight, you will receive regular e-mails about product upgrades and other related product information. Upgrades and new releases are included in our eCare support contracts at no additional cost.

The Setup Procedure

The installer is a wizard that guides you through the installation process and prompts you for necessary information.

Pre-Installation Check

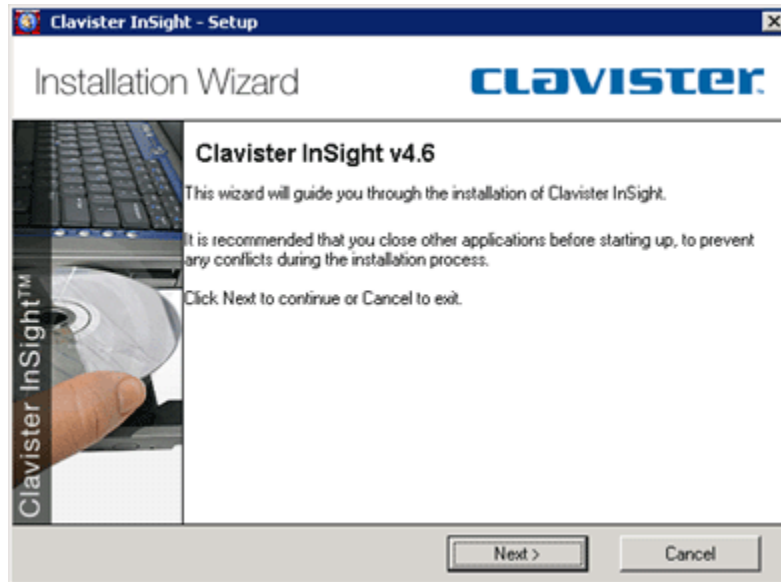


- ❖ The installation starts with the pre-installation checker verifying if the necessary DLLs and ActiveX components exist. To examine the contents of the checker log file, click **View Log**. If the pre-installation check completes successfully, click **Install** to run the Clavister InSight setup. If a previous version of Clavister InSight exists on your system, you must uninstall it before installing Clavister InSight v4.6.

Welcome

When you start the setup program, the Welcome screen appears. To proceed through the installation, follow the steps below

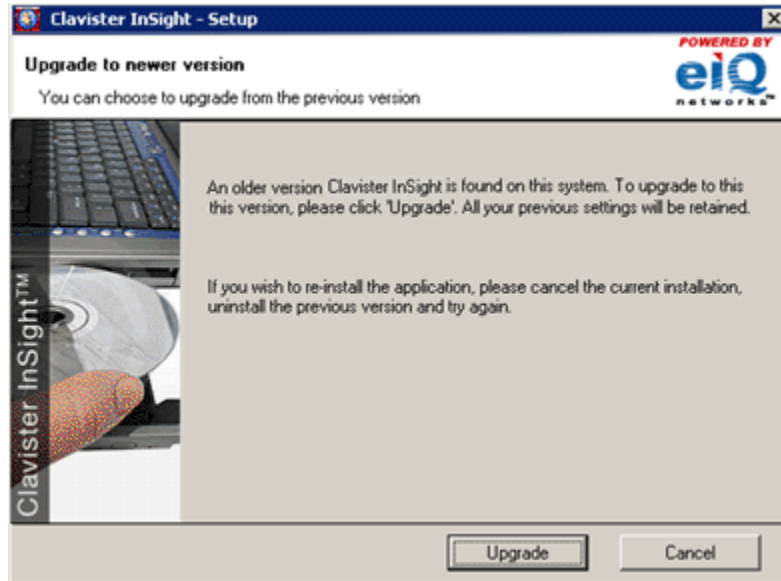
Installation Wizard



- ❖ Click **Next**.

Product Upgrade

Product Upgrade Screen



This screen appears only if you are upgrading from over a minor release of Clavister InSight v4.6.

- ❖ To upgrade, click **Upgrade**.
- ❖ If you do not want to upgrade, click **Cancel** to exit setup.

The End User License Agreement

The **End User License Agreement** details the terms and conditions under which you can use the software. Read the agreement carefully and follow the steps described below:

End User License Agreement



- ❖ If you agree to the terms and conditions in the agreement, select the **I have read and agree to the License Agreement** check box and click **Next**.
- ❖ If you do not agree to the terms and conditions, click **Cancel** to cancel the installation and exit the setup program.

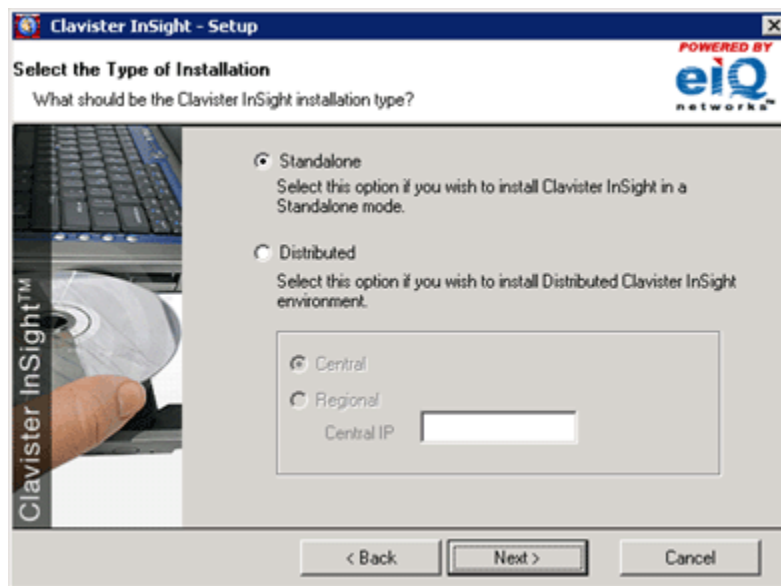
Choosing Installation Type

Before you install CIS 4.6, you will need to decide on the type of deployment. To do this, you will have to understand the topology of your network and identify which of the installation types best suits you.

You can install CIS in any of the following two modes:

- ❖ Standalone
- ❖ Distributed
 - ❖ Regional
 - ❖ Central

Standalone Deployment



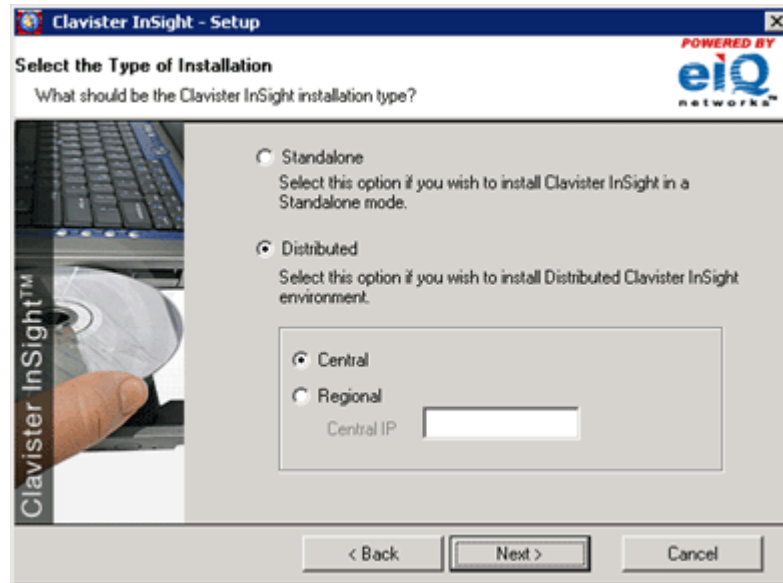
Standalone Deployment

This type of deployment is best suited to a relatively small network environment that is composed of several internal networks with Internet access. Publicly accessible server resources are placed in an isolated network and are protected by a firewall. A standalone CIS server can be installed and used to monitor and report on events on all the devices in such a network.

Distributed Deployment

This type of deployment is best suited to a large network, where the devices are geographically dispersed in various intranets, which in turn are connected to the Internet. You can install Clavister InSight in the distributed mode where several regional servers collect syslog data and provide a picture of the local network environment. The syslog data is also forwarded by the regionals to a centralized repository on the Central server where data is stored. You can then generate reports and get an overall picture of the entire network.

Distributed Deployment



To install CIS in a standalone mode, follow the steps described below:

- ❖ Select the **Standalone** button and click **Next**.

To install CIS in a distributed mode, follow the steps described below:

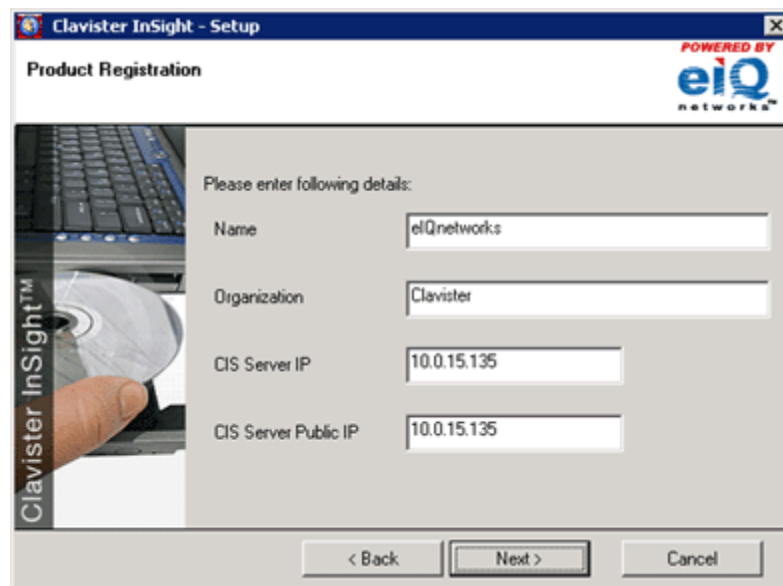
- ❖ Select the **Distributed** button.
- ❖ To install a Central server, select the **Central** button and click **Next**.
- ❖ To install a regional server, select the **Regional** button and enter the IP address of the machine where the Central server is installed. Then click **Next**.

Enter Product Registration Details

To register Clavister InSight, enter the following mandatory details:

1. Enter the **Name** of the User/Machine to register CIS.
2. Enter the name of the **Organization** on whose name CIS will be registered.
3. Enter the **CIS Server IP**, that is, the IP address of the machine where CIS is installed.
4. Enter the **CIS Server Public IP**, that is, the Public IP address of the system where CIS is installed.

Product Registration screen



Clavister InSight - Setup

Product Registration

POWERED BY eiQ networks

Please enter following details:

Name: eiQnetworks

Organization: Clavister

CIS Server IP: 10.0.15.135

CIS Server Public IP: 10.0.15.135

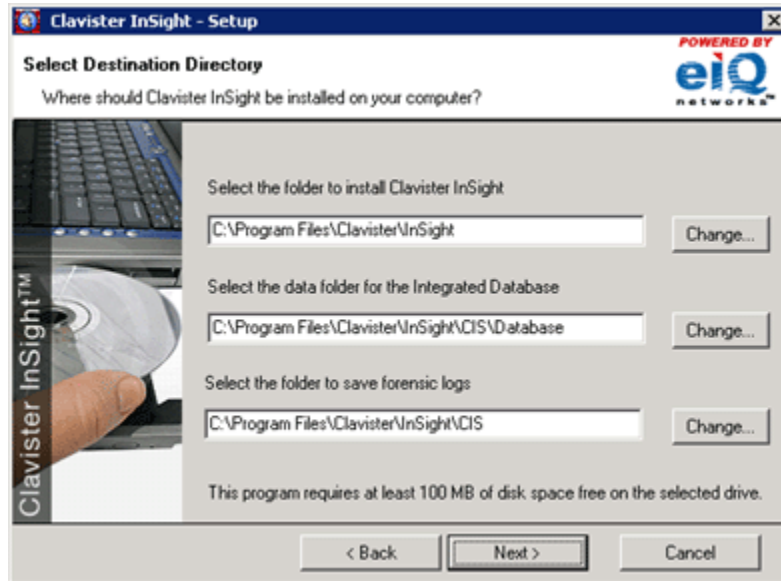
< Back Next > Cancel

CIS server is identified by the DB agents and syslog server through its IP address. In a network, if CIS is running on a system, which has multiple NIC cards, there is a possibility that its IP address could differ. In order to resolve this enter the **CIS Server IP** and **CIS Server Public IP** the system on which CIS is installed.

Destination Directory

This screen lets you specify the directory in which you want to install Clavister InSight. The program requires a minimum of 50 MB of disk space, so you must choose a drive that has at least 100 MB on it. By default, Clavister InSight installs in your Program Files directory.

Destination Directory



Follow the steps given below to select the destination directory:

- ❖ To install Clavister InSight in the default location C:\Program Files\Clavister\InSight click Next.
- ❖ Specify the location to install the built-in database.
- ❖ Specify a location to save the forensic log files. By default, the logs are stored in C:\Program Files\Clavister\ InSight\CIS.



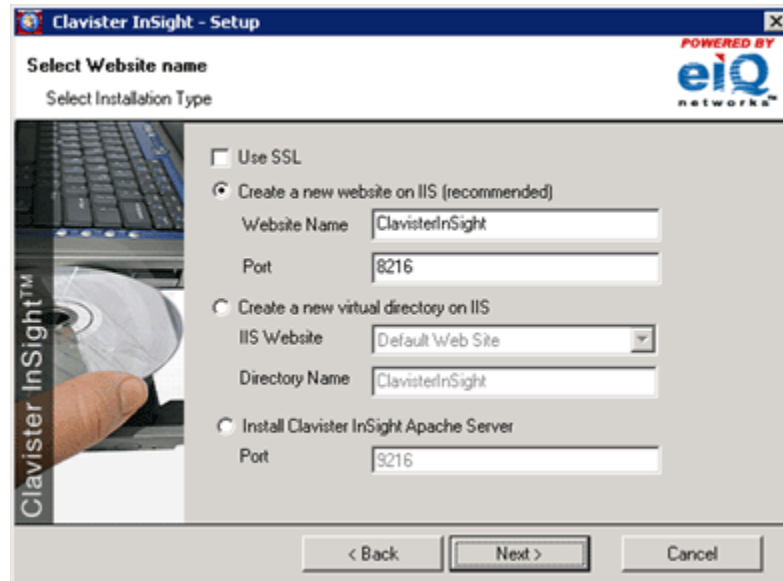
To install Clavister InSight, you must be a user with administrator rights.

Install Clavister InSight as Website on IIS

This screen allows you to specify the installation location. You can install Clavister InSight either as a website or a virtual directory on IIS, or on the

CIS Apache server. The following section explains the conditions under which each of these options is valid.

Website on IIS



- ❖ **Create a new Website on IIS:** This is the default option. Clavister InSight installs as a website on IIS and runs on port 8216. If your machine does not have IIS installed, then the **Install Clavister InSight Apache Server** option is the default option.
- ❖ By default, Clavister InSight installs as a website with the name **Clavister InSight** and runs on the port 8216. If you want to change the website name and/or the port, just type in a new name and/or port.
- ❖ Click **Next**.

If you are installing Clavister InSight on a Windows 2003 machine, make sure that all unknown CGI extensions are allowed. Click [here](#) for instructions on how to do this.

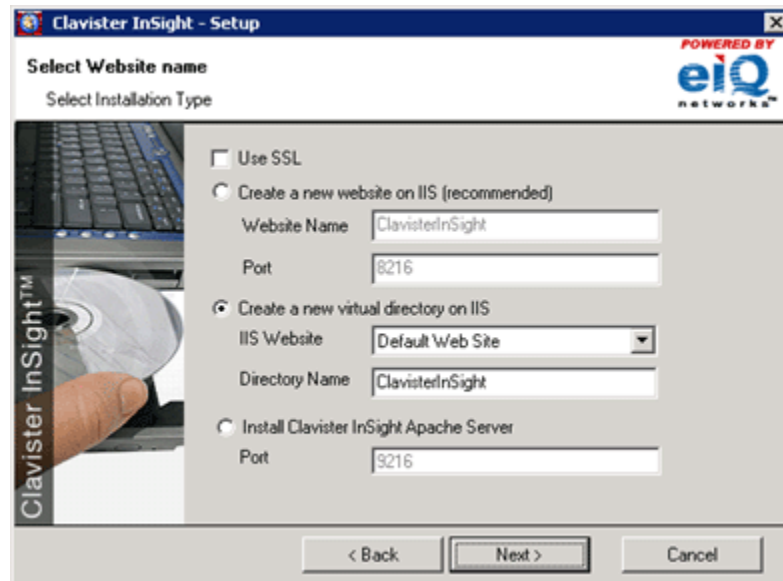


Windows XP allows you to run only on one website at a time. We recommend that you choose virtual directory installation if you have a website already running.

Installation as a Virtual Directory on IIS

Select this option if you have IIS on your machine but do not want to install Clavister InSight as a website. Setup creates a directory with the name Clavister InSight under the default website and the program runs as a virtual directory.

Virtual Directory on IIS



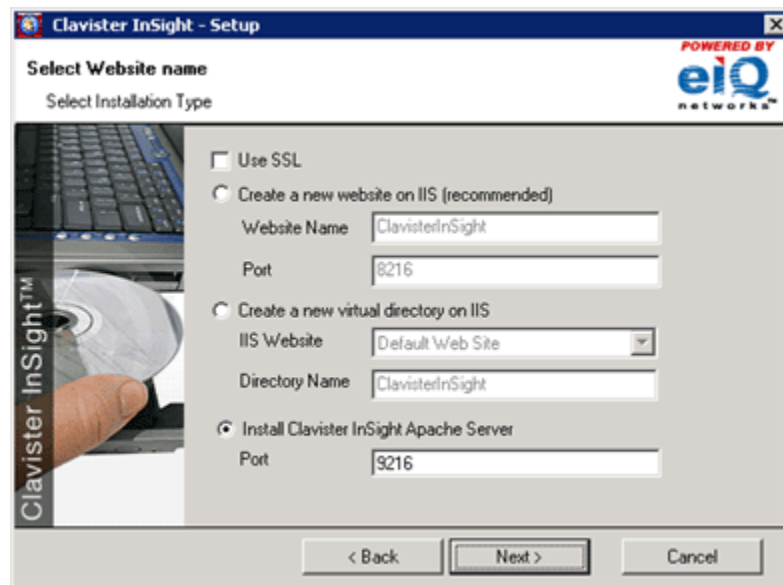
Follow the steps given below to install Clavister InSight as a virtual directory under the default website:

5. Select the **Create a new virtual directory** on IIS option.
6. Select the default website under which to create the directory. Setup creates the default directory **Clavister InSight**. To change this, simply type in a new name.
7. Click **Next**.

Install Clavister InSight on Apache Server

If IIS is not installed on your machine, setup defaults to this option. Follow the steps given below to install Clavister InSight Apache server:

Apache Server

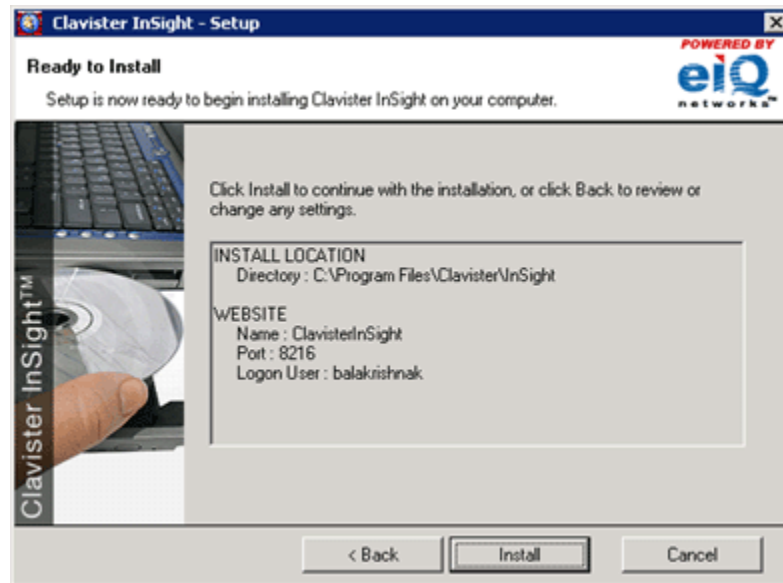


1. Select the **Install Clavister InSight Apache Server** option.
2. The default port is 8216. To change the port number, just type in the new port number in the Port box.
3. Clavister InSight allows you to use an SSL Port in conjunction with Apache Server. The default port is 9216. To change this, just enter a different port number.
4. Click **Next**.

Summary

This screen displays the summary of the settings that will determine where Clavister InSight is installed, what it has been installed as, and what port it uses to run on.

Summary Screen

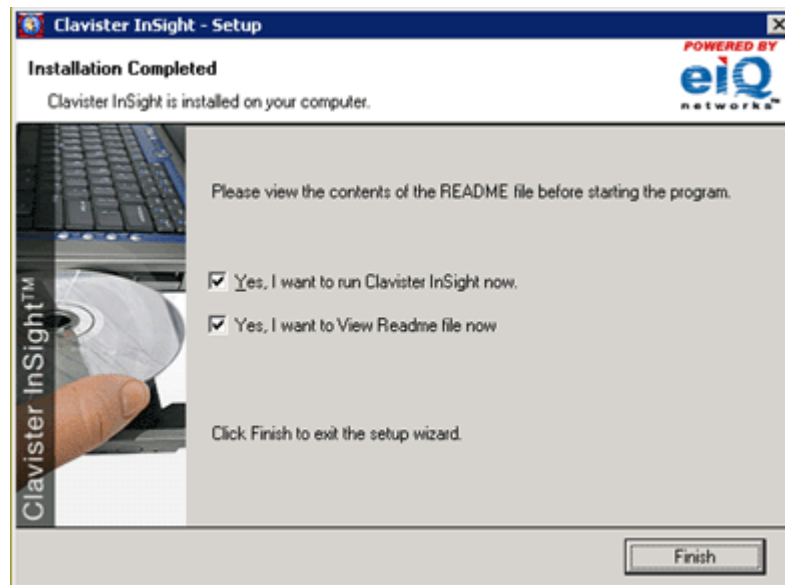


- ❖ Click **Install**.

The Finish Screen

The **Finish** screen displays after a successful installation. To run Clavister InSight, select the **Yes, I want to run Clavister InSight now** check box. To view the readme file, just select the **Yes, I want to View Readme file now** check box and click **Finish**.

The Finish Screen



- ❖ Click **Finish** to complete the installation and exit the setup wizard.



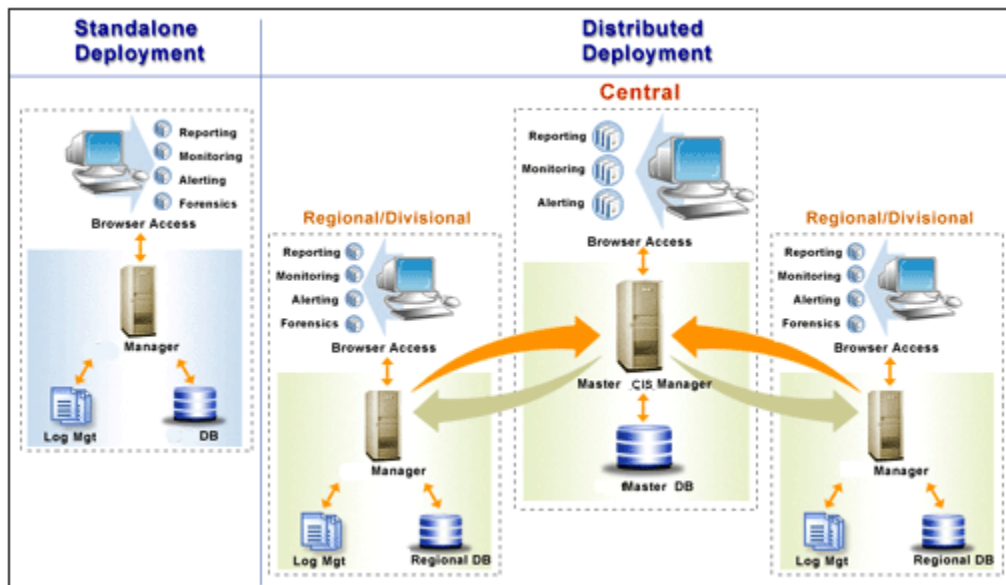
If you are installing Clavister InSight on Windows 2003, click [here](#) for instructions on how to configure the Internet Information Server.

Choosing Installation Type

You can install CIS in the following modes:

- ❖ Standalone
- ❖ Distributed
 - ❖ Regional
 - ❖ Central

CIS Deployment Schematic Diagram



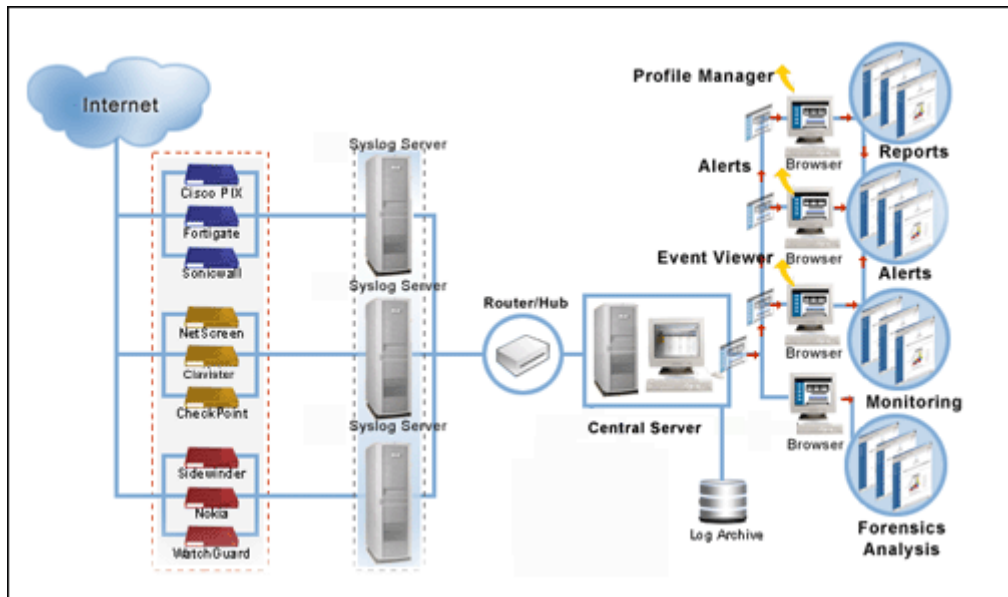
Choosing an Installation Option

After you understand the different installation options, you must decide which option is the most practical for your network. To do this, you will compare your network topology to the following topology scenarios. Each scenario represents a general network topology and the optimal CIS installation for that scenario.

Scenario for a Standalone Installation

It is a relatively small environment composed of several internal networks with Internet access. Publicly accessible server resources are placed in an isolated network and are protected by a firewall. Each floor network is also protected by a firewall/gateway. Another firewall protects the internal server farm network containing web, e-mail, FTP, file, and print servers. A standalone CIS server is used to monitor and report on events on all the devices in such networks.

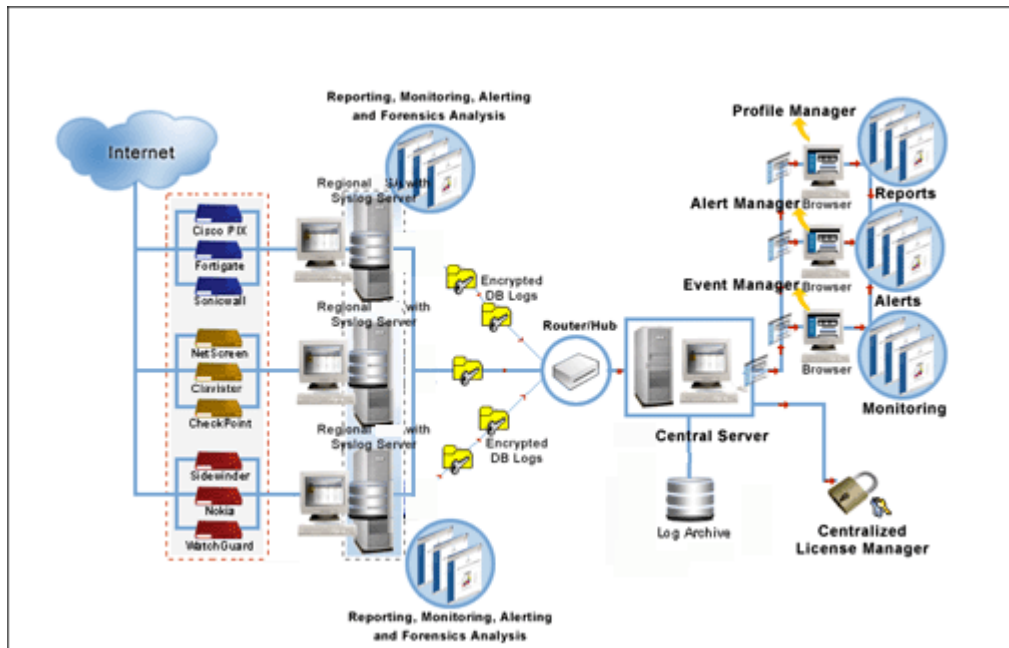
Standalone Scenario



Scenario for Distributed Installation

It is a multi-office environment composed of several internal networks dispersed across locations. Connectivity between these networks is provided through a service provider network. Internet access is provided only through a common location in the network with a firewall in place to support an isolated network and for general protection. Each remote office is also protected by a proprietary firewall/gateway. A CIS Central server operating in a distributed environment enables centralized reporting, device, configuration and license management for all the devices in the corporate network.

Distributed Scenario



A distributed CIS installation enables continuous management of security services throughout the company network from a single location called the Central. The distributed installation enhances CIS performance by off-loading critical functions of fetching data, processing it to OLF format and transforming them into deltas and finally storing them in the database. Now the job of central is only to report on the overall scenario from all its regional servers by only considering the top records for queries from each individual regional CIS servers.

Installation Guidelines

Keep the following guidelines in mind as you decide how to install your CIS Server.

- ❖ Encryption secures data traversing between different devices configured to your CIS; however, data traversing between a configured device and a CIS server is secure only if you choose your communication to be secure.
- ❖ Syslog data is streamed to CIS syslog server device via UDP packets to UDP port listening on port number 514 which can flood a network and all workstations directly connected to it. Do not install standalone system or a regional server in a network that cannot sustain heavy UDP traffic.

Installing Syslog Server

While some devices can export log files in a readable format, others typically do not write log information to a readable file. In such cases, you will have to rely on a syslog server to capture log information. Clavister InSight uses the syslog service to capture log file data.

The syslog service binds to the specified port and collects syslog data, which is streamed from single or multiple devices. It also allows you to delete old log files after a specified interval of time. The syslog service transfers delta log files to the Clavister InSight server in compressed format (GZIP files). These files are created depending on the delta frequency.

Example: If the delta interval is set to 30 minutes, the Clavister InSight syslog server creates a delta file every 30 minutes.

Once installed, the syslog server automatically updates delta files to the Clavister InSight database on a regular basis without intervention from the administrator.

The syslog server can be installed on any computer in the network.

One of the first things you should do after installing Clavister InSight is configure the syslog server. While doing this, you can backup all the logs streamed to the syslog server from various devices by setting up a backup syslog server.



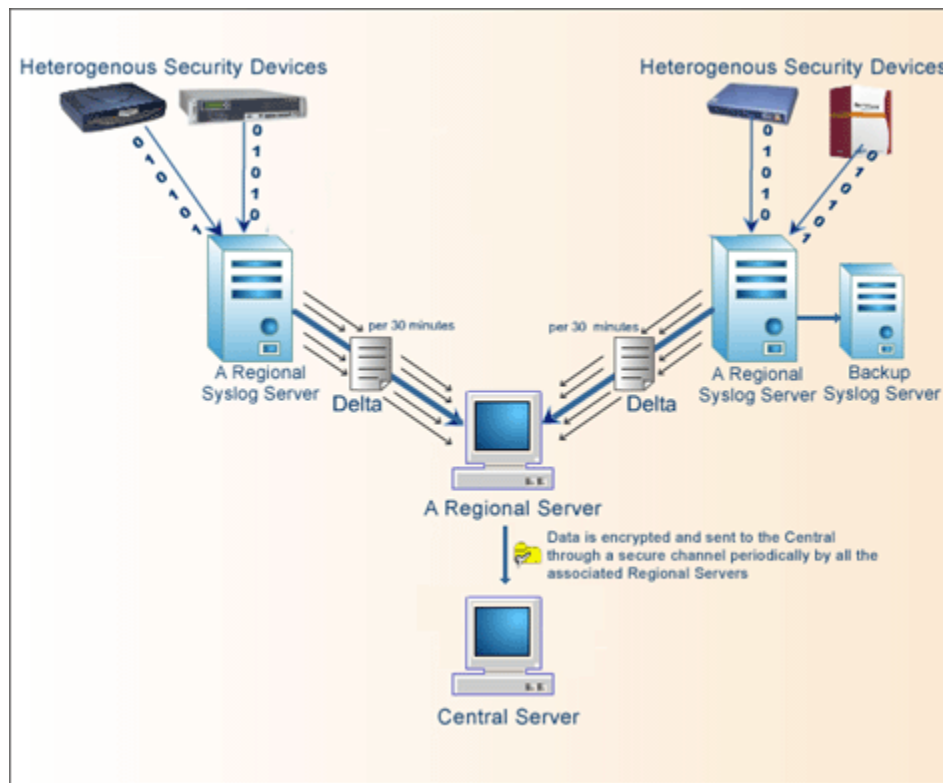
The backup syslog server must be a third party syslog server. The CIS syslog server forwards all the packets received from the devices to the backup syslog server. If the backup syslog server forwards any data back to the CIS syslog server, all such packets will be ignored.

CIS Architecture

This section explains how the logs are made available to Clavister InSight and how it generates a report.

In CIS 4.6, you can either opt for a stand-alone deployment, or a distributed deployment where one or more regional CIS servers forward syslog data to the central CIS server which stored it in a centralized repository.

Architecture for a Regional/Stand-alone



† Delta: A delta is an extract of an original log file that only contains data that has been logged since the last update.

† DB Logs: A DB Log is an extract of the top records for each query on a regional CIS server, which will be in encrypted format, and sent through a secure channel.

System Requirements

Make sure that the machine where you plan to install the syslog server meets the following minimum system requirements:

- ❖ Pentium 4
- ❖ 100MB Free Space
- ❖ 512 MB RAM

Recommended System Requirements:

- ❖ Pentium 4
- ❖ 1GB Free Space
- ❖ 1GB RAM



Since the CIS syslog server runs as a Windows service, it must be installed on Windows NT, 2000, XP or 2003.



To configure the Clavister InSight syslog server, you must be logged in as administrator.

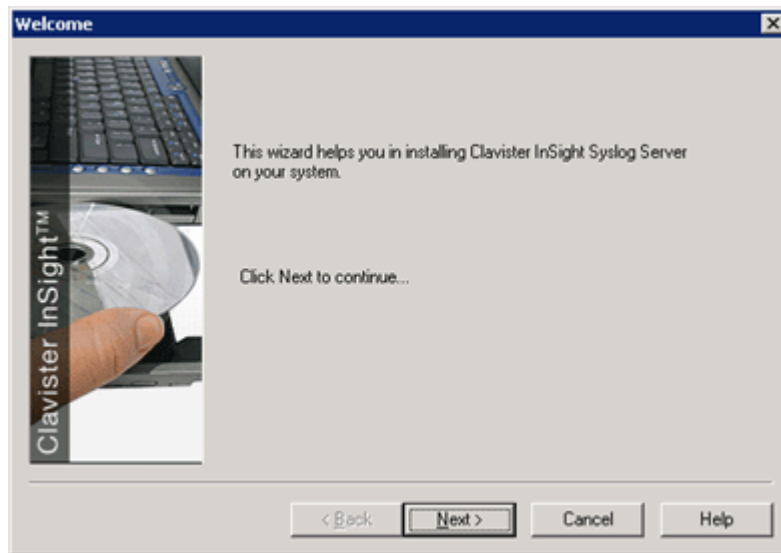


Since Windows XP with Service Pack2 features stricter Windows firewall rules and blocks all external applications, make sure you configure it to unblock the Clavister InSight Apache Server.

The Welcome Screen

The **Welcome** screen is the first screen that appears when you start the setup program. To proceed through the installation process, follow the steps given below:

The Welcome Screen

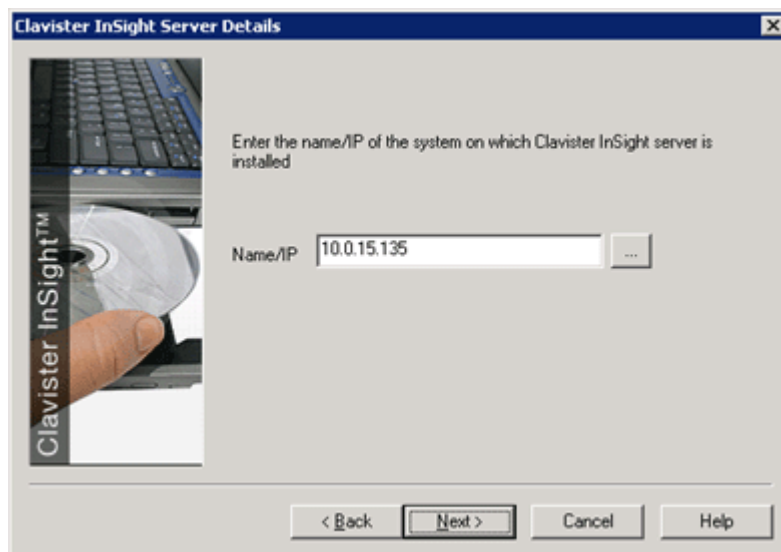


- ❖ Click **Next**.

Clavister InSight Server Location

Enter the system name/IP of the machine where the Clavister InSight server is installed. You can either type in the Name/IP of the system, or click the **Browse** button to select the machine where the Clavister InSight server is installed. This will enable the syslog server to identify the Clavister InSight server and update log file information. Follow the steps given below to specify the system name/IP:

Clavister InSight Location

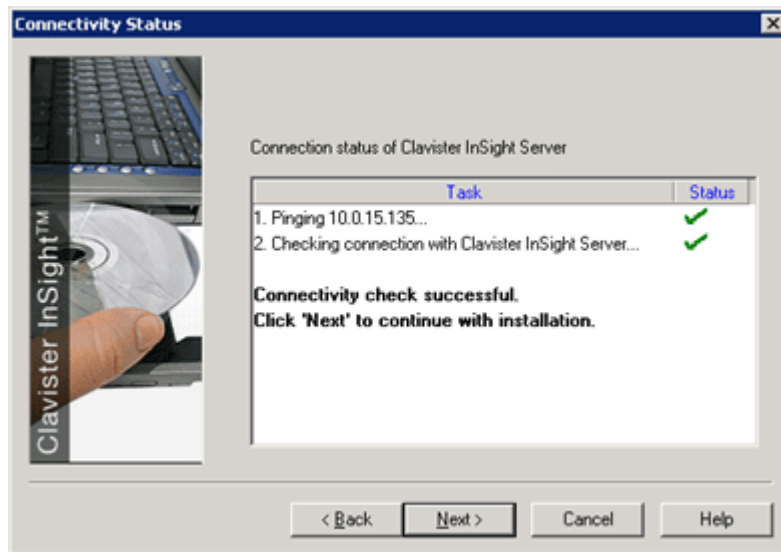


1. Enter the Name/IP of the machine where Clavister InSight is installed, or select a machine from the network.
2. Click **Next**.

Pre-Install Checker

This step displays the status of the connectivity of the syslog server with Clavister InSight. It lists the reasons for the failure of any checks with notes on how to correct the problems. The syslog server immediately tries to connect to the Clavister InSight server as per the information provided in the previous screens.

Connectivity Status



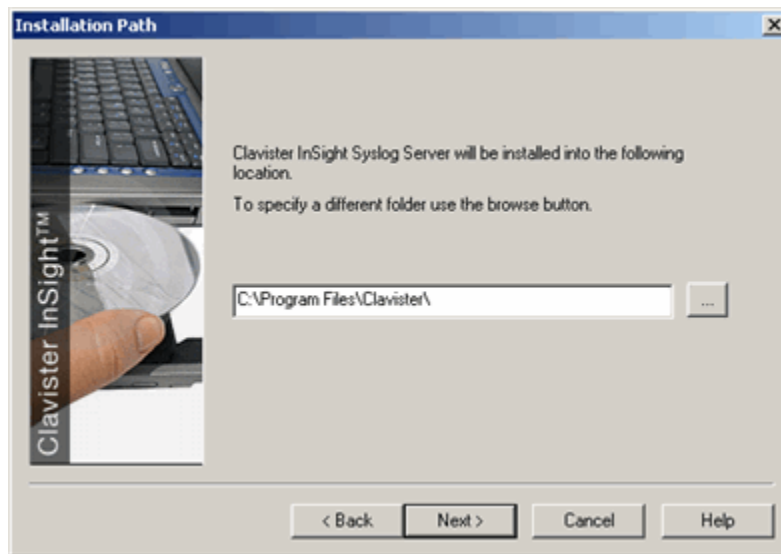
❖ Click **Next**.

Installation Path

This screen lets you specify the location where the syslog server must be installed. By default, the syslog server installs in the following location:

C:\Program Files\Clavister\

Installation Path

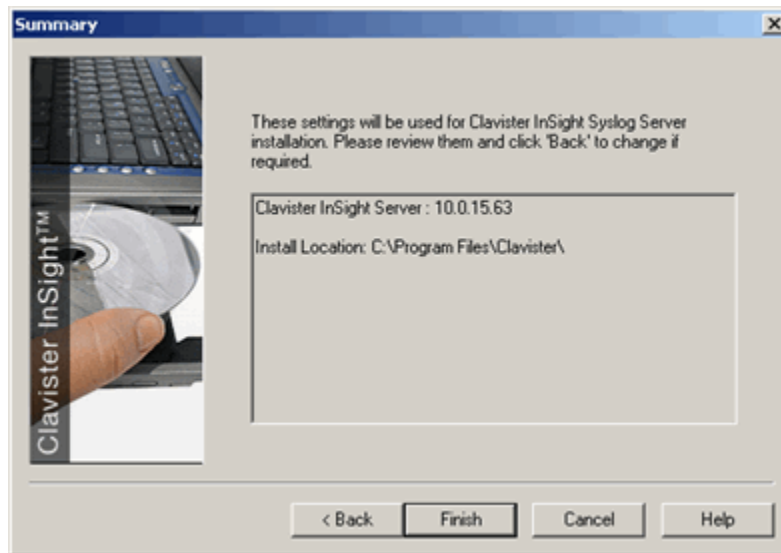


- ❖ To choose an alternate location, browse and specify a different location, and click **Next**.

The Summary Screen

The Summary screen displays a status summary of installation options you selected. To complete the installation process Click Finish.

Summary Screen



Uninstalling Syslog Server

To uninstall the syslog server, go to the **Add/Remove Programs** of the Windows Control Panel. The entry in the **Add/Remove Programs** added by the installer is *CIS Syslog Server*. The uninstaller is responsible for stopping all the related services and deletes all the files and registry keys copied during the installation procedure. It also provides you with an option to delete the collected log files.

- ❖ Click **Add/Remove** to uninstall the syslog server.

The Configuration Screen

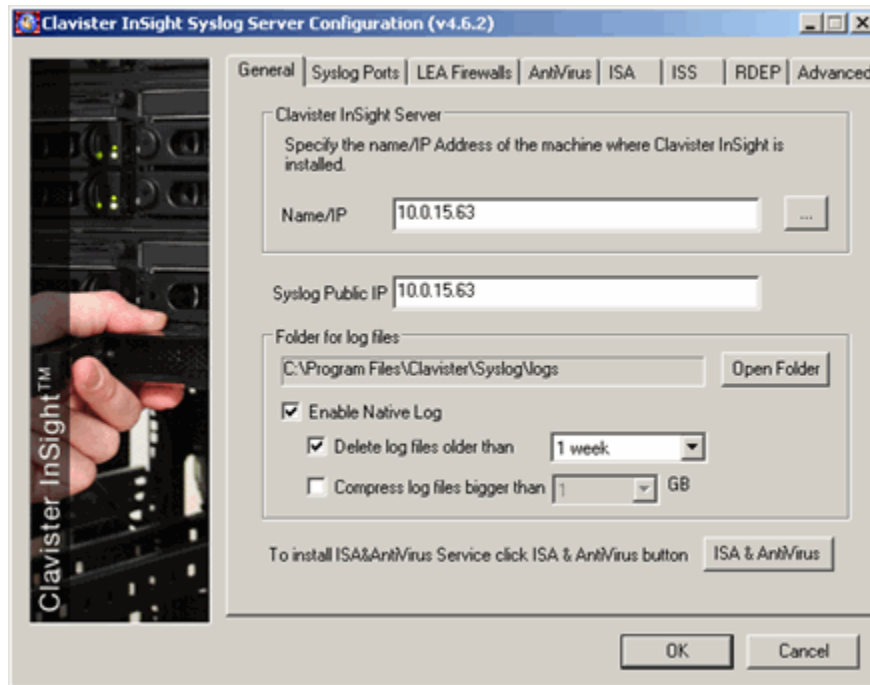
The **Configuration** screen allows you to configure settings for the syslog server. It contains the tabs General, Syslog Ports, LEA Firewalls, ISS, RDEP and additional tabs for ISA Devices and Anti-Virus Server. In addition, the Advanced tab in the Configuration window a backup syslog server.

The General Screen

This screen allows you to change the target location for the collected logs. The default delta file update frequency is 30 minutes and can be customized as per your requirement. You can also specify the time period to retain the old logs.

By default, the syslog server receives data and redirects it to the CIS server once every 30 minutes. But the database is updated every 1 hour. So in the first hour after installation, Clavister InSight will not have data in the database.

General Syslog Server Configuration



- ❖ Enter the Clavister InSight server Name/IP in the **Name/IP** box. Alternately, browse to the Clavister InSight machine using the browse option.
- ❖ **Enable Raw Logging:** Select this option to store log files collected by the CIS syslog server. If you leave this check box clear, logs are not stored on the syslog server, but forwarded to the CIS server.
- ❖ **Delete raw log files:** You can delete raw log file collected by the CIS syslog server earlier than 2 Days, 1 Week, 1 Month, 3 Months, 6 Months, 1 Year, 2 Years, and 3 Years.
- ❖ **Compress log files bigger than:** You can specify the size limit of the raw log file collected by the CIS syslog server. All log files exceeding this size will be compressed into zip format.

Install ISA and Anti-Virus Service

To activate ISA and anti-virus services, click the **ISA & Anti-Virus** button in the Syslog Server Configuration window.

Installing ISA and Anti-Virus service



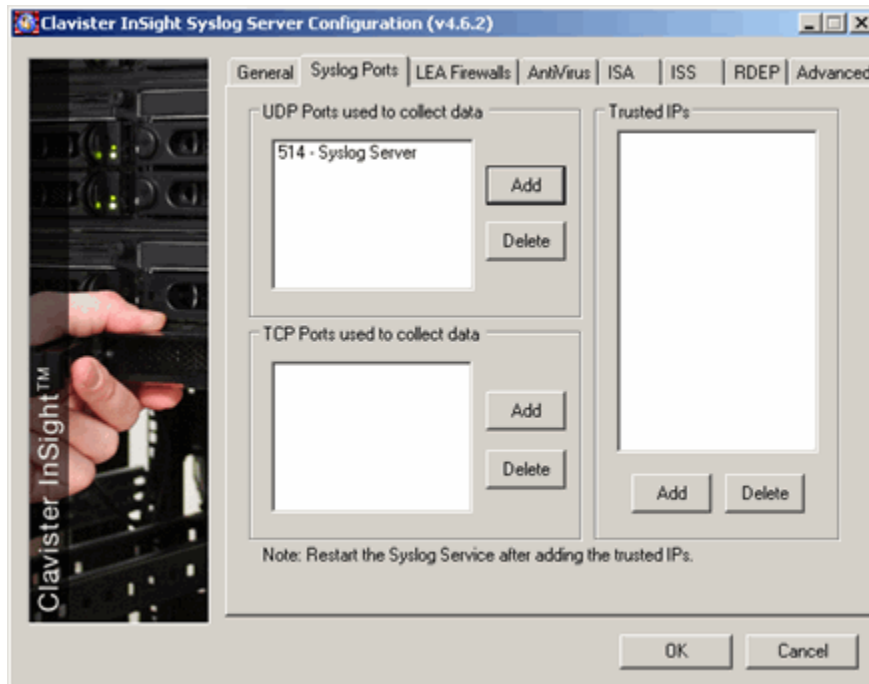
Follow the steps below to install the ISA and anti-virus service:

1. Click the **ISA & Anti-Virus** button to view the corresponding window.
2. Enter the user name and password with the administrator privileges on the local system.
3. Select the **Do not verify user name and password** check box if you have logged in with the same user privileges as entered in the respective text fields.
4. Click **OK**.

Syslog Ports Screen

This screen displays the standard TCP and UDP ports that the syslog server listens on. You can add additional ports that the syslog server will use to collect the log data. Port numbers must be between 1 and 65,535.

Syslog Server Ports Configuration



Follow the steps described below to add a TCP port:

1. Click **Add**. The **Add UDP Port** screen opens.
2. Enter the UDP port number to listen for the incoming data from the Syslog server.
3. Click **OK**.
4. To delete a port number, select the port number from the list and click **Delete**.

Follow the steps described below to add a TCP port:

1. Click **Add**. The **Add TCP Port** screen opens.
2. Enter the TCP port number to listen for the incoming data from the Syslog server.
3. Click **OK**.

4. To delete a port number, select the port number from the list and click **Delete**.

Follow the steps described below to add Trusted IPs:

In this pane, local network security administrator enters the details of the IP addresses which come under firmware IP addresses.

1. Click **Add** to enter a trusted IP address in the IP box.
2. Click **OK**.

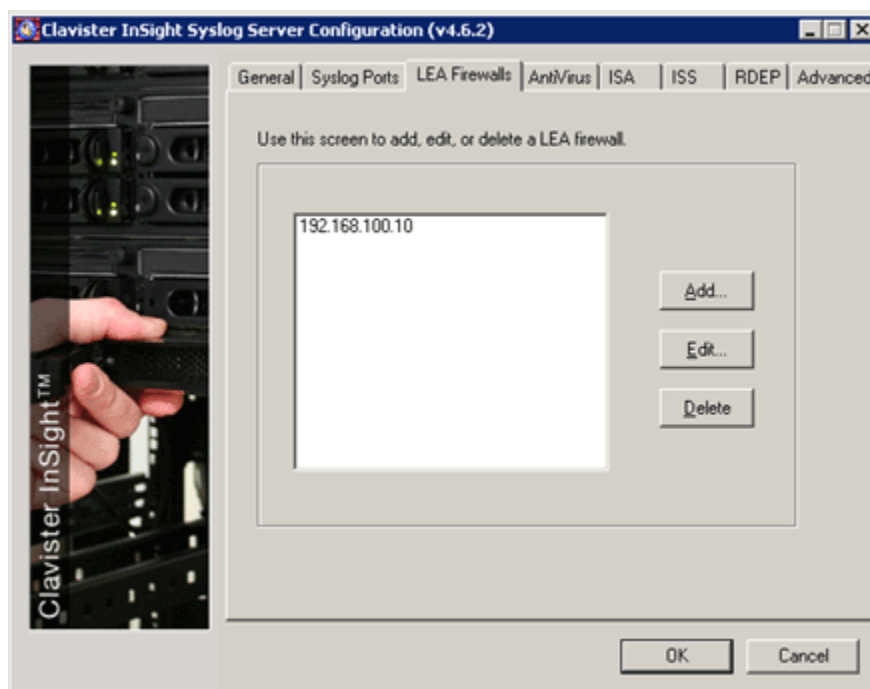
LEA Firewalls

Use this tab to add, edit, or delete a LEA firewall. In addition, you can also enable streaming of events collected from the LEA firewall to the Security Center



Before adding a LEA firewall, configure the Check Point server and the CIS syslog server.

LEA Devices Configuration



1. In the **User Name** box, enter a user name with administrator rights to connect to the machine running Clavister InSight.
2. Click **OK**.

Add LEA Firewall

To open the **Add LEA** screen, click **Start → Programs → Clavister → Clavister InSight v4.6 → Configure Syslog Server → LEA Firewalls → Add**.

Configure the OPSEC™ Application object in the SmartCenter Server.

1. In SmartDashboard → Manage → Network Objects → New.. → Node → Host, enter a name and IP address for the CIS host.
2. In Manage → Servers and OPSEC Applications → New.. → OPSEC Application enter a name, the host object created in step 1 above, and check LEA in the Client Entities list. Click on the **Communication** button and enter an Activation Key. The Trust state will be “Initialized but trust not established”.

Adding LEA Firewall

This screen allows you to add a LEA firewall.

1. Enter the IP address and host name of the machine where Check Point Management Server is installed and running.
2. Enter the LEA port number in the **LEA Port** box.
 - ❖ 18184 → for authenticated connection
 - ❖ 0 → for unauthenticated.

Note: the default connection is authenticated and the port number entered must not be greater than 32767.

3. Enter the values (between -720 and +720) for Gmt Offset in the **Gmt offset** box.
4. Choose your connection mode:
 - ❖ Select the **Use Authentication** check box for authenticated connection with the LEA firewall.
 - ❖ Select the **Use Encryption** check box to encrypt communication with the LEA firewall.
 - ❖ Leave both the check boxes clear to use unauthenticated communication.
Note: The default connection method is Authenticated and Encrypted. Contact Check Point Tech Services for instructions on configuring the Check Point SmartCenter Server to accept unauthenticated connections.

Verify the Configuration

On the SmartCenter server check the OPSEC Application object -> select the Communication button. The Trust state should be "Trust established".

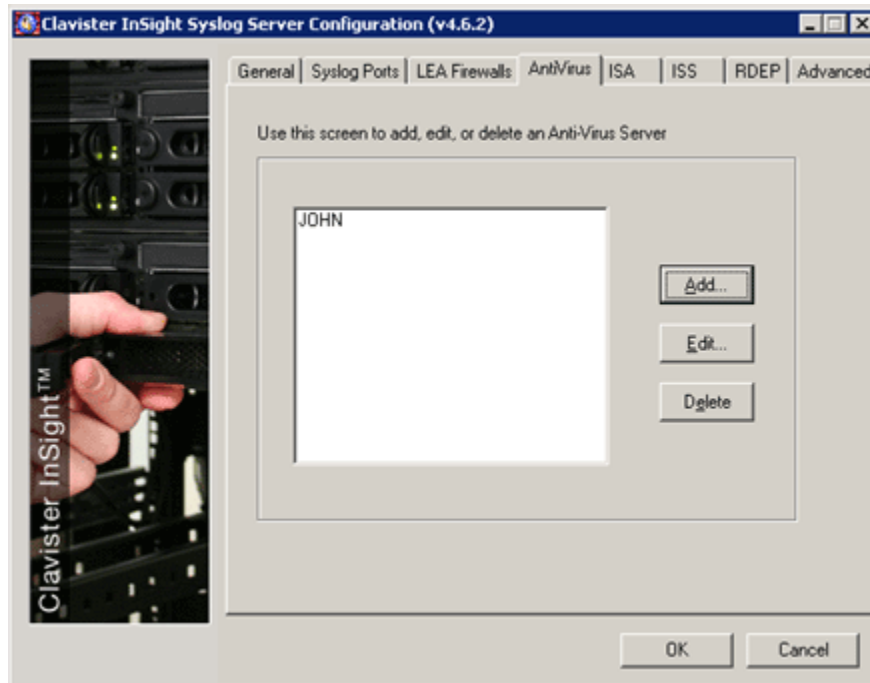
5. If you have chosen the Use Authentication mode, enter:
 - ❖ OPSEC™ application name in the **Application Name** box.
 - ❖ Activation key to activate the application in the **Activation Key** box.
6. Click **OK** to save your settings. This will create .sic file and a certificate in the syslog folder.

For more detailed instructions on how to obtain authentication from the Check Point server, click the Help button on this window.

The Anti-Virus Screen

This screen contains a box that lists the Interscan Viruswalls added for the anti-virus service. Use the **Add**, **Edit** and **Delete** buttons to add, edit and delete an Interscan Viruswall.

Anti-Virus Configuration

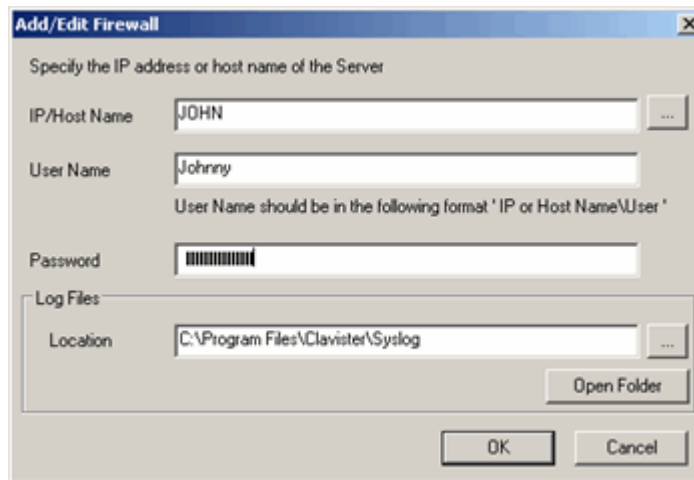


Add Anti-Virus Service

This screen adds an anti-virus service. Click the **OK** button to save the settings or discard the changes by clicking the **Cancel** button.

To open the **Configuration** screen later, click **Start → Programs → Clavister → Clavister InSight v4.6 → Configure Syslog Server → AntiVirus → Add**.

Add Anti-Virus Service



The screenshot shows a dialog box titled "Add/Edit Firewall". The main instruction is "Specify the IP address or host name of the Server". The fields are as follows:

- IP/Host Name:** JOHN
- User Name:** Johnny
- Password:** [Masked]
- Log Files Location:** C:\Program Files\Clavister\Syslog

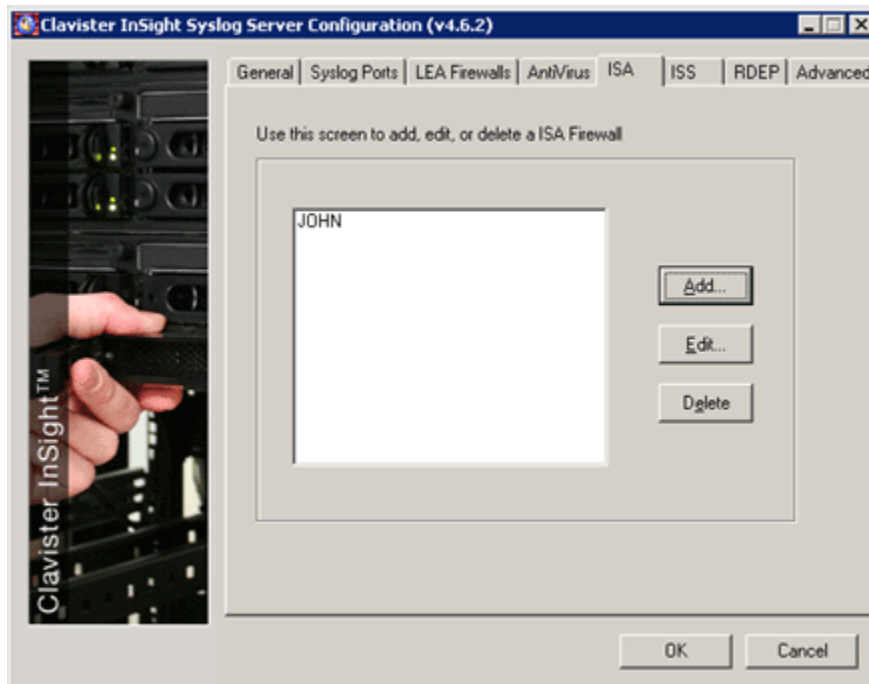
Buttons include "OK", "Cancel", and "Open Folder" (located next to the Log Files Location field).

1. Enter the IP Address or Host Name for the machine in the **IP/Host Name** box where Interscan Viruswall Anti-Virus Server is installed and running.
2. Enter the User Name and Password that has admin privileges on the machine running the anti-virus server.
3. Browse to the location where the log files are stored.
4. Click **OK**.

The ISA Device

This screen contains a list box showing the ISA Devices added for the anti-virus service. The **Add**, **Edit** and **Delete** buttons are provided to modify the configuration of ISA Devices.

ISA Device Screen

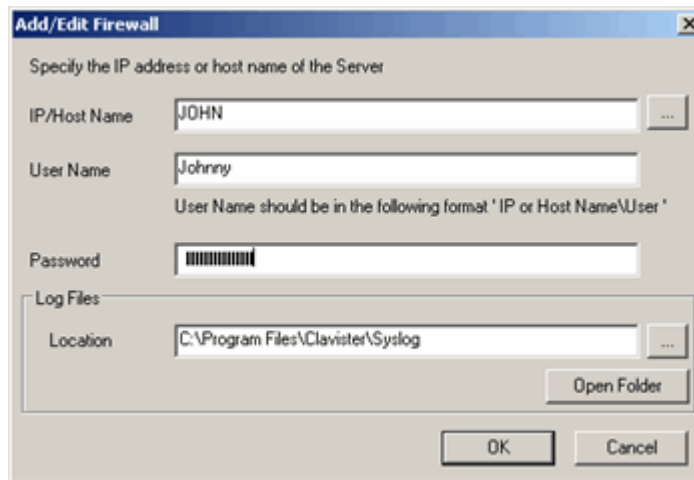


Add ISA Firewall

This screen allows you to add an ISA firewall. Click the **OK** button to save the settings or discard the changes by clicking the **Cancel** button.

To open the **Configuration** screen later, click **Start → Programs → Clavister → Clavister InSight v4.6 → Configure Syslog Server → ISA → Add**.

Add ISA Firewall Service



Specify the IP address or host name of the Server

IP/Host Name: JOHN

User Name: Johnny

User Name should be in the following format 'IP or Host Name\User'

Password: [Masked]

Log Files Location: C:\Program Files\Clavister\Syslog

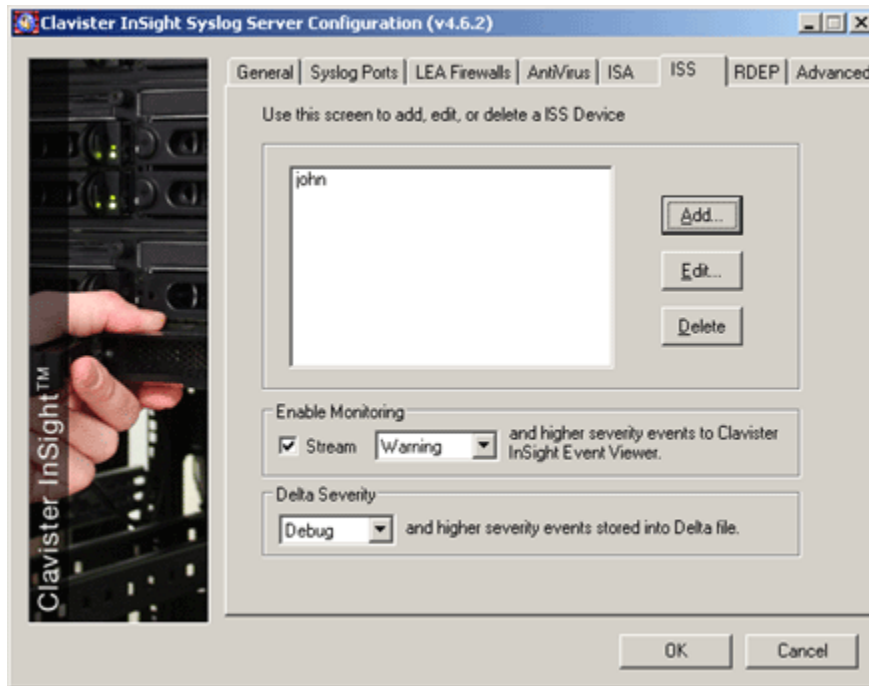
Buttons: OK, Cancel, Open Folder

1. Enter the IP address or host name for the machine in the **IP/Host Name** box where ISA Server is installed and running.
2. Enter the User Name and Password that has admin privileges on the machine running ISA Server.
3. Browse to the location where the log files are stored.
4. Click **OK**.

The ISS Device

This screen contains a list box showing the ISS Devices added for the AntiVirus service. The Add, Edit and Delete buttons are provided to modify the configuration of the ISS Devices.

ISS Device Screen



Add ISS Firewall

This screen allows you to add an ISS firewall. Click Save to save the settings or discard the changes by clicking the Cancel button.

To open the **Configuration** screen later, click **Start → Programs → Clavister → Clavister InSight v4.6 → Configure Syslog Server → ISA → Add**.

Add ISS Firewall Service

The screenshot shows a dialog box titled "ADD/EDIT DEVICE" with a close button in the top right corner. Below the title bar, it says "Enter information for the new ISS SQL Server." There are four input fields: "Device Name/IP" with the text "Johnny", "User Name" with "jwilliam", "Password" with "*****", and "Refresh Interval" with a dropdown menu showing "10 Sec". At the bottom, there are three buttons: "Save", "Cancel", and "Check Connection".

1. Enter the IP address or device name for the machine in the **Device Name/IP** box where ISS Server is installed and running.
2. Enter the User Name and Password that has admin privileges on the machine running ISS Server.
3. Select the refresh interval from the **Refresh Interval** drop-down list.
4. Click on the **Check Connection** button to verify the availability of the ISS server.
5. If the connection check is successful, click **Save**.

Enable Monitoring for Syslog Server: Specify what events should be logged onto the Event Manager from the raw log data that is retrieved by the syslog server. Follow the steps to enable monitoring.

6. To enable streaming of events to the Event Viewer, select the **Stream** check box.
7. From the drop-down list select the event severities. To view all events, select **Debug**. Available severity types are:
 - ❖ Emergency
 - ❖ Alert
 - ❖ Critical
 - ❖ Error
 - ❖ Warning
 - ❖ Notice
 - ❖ Information
 - ❖ Debug

Delta Severity: Specify what events should be considered to save in the deltas while the raw log files are compressed into delta files. Follow the steps below to specify delta severity.

From the drop-down list select the event severities, you want to store in the delta files. Available severity types are:

- ❖ Emergency
- ❖ Alert
- ❖ Critical
- ❖ Error
- ❖ Warning
- ❖ Notice
- ❖ Information
- ❖ Debug

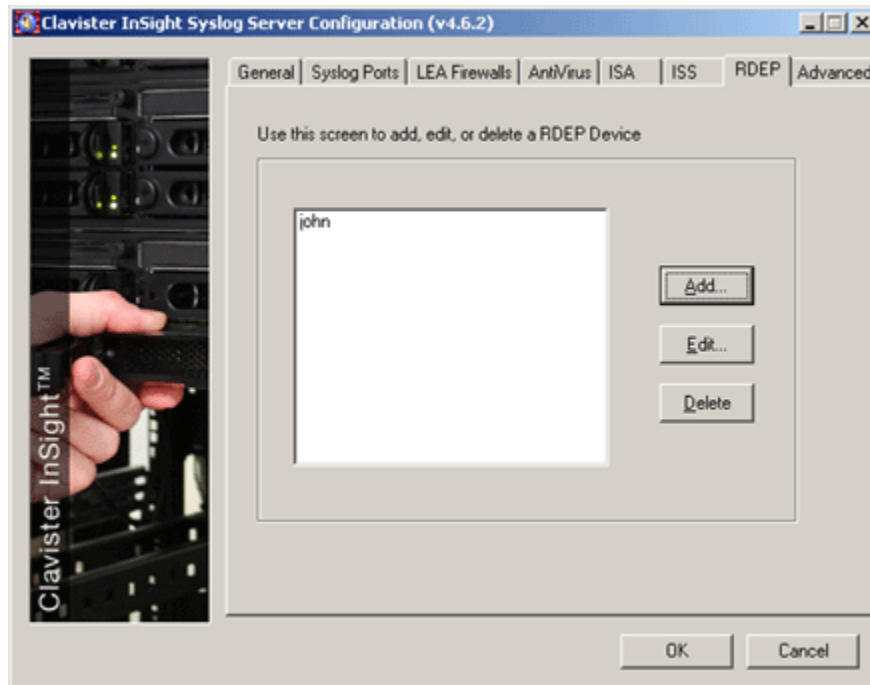
8. Click **OK**.

RDEP

Remote Data Exchange Protocol (RDEP) is the protocol used in Cisco 4.x sensors. For example, a Cisco CSIDS 4235 device uses RDEP to transfer the XML formatted logs. Since RDEP is a pull technology, a remote CIS syslog server must connect to the sensor on port 443 as an authorized user with a minimum of "view" privileges, access the log directory and pull them to the CIS syslog server.

The session is decrypted and the logs are stored in the clear text XML format on the CIS syslog server. In a distributed environment, you might be able to set up the syslog server to read the logs and send them to CIS server where the data is stored in the database.

RDEP Screen



Add RDEP Device

Follow the steps described below to add an RDEP device:

1. Enter the IP address or device name of the machine where the IDS Server is installed and running in the **Device Name/IP** box.
2. Enter a username and password with admin privileges on the machine running the IDS Server.
3. Enter the polling interval at which you want your agent to connect to the Cisco IDS using RDEP protocol and pull logs from device to the syslog server.
4. To save your configured settings, click **Save**.



Use the **Edit** button to modify the configuration settings of your IDS Device.

Add RDEP



Enter information to add the new RDEP Device

Device Name/IP: JOHNNY

User Name: John

Password: *****

Polling Interval: 30 Sec

IDS Version: 4.x

SSL Enabled

Save Cancel

The Advanced Tab

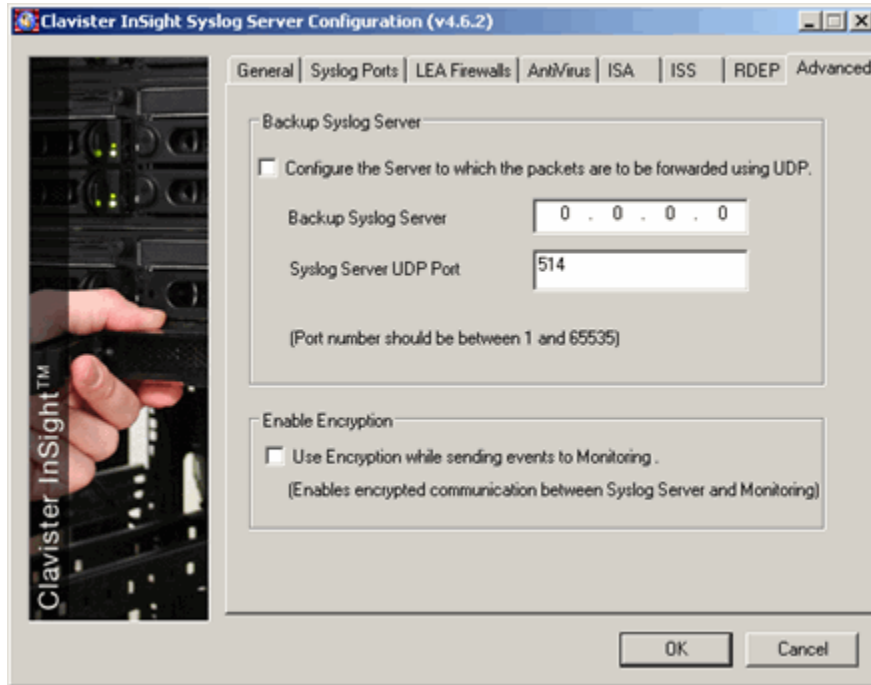
This screen helps you configure a backup syslog server to store backups of the syslog data that is forwarded by the CIS syslog server.

The backup syslog server must be a third party (for example, Kiwi) syslog server. The CIS syslog server forwards all packets received from the devices to the backup syslog server.

Follow the steps described below to configure a backup syslog server:

1. Enter the IP address of the machine where the backup syslog server is installed and running.
2. Enter the syslog server port from where the syslog events are to be collected.
3. To enable the backup syslog server, select the **Enable Encryption** check box. To disable it, leave the check box clear.
4. Click **OK**.

Advanced Screen



Appendix A

Steps specific to the Windows 2003 Platform

For Clavister InSight to work properly, the following are the settings you will need to make on IIS:

- ❖ [Adding ISAPI Filter](#)
- ❖ [Enabling SSL ports on IIS](#)

Windows 2003 operating system requires a few configuration changes to allow Clavister InSight (CIS) to work properly. The following are the settings you will need to make:

- ❖ [Configure IIS 6.0 for CIS to allow web service extensions](#)
- ❖ [Configure IIS to allow all CGI extensions](#)
- ❖ [Configure IIS to provide exception for MIME Type extensions](#)
- ❖ [Configuring IIS to use the IUSR Account](#)
- ❖ [Configuring the IUSR Account to have the necessary permissions](#)
- ❖ [Configure IIS to remove the application mapping for .ext files](#)
- ❖ [Enable ActiveX Controls and Plug-ins](#)
- ❖ [Configuring IIS for accessing the application using Remote Desktop](#)

Note: If you install CIS as a Virtual Directory on IIS, it is essentially an alias to the default website. So, all the configuration changes made on the default website will be inherited by the virtual directory.

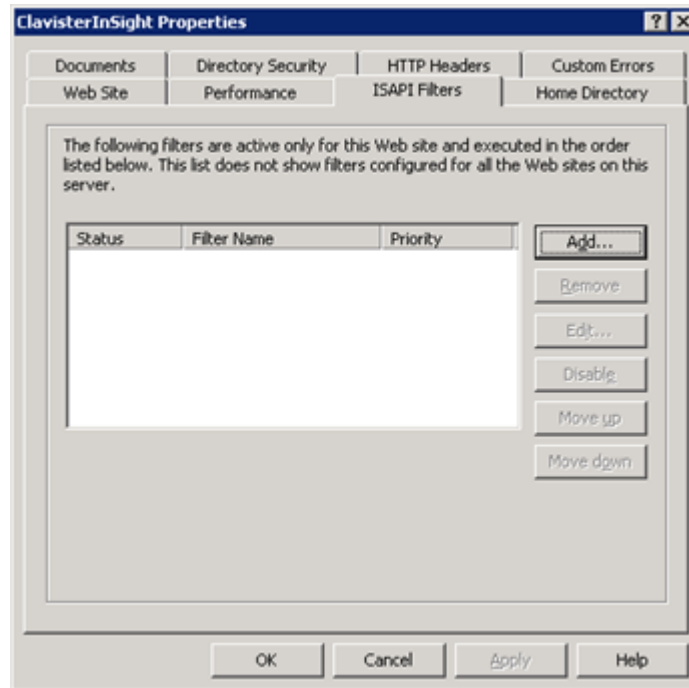
Windows 2003 - Service Pack Requirement

If Clavister InSight is installed on Windows 2003, it is necessary to have SP1 installed on it to facilitate MHTML report generation.

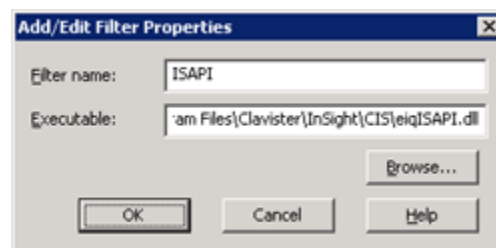
Adding ISAPI Filter

Follow the steps described below to add the eiqlsapi.dll filter to the website:

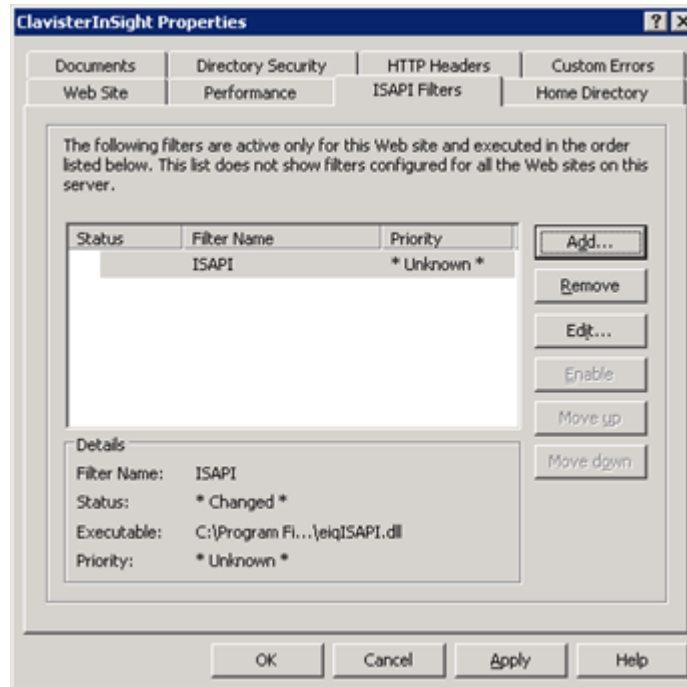
1. Right-click on the website name and click **Properties**.



2. Select the **ISAPI filters** tab and click **Add**.



3. In the **Filter Name** box, type iPolicy and enter (or browse to) the location where the file eiqlsapi.dll is located.



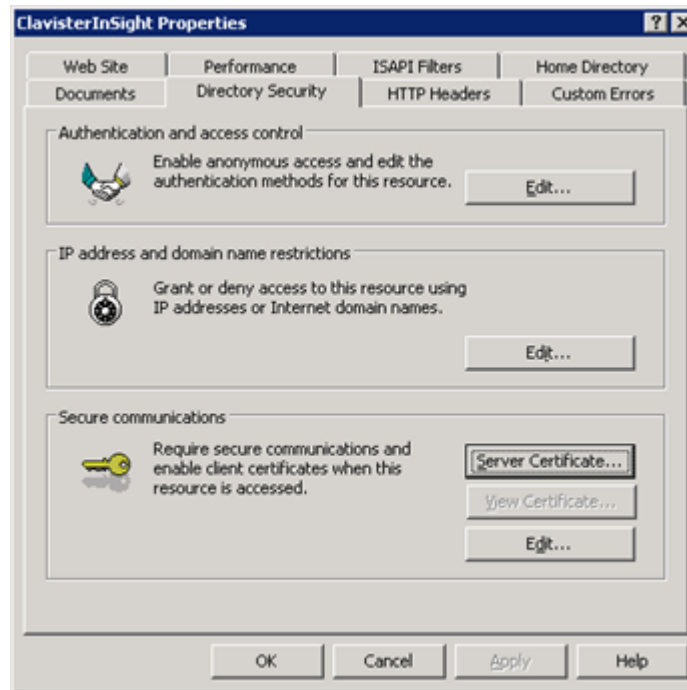
Click **OK** and then click **OK** again.

Enabling SSL Port on IIS

Follow the steps described below to enable an SSL port on IIS:

Step 1: Generate the certificate request:

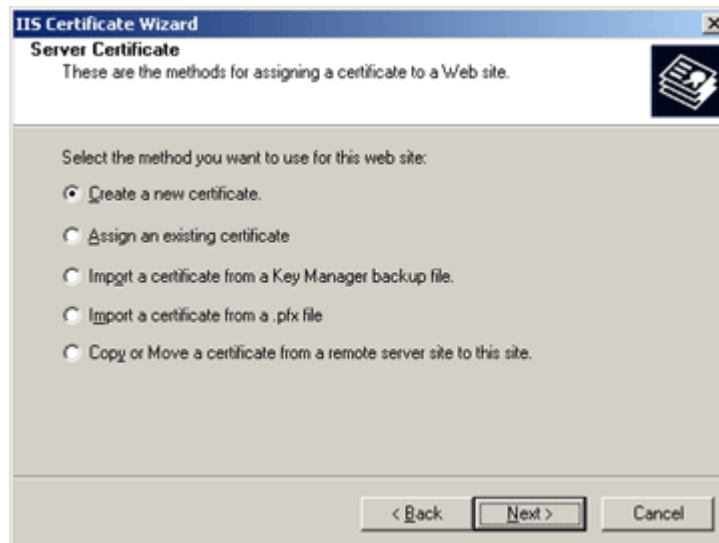
Right-click on the website name and click **Properties**:



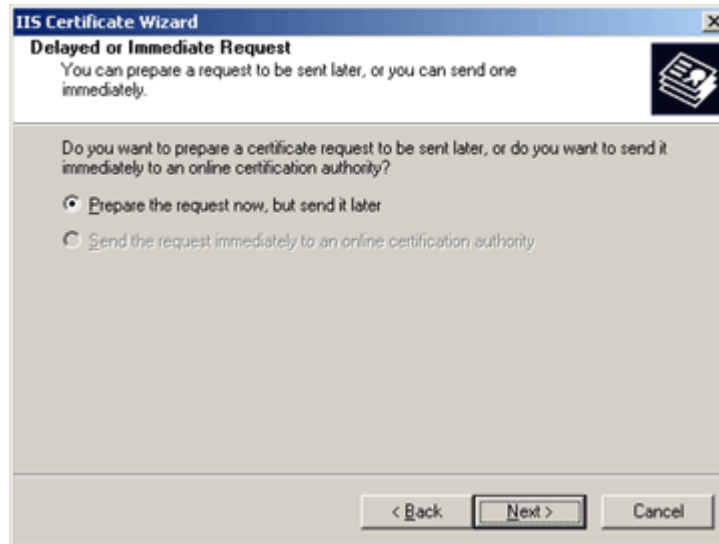
Step 2: Select the Directory **Security** tab and click **Server Certificate**.
The **Web Server Certificate** wizard opens.



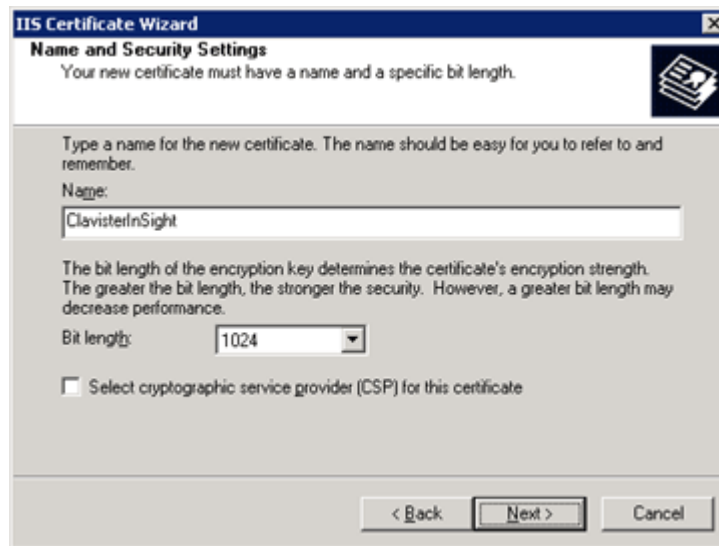
Click **Next**. The **Server Certificate** screen opens.



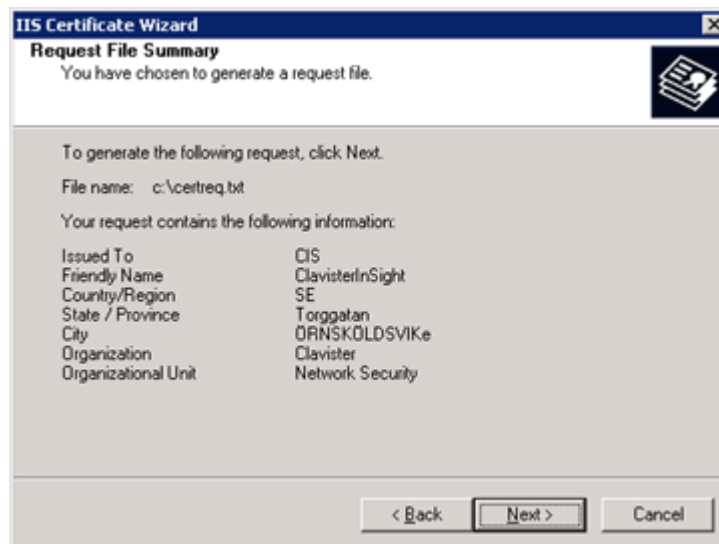
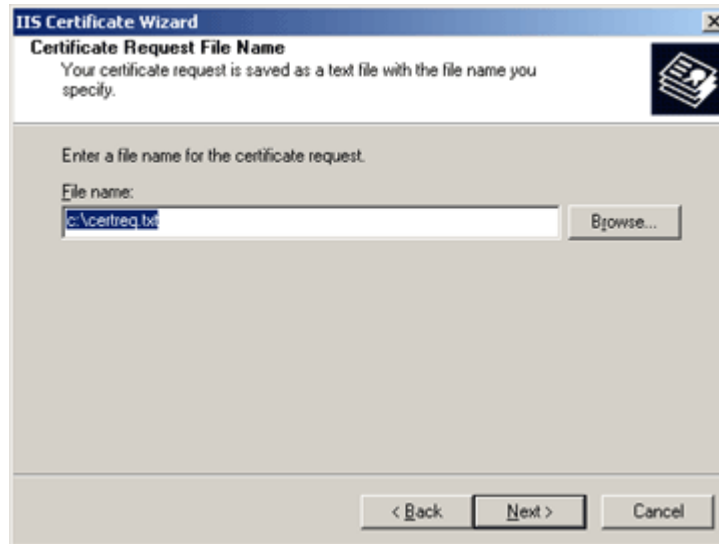
Select the **Create a new certificate** option and click **Next**.



You can prepare a request and send it later or prepare and send one immediately. Select **Prepare the request now, but send it later** and click **Next**.



Enter the details of the Organization, common name of the site and the geographical information in the appropriate screens.



Click **Next** and then click **Finish** to complete the wizard.

Step 3: Immediately, copy the request generated (**C:\certreq.txt**) and put it in the same path as you installed the application (Apppath ...\Clavister\InSight\CIS).

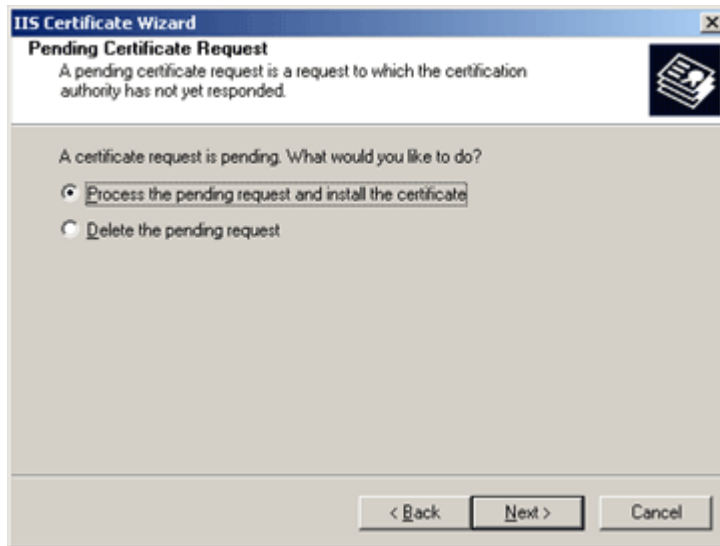
Rename the **certreq.txt** file to **CIS.csr**

After you rename the certreq.txt file, go to **Start → Programs → Clavister → Clavister InSight v4.6 → Create SSL Certificate**. The **Create SSL Certificate** wizard opens. From the wizard, browse to select the **CIS.csr** file and finish the process of creating a certificate (*CIS.cer*).

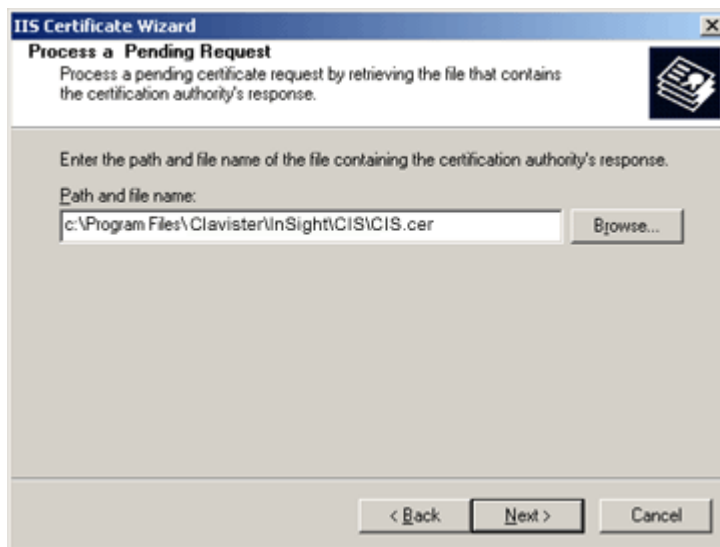
Click here for detailed explanation on creating a certificate on IIS.

Now go back into **IIS admin** → **Right-click on the website** → **Properties** → **Directory Security tab** → **Click on the Server Certificate** button and follow the steps below to import the certificate (*CIS.cer*) you created from the Create SSL Certificate wizard.

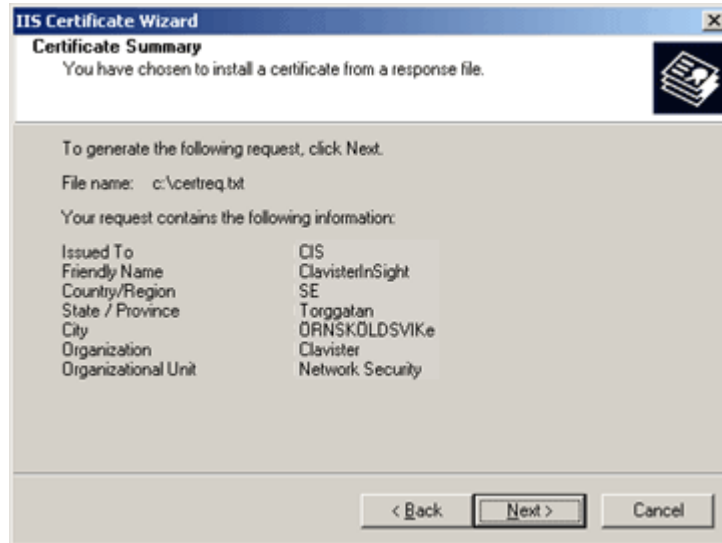
Step 4: Go to **Directory Security** screen, and click **Server Certificate** under **Secure Communications** for processing the pending request. Click **Next**.



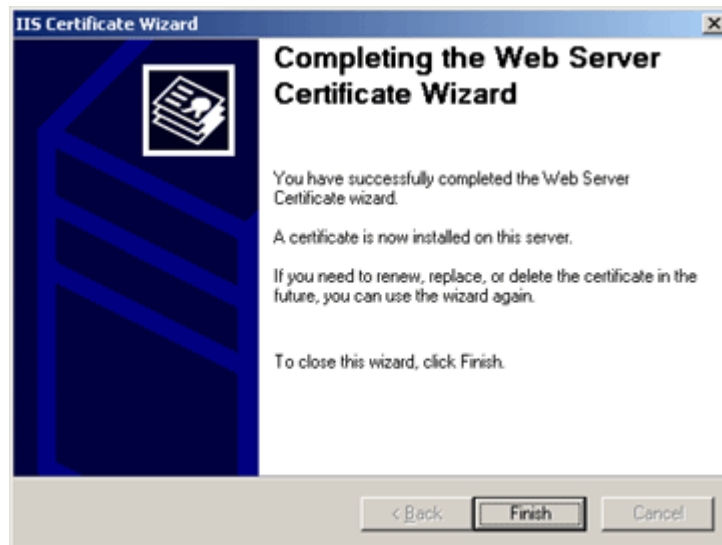
Browse to add **CIS.cer** file as shown below



The pending certificate request can now be processed and a new certificate can be generated.



Verify the details of the certificate that is to be created and click **Next**.



Click **Finish**. The certificate is created successfully.

Now from the IIS wizard, right-click on Clavister InSight website properties window and click the **Web Site** tab, you will see that the **SSL** option is enabled.

Change the port to any number (for ex: 9216) you want browse CIS application with **SSL**.

Note: If you have installed CIS on IIS using SSL, you need to leave the **Do not save encrypted pages to disk** check box clear on the **Advanced** tab of Internet Options.

Creating SSL Certificate on IIS

SSL Certificate can be created either:

- ❖ At product installation time by selecting **Use SSL** option; OR
- ❖ After product installation by choosing: **Start -> Programs -> Clavister -> Clavister InSight v4.6 -> Create SSL Certificate.**

SSL Certification Wizard pops up in either of the options above.

4. Selecting to create SSL certificate, the Introduction Screen of the wizard for SSL Certificate pops up. Click **Next**.
5. The Distinguished Name Details window opens. Enter the details of Organization, Geographical location, e-mail address and the Common Name that you want to associate with the certificate.
6. Provide the Password which is to be used to generate the certificate.
7. Click Next. The Generate Master Certificate screen opens.
8. Click Next to create a Master Certificate to be used for signing client and server certificates. Accept to sign the certificate by typing 'y' for yes in the command prompt.
9. You would need a certificate request created through IIS Admin to be signed by the Master Certificate Created above.

NOTE: Using IIS Admin, create a certificate request and copy that file as **CIS.csr** to product installation path.

10. Click **Next** to proceed to sign the certificate request and create CIS.cer certificate file for IIS.

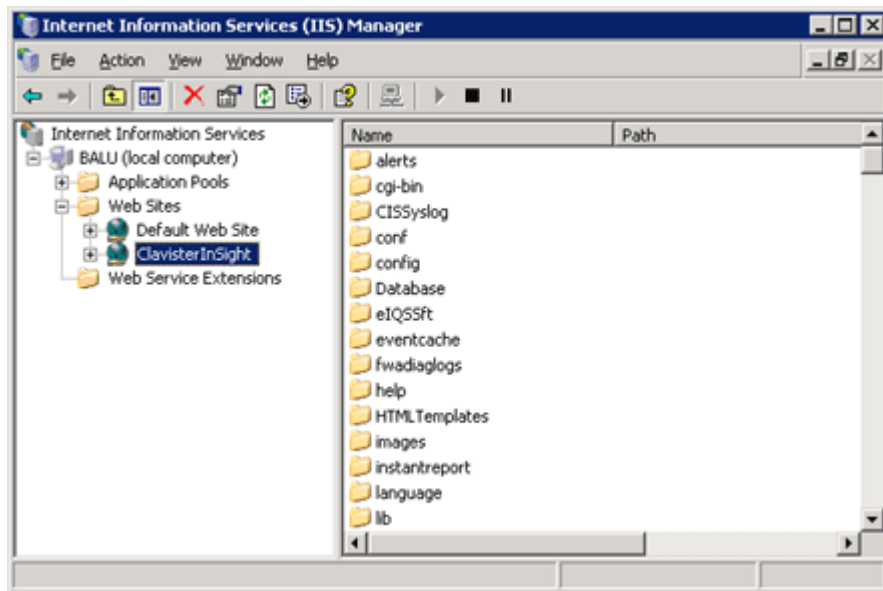
Note: The **CIS.cer** file generated by the Create SSL certificate wizard can be used to process the pending certificate request in the IIS Create Certificate wizard.

Now go back into IIS admin -> right-click on **web site -> Properties -> Directory Security Tab -> Click on server certificate button ->** follow the steps and import the certificate you created above.

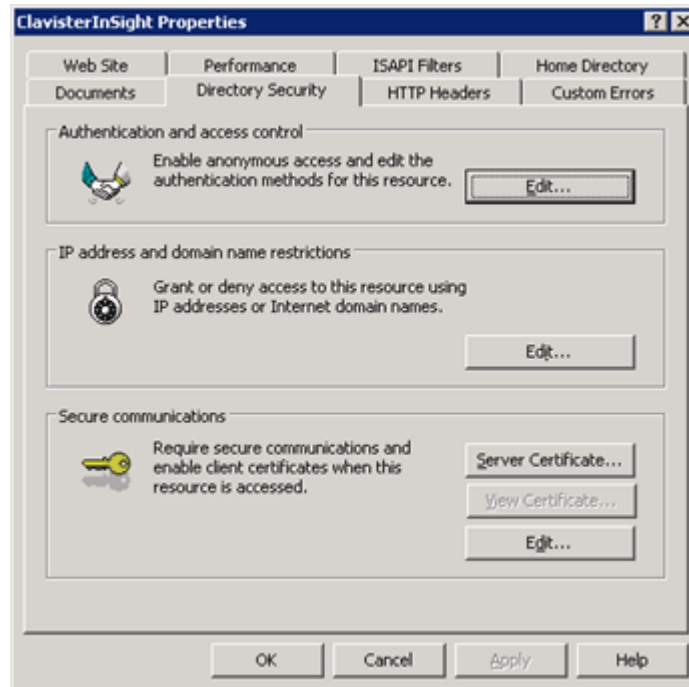
By default IIS on Windows 2003 does not allow .cgi and .pl. IIS makes a call to perl.exe to run the code. If you associate .pl and .cgi in Explorer to perl.exe by allowing all unknown CGI extensions, it will run it in a DOS window using perl.exe. IIS then makes a call to Perl and displays the code produced.

Configuring IIS 6.0 for Clavister InSight

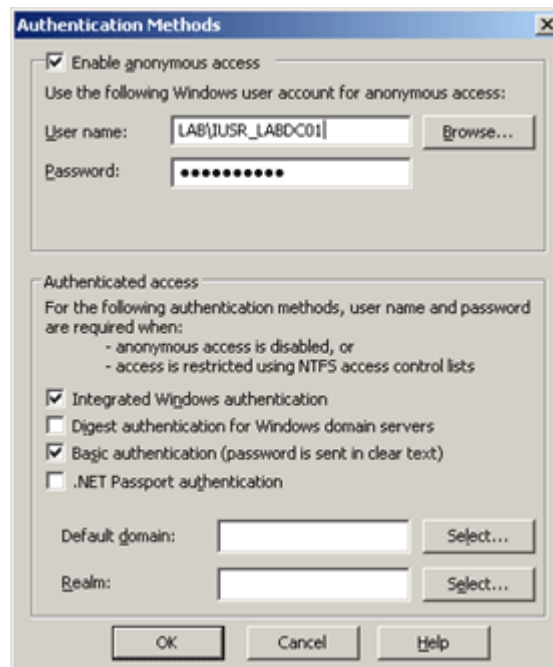
1. Start by opening the IIS Manager. Load IIS from the Administrative tools in the Control Panel by clicking **Start** → **Administrative Tools** → **IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).



2. Right-click on the Clavister InSight site and go to Properties.

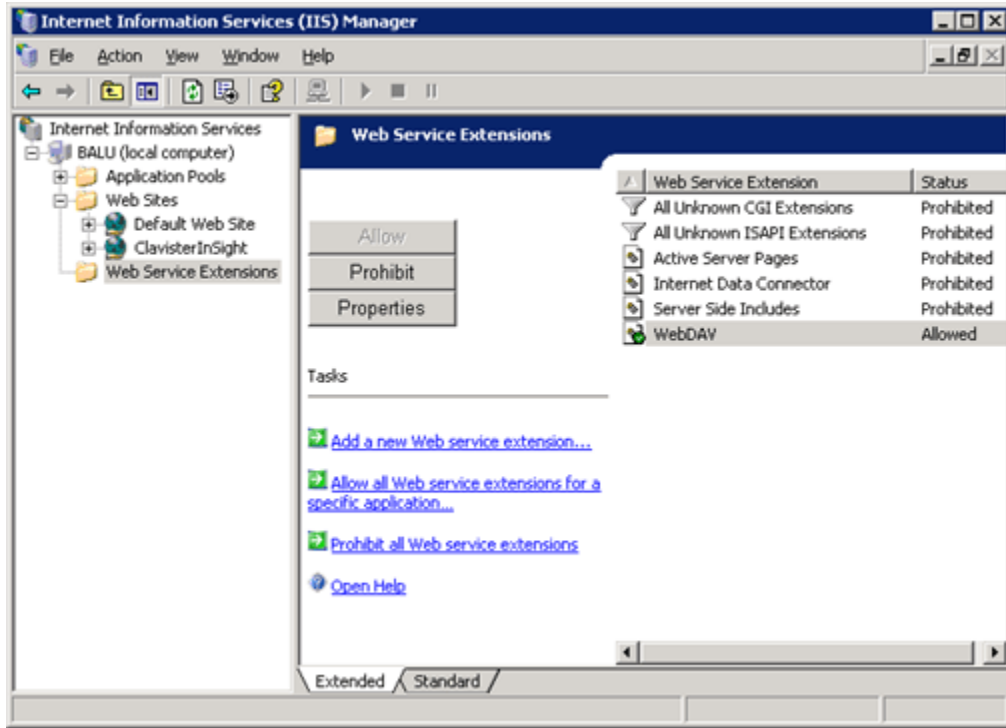


3. Click on **Directory Security**.
4. Click on **Edit** under Authentication and access control.

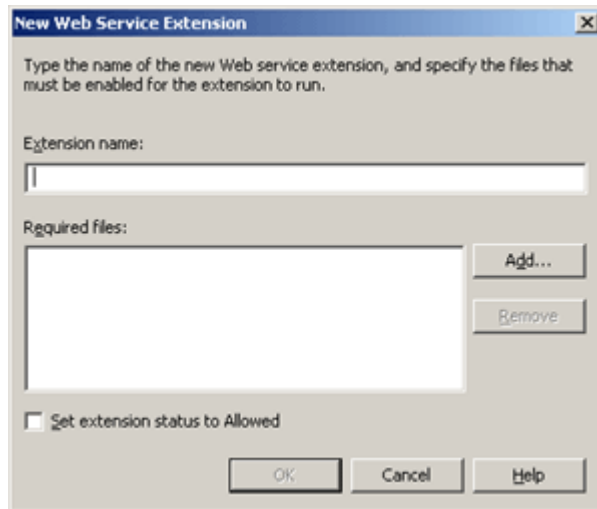


5. Use the IUSER_MACHINE account.

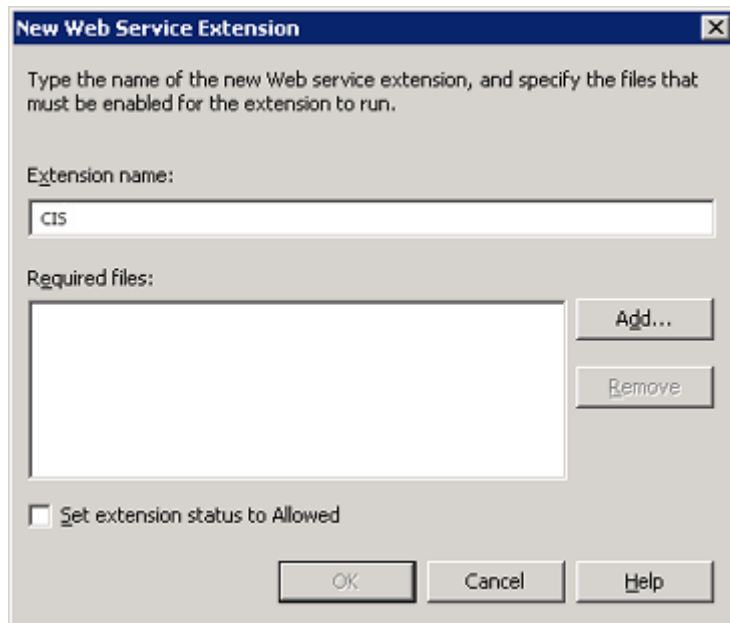
6. Click **OK**. The password for the IUSER_MACHINE account will automatically be populated after you have clicked "OK".
7. Click **OK** again.
8. Now please click on Web Service Extensions (found on the left hand-side menu).



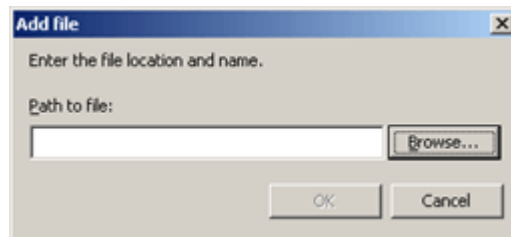
9. Choose **Add a new Web Service** extension.



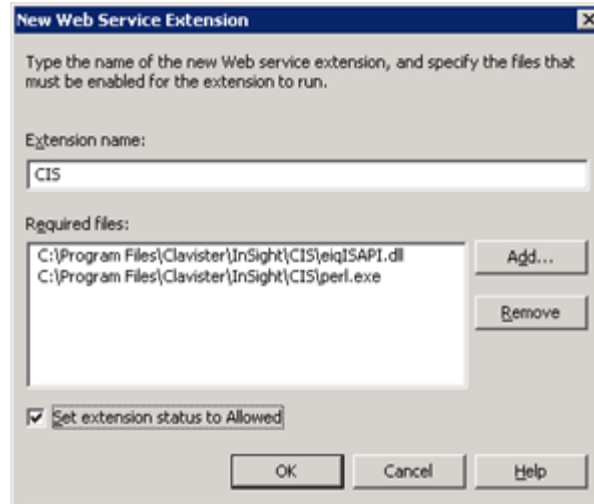
10. Name the web service extension **CIS**.



11. Click on **Add**.



12. Browse to: "C:\Program Files\Clavister\InSight\CIS\perl.exe" (please note this is the default path, if you did choose a different directory on install browse to that directory)
13. Click on **OK**.
14. Set the extension to Allowed.

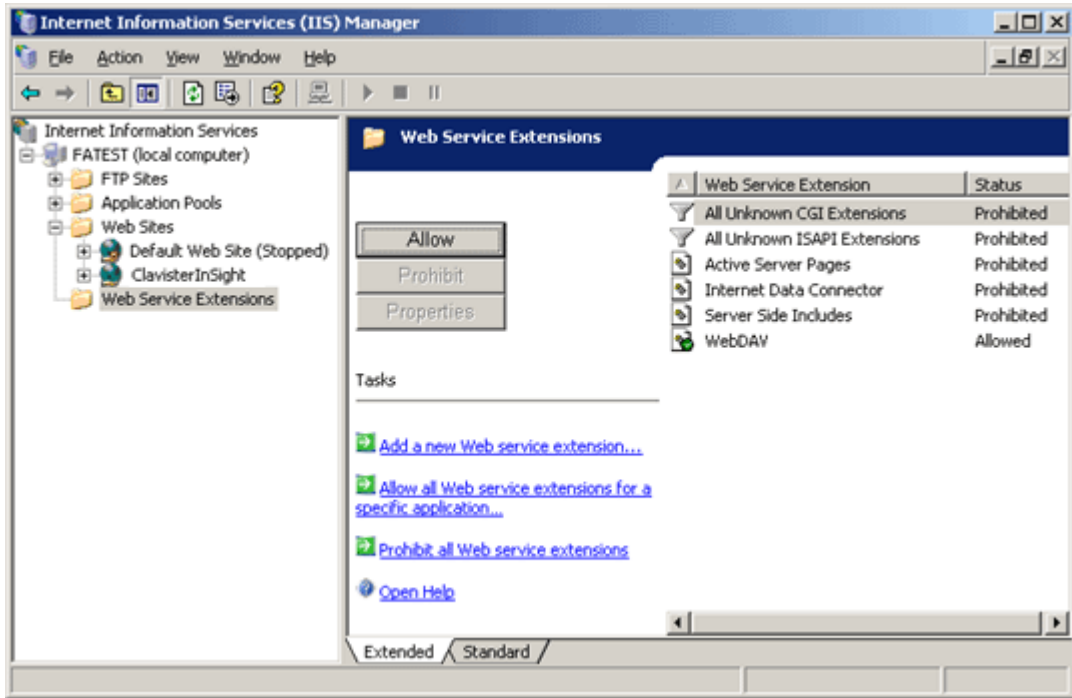


15. Click on **OK** again.
16. You have completed the setup steps for CIS in IIS and may now close out of the IIS Manager.

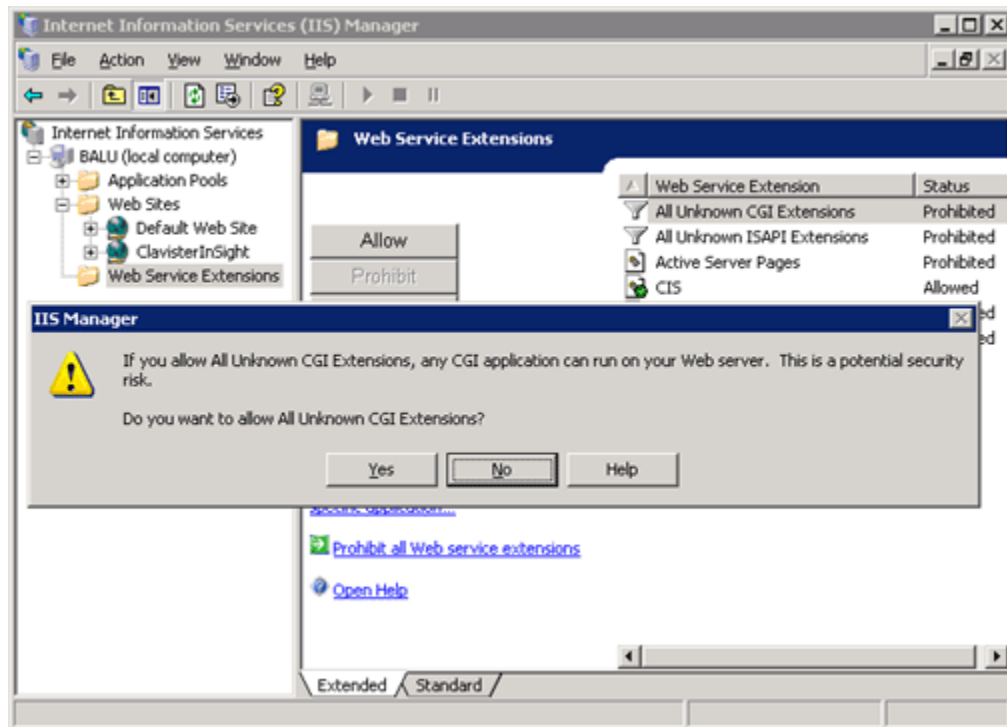
Configuring Windows 2003 To Allow CGI Extensions

By default IIS on Windows 2003 does not allow .cgi and .pl. IIS makes a call to perl.exe to run the code. If you associate .pl and .cgi in explorer to perl.exe by allowing all unknown CGI extensions, it will run it in a DOS window using perl.exe. IIS then makes a call to perl and displays the code produced.

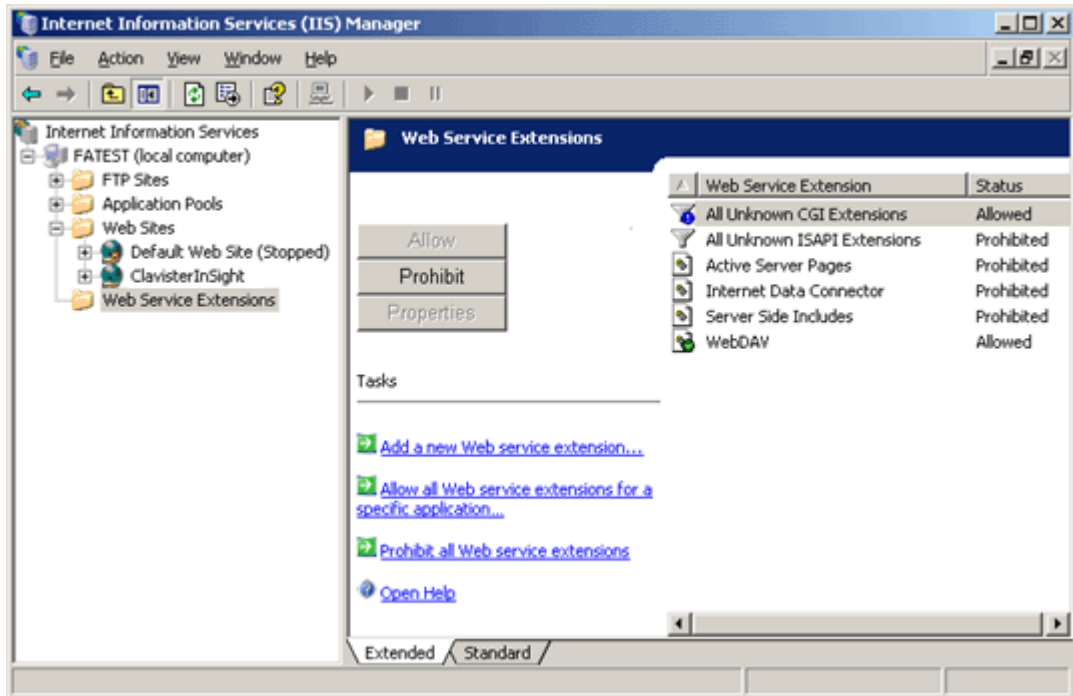
1. Load IIS from the Administrative tools in the Control Panel by clicking **Start → Administrative Tools → IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).



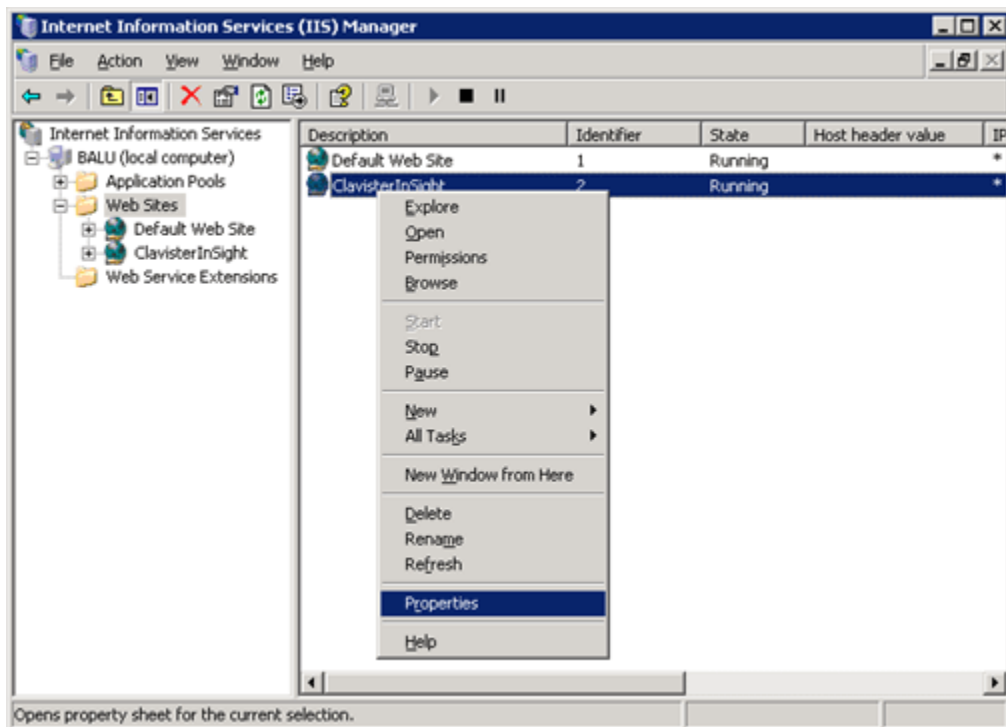
2. Click the name of your System then click **Web Service Extensions**.



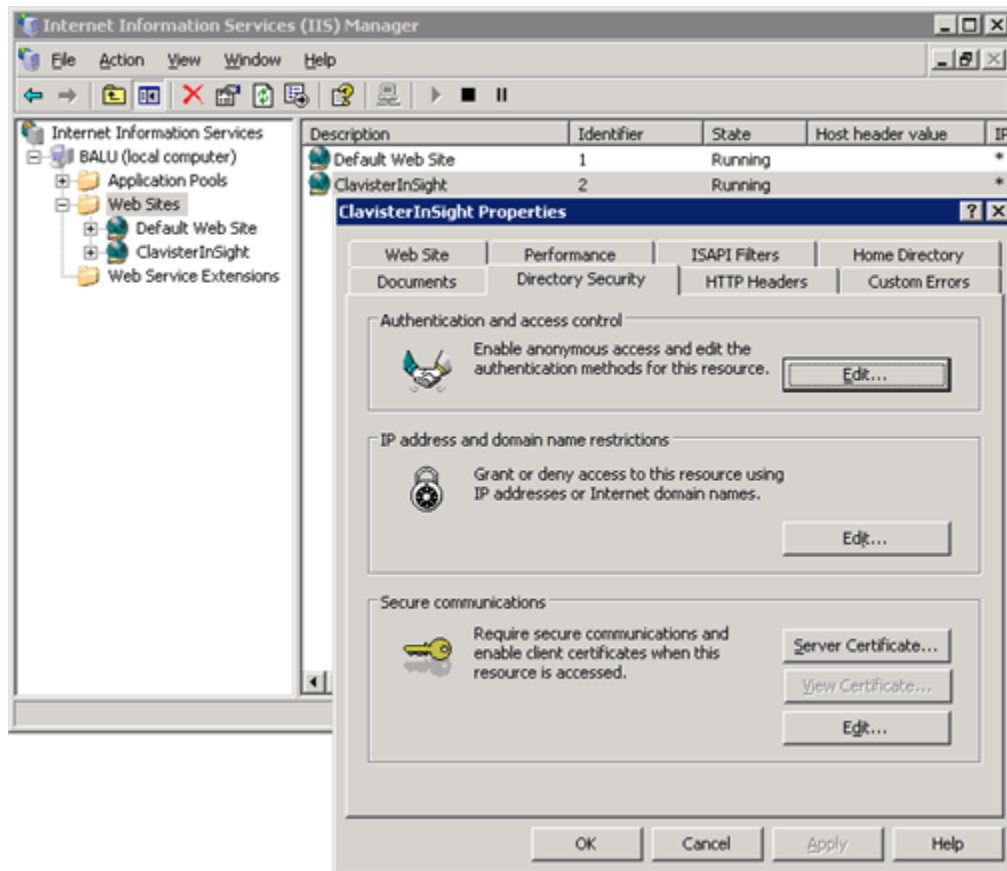
3. On the left side of the main frame under Web service extension column select the **All Unknown CGI extensions**, click **Allow**. Finally, click **Yes**.



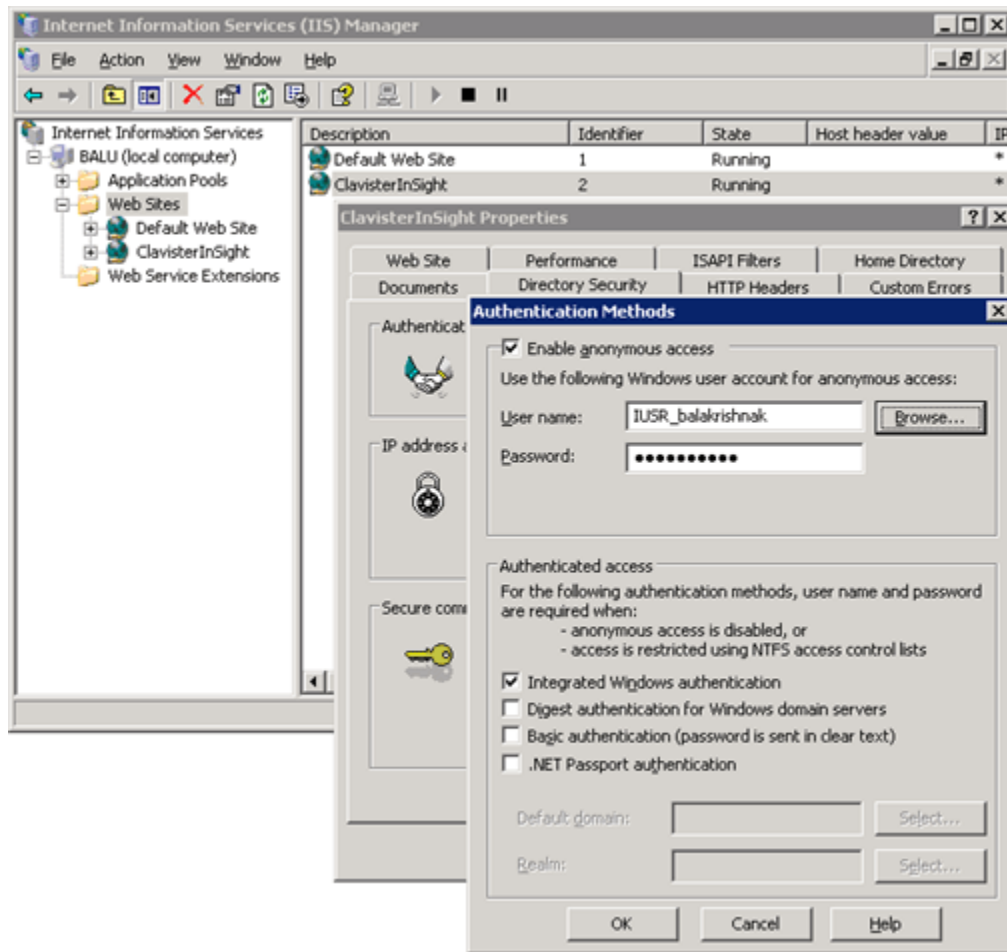
- Right-click on the Clavister InSight website in the right pane and select **Properties**.



5. Select **Directory Security** tab and click **Edit**.



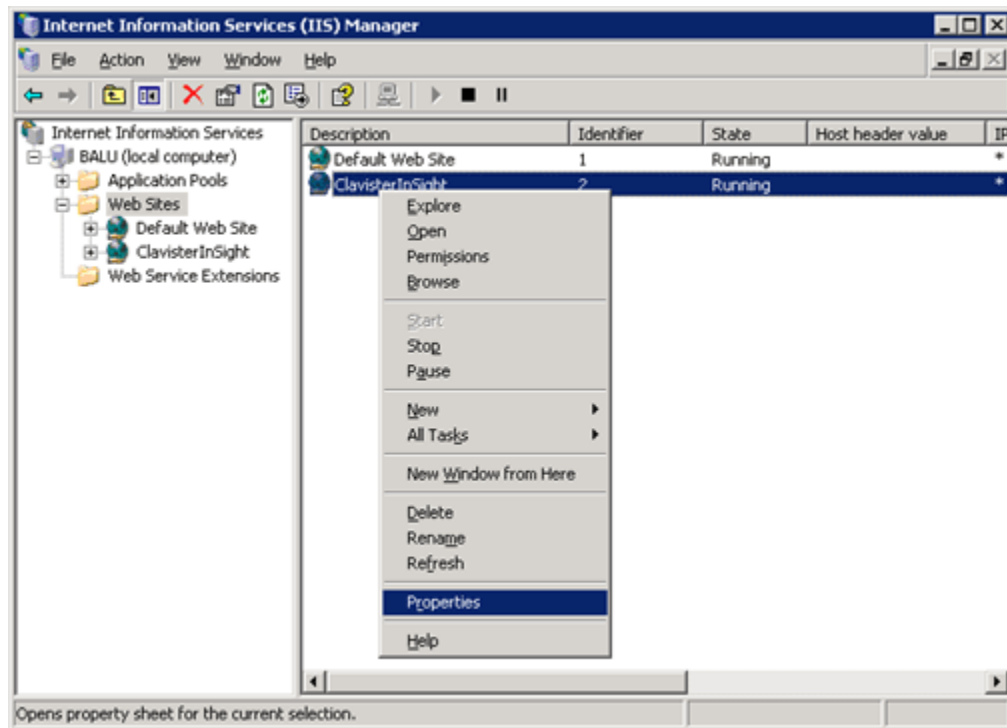
6. Enter IUSR account Username and Password details.



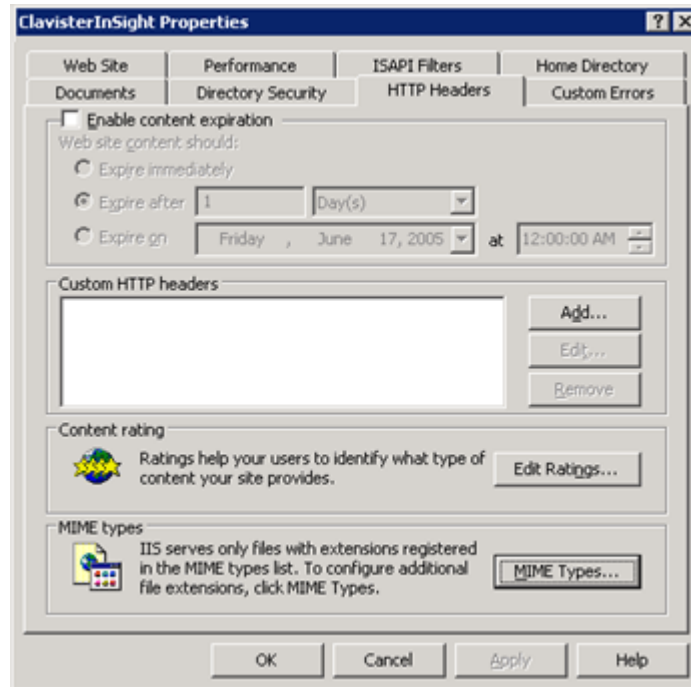
7. Click **OK** and re-enter the password to verify it.

Configuring MIME Type Extension for IIS on Windows 2003

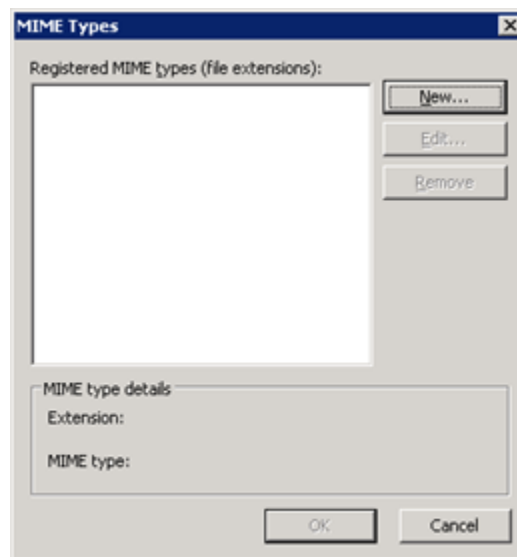
1. Load IIS from the Administrative tools in the Control Panel by clicking **Start → Administrative Tools → IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).



2. Right-click on the Clavister InSight website in the right pane and select **Properties**.

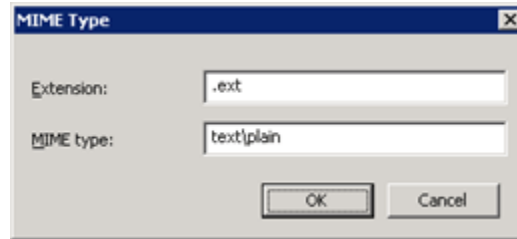


3. Select the **HTTP Headers** tab and click **MIME Types**. The MIME Types screen opens.

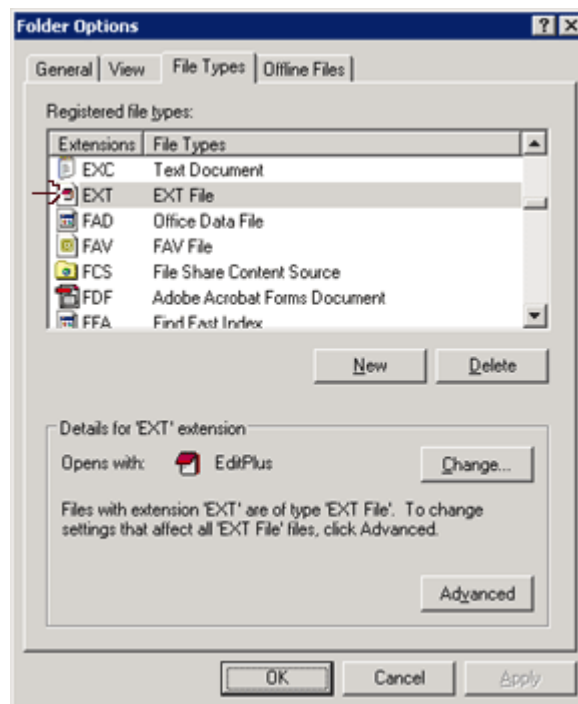


Note: IIS serves only files with extensions registered in the MIME Type list.

4. To add a new MIME Type extension, click the **New** button.



5. In the **Extension** box, type the file name extension as .ext.
6. In the **MIME type** box, enter a valid MIME type (text/plain).

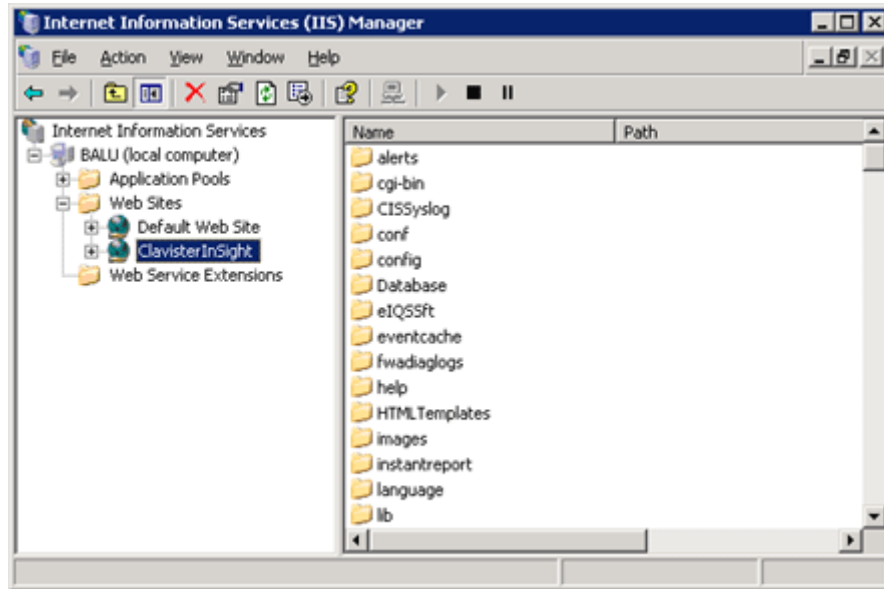


7. Click **OK**.

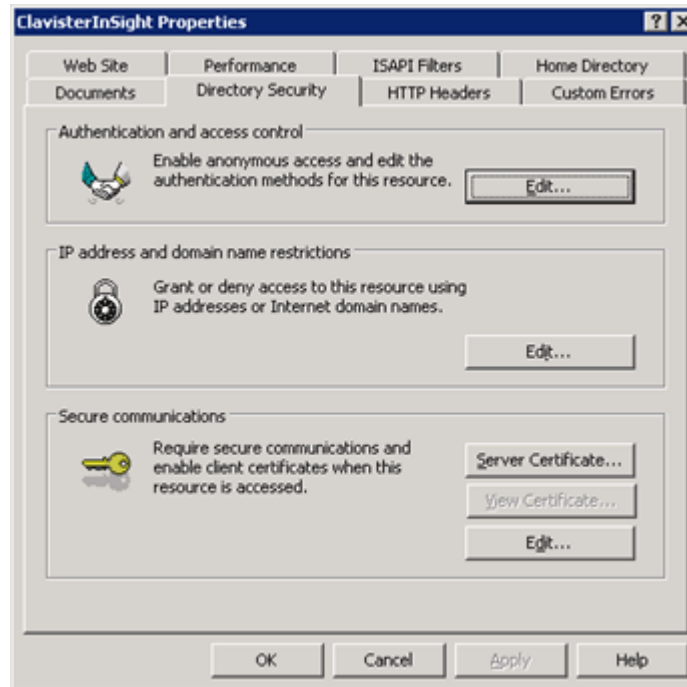
To check if the MIME type is added to the list of registered file types, open **Folder Options** → **File Types**. You can see that extension EXT is now a registered file type.

Adding IIS to use the IUSR Account

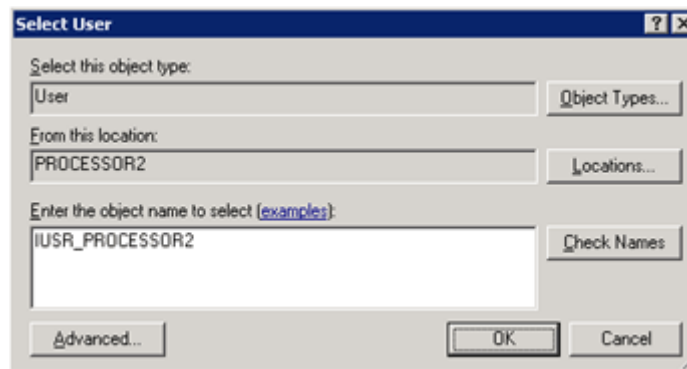
1. Load IIS from the Administrative tools in the Control Panel by clicking **Start → Administrative Tools → IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).



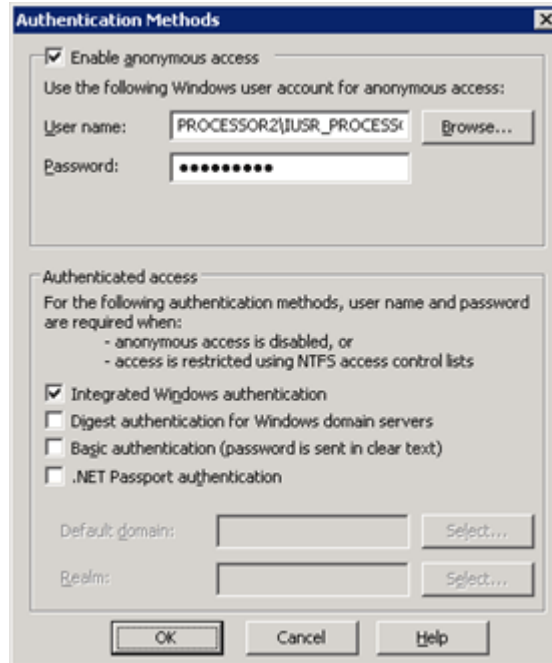
2. Right-click on the Clavister InSight website in the right pane and select **Properties**.



3. Click the Directory Security tab.
4. Click Edit under Authentication and access control.
5. The Authentication Methods window opens. Click the Browse button to select the IUSR user account present in the system.
6. Enter the IUSR object name to select and click OK.



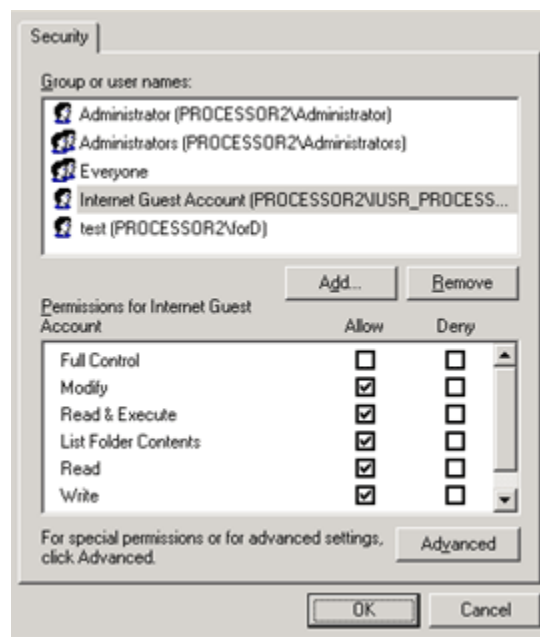
7. Click OK. The password for the IUSR_MACHINE account is automatically populated after you click OK.



Note: You will need to have a password for IUSR_MACHINE account because IIS on Windows 2003 server does not allow accounts without passwords. A password is required even for anonymous access.

Configuring the IUSR Account to have the necessary permissions

1. Load IIS from the Administrative tools in the Control Panel by clicking **Start → Administrative Tools → IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).
2. Right-click on the Clavister InSight website and go to Permissions.
3. Select the IUSR_ account and grant the following permissions: Modify, Read & Execute, List Folder Content, Read, and Write.



Configuring IIS to remove application mapping for .ext files

1. Load IIS from the Administrative tools in the Control Panel by clicking **Start → Administrative Tools → IIS Manager** (or loading the Control Panel, entering the Administrative Tools folder, and double clicking IIS Manager).
2. Panel, entering the Administrative Tools folder, and double clicking IIS Manager).
3. In IIS Manager, double-click the local computer, and then click the starting-point directory of the application you want.

4. Right-click on the Clavister InSight website in the right pane and then click **Properties**.
5. Click the appropriate tab: Home Directory, Virtual Directory, or Directory.
6. In the Application settings area, click Configuration, and then click the **Mappings** tab.
7. On the Mappings tab, click **Remove**.

Requests for files with this file name extension are no longer processed in this Web site or directory.

Enable ActiveX Controls and Plug-ins

When you try to download and install Macromedia Shockwave Player from the Macromedia Shockwave Player Download Center website, you may receive the following error message:

"Your Current Security Settings Prohibit Running ActiveX Controls on this Page".

This issue occurs if the Internet Explorer Enhanced Security Configuration feature is enabled. By default, the Internet Explorer Enhanced Security Configuration feature is enabled in Internet Explorer on Windows Server 2003-based computers.

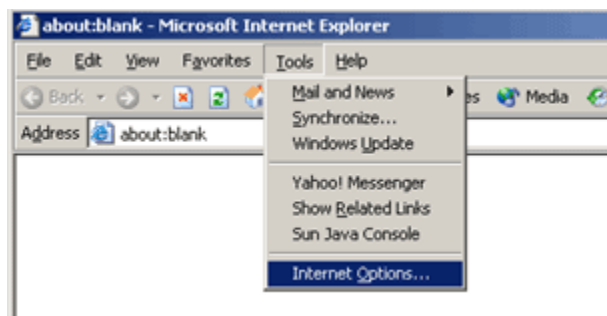
This enhanced level of security may prevent certain websites from displaying as expected in Internet Explorer. For example, programs that require the Web browser may not work as expected because scripts, ActiveX controls, and downloads are disabled.

To resolve this issue, add the following Macromedia websites to the Trusted sites zone in Internet Explorer:

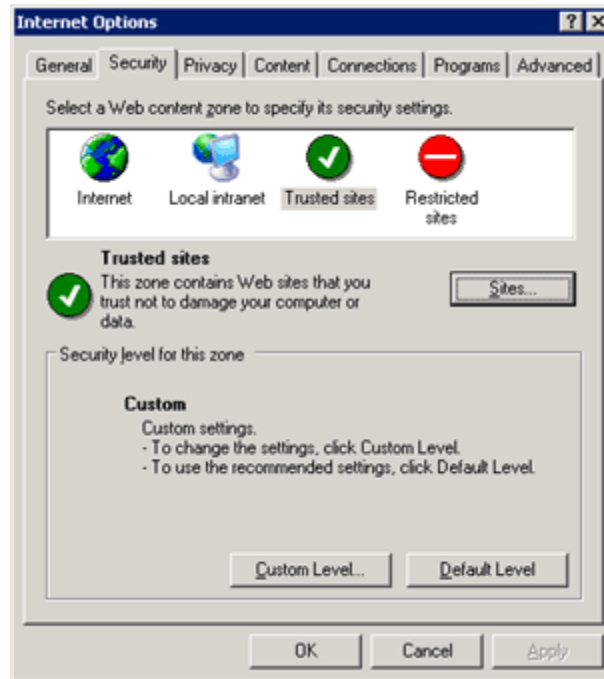
- ❖ <http://www.macromedia.com>
- ❖ <http://fpdownload.macromedia.com>
- ❖ <http://sdc.shockwave.com>

To do so, follow these steps:

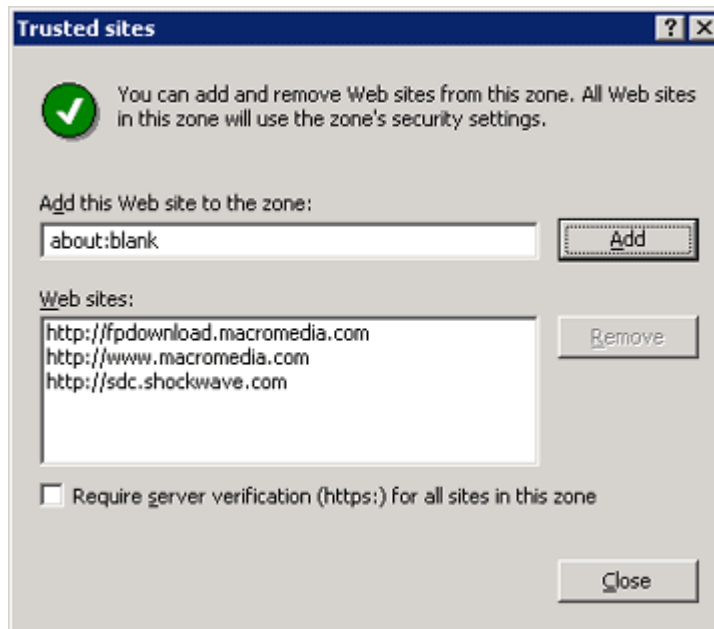
1. Start Internet Explorer (if it is not already running).
2. On the Tools menu, click Internet Options.



3. Click the Security tab.
4. Under Select a Web content zone to specify its security settings, click **Trusted sites**, and then click **Sites**.



- In the **Add this Web site to the zone** box, type `http://www.macromedia.com`, and then click **Add**.



- Similarly add the other two websites. The Macromedia websites are displayed in the Web sites list.
- Click **Close**, and then click **OK**.

Configuring IIS for accessing the application using Remote Desktop

To facilitate accessing the application using remote desktop connection, anonymous access should be provided with the credentials of a local user account having 'Administrator' privileges.

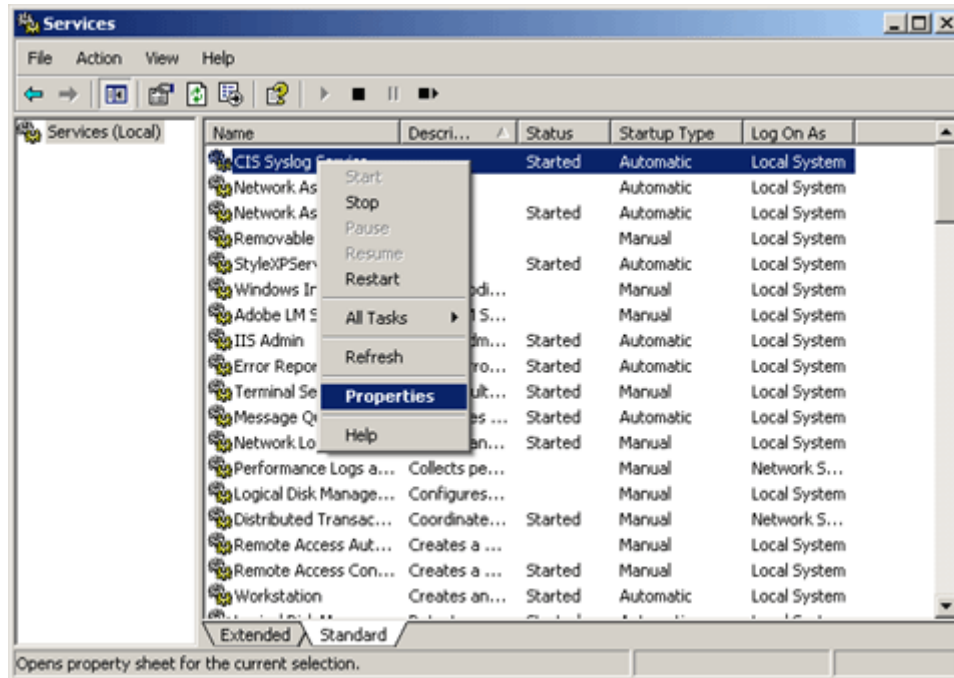
Follow the steps given below to provide anonymous access:

1. Load IIS from the Administrative tools in the Control Panel by clicking Start → Administrative Tools → IIS Manager.
2. Right-click on the website and select Properties.
3. Select the Directory Security tab.
4. Click the Edit button under Anonymous access and authentication control.
5. Authentication Methods window opens.
6. Provide the credentials of the local user account having administrator privileges.
7. Apply the settings and restart the website.

Appendix B

Administering Services Running on Services Window

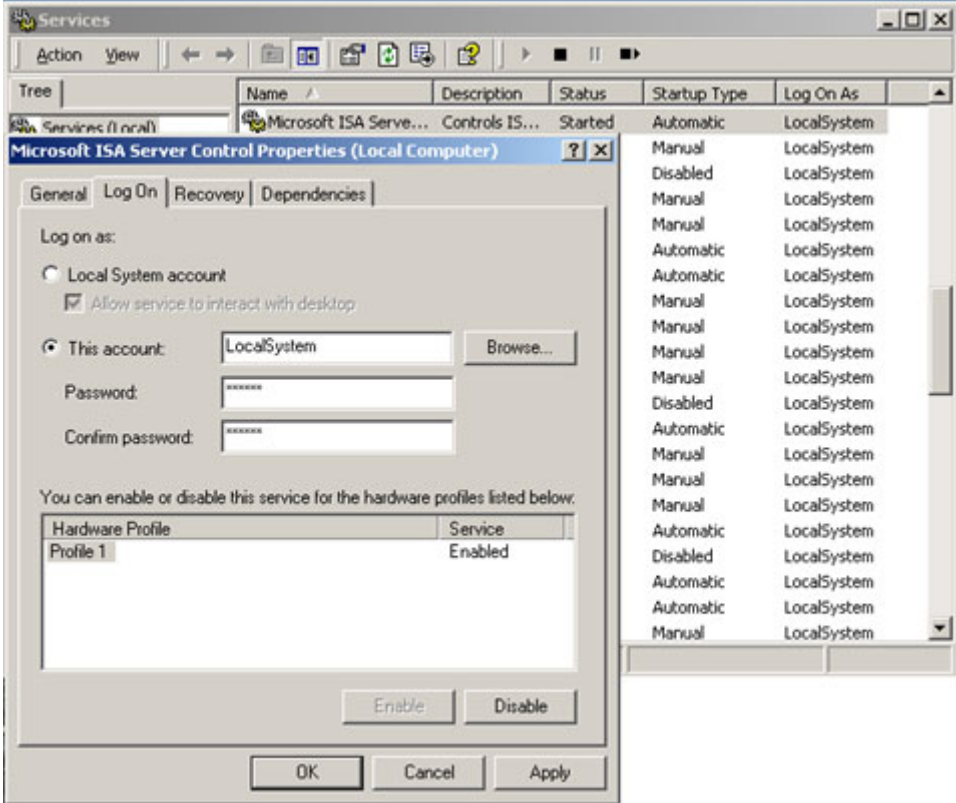
Go to Services in the Administrative Tools of the Control Panel and find the appropriate service for the firewall. For example, Right click on Clavister InSight Service and select **Properties**.



❖ Click **Properties**.

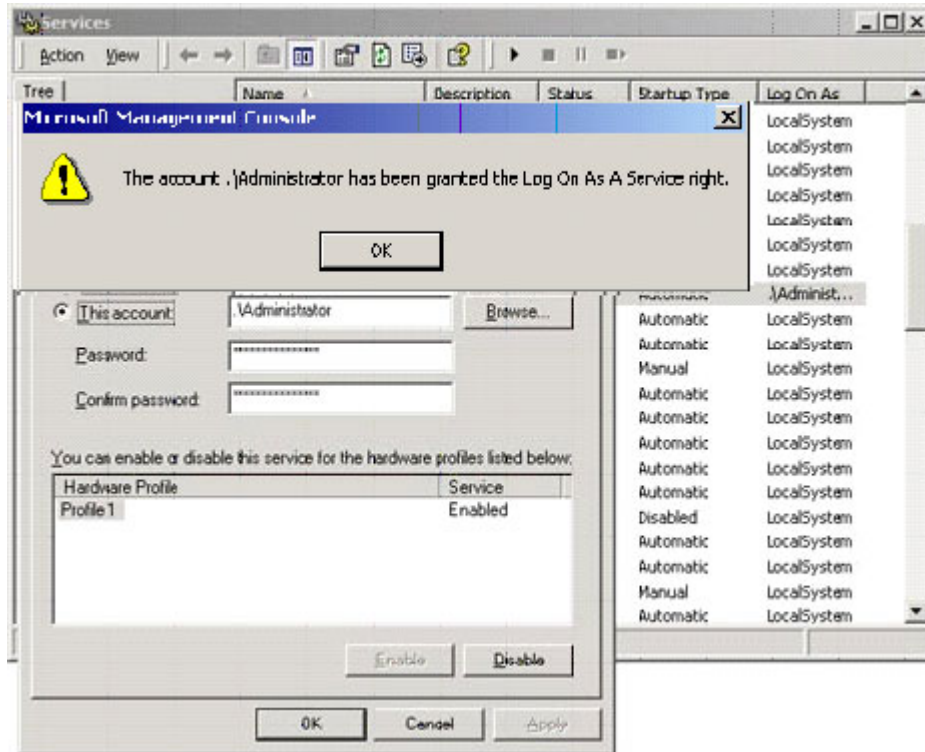
Properties Window

You will be prompted with a screen as shown below. Delete and retype the Username and Password of an account with administrative privileges within your messaging environment. Then click **Apply**.



Granting Privilege

A dialog box will pop-up telling you the account (Username you used with Administrative privileges) has been granted **Log On as a Service right**. Click **OK**. (See screen shot attached below)



Verifying Granted Privileges

You are now returned to a window like below. Click **OK** and then start the appropriate service. Also check to ensure that the service is set to automatically startup.

