



Administrators Guide Clavister InControl

Version 1.10.02

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com

Published 2010-04-07
Copyright © 2010 Clavister AB

**Administrators Guide
Clavister InControl
Version 1.10.02**

Published 2010-04-07

Copyright © 2010 Clavister AB

Copyright Notice

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without the written consent of Clavister.

Disclaimer

The information in this document is subject to change without notice. Clavister makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Clavister reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties of such revision or changes.

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL CLAVISTER OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE CLAVISTER PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF CLAVISTER IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, CLAVISTER WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. CLAVISTER WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT CLAVISTER RECEIVED FROM THE END-USER FOR THE PRODUCT.

Table of Contents

Preface	5
1. InControl Overview	7
2. Installing InControl	10
3. The Client Interface	16
4. Server Management	20
5. Adding Security Gateways	24
6. Revision Management	31
7. A First Security Policy	37
8. Licensing	44
9. Alarms	50
10. The Audit Trail	54
11. Creating Domains	55
12. User Accounts and Groups	57
13. Remote Console	62
14. Real-time Monitoring	64
15. Log Monitoring	76
16. High Availability	78
17. The Log Query Server	82
18. Remote Management	88
19. Certificate Requests	91
20. Importing FineTune Datasources	95
21. Troubleshooting Connections	99
A. NetCon Key Generation	101
B. Keyboard Shortcuts	104
C. LQL Reference	105
InControl Glossary	110
Alphabetical Index	112

List of Examples

C.1. Using Logical Operators	105
C.2. Using Comparison Operators	106

Preface

Target Audience

The target audience for this publication is the administrator of a security gateway running the CorePlus operating system. The system may be running on Clavister hardware or non-Clavister hardware and is to be administered from a management workstation running the Clavister InControl software.

Text Structure

The text is divided into chapters and subsections. Numbered subsections are shown in the table of contents at the beginning of the document.

Text links

Where a "See section" link is provided in the main text, this can be clicked on to take the reader directly to that reference for example, "see Chapter 2, *Installing InControl*".

Web links

Web links included in the document are clickable, for example <http://www.clavister.com>.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:



Note

This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasised or something that is not obvious or explicitly stated in the preceding text.



Caution

This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.



Important

This is an essential point that the reader should read and understand.



Warning

This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Trademarks

Certain names in this publication are the trademarks of their respective owners.

CorePlus is the trademark of Clavister AB.

Windows, Windows XP, Windows Vista and *Windows 7* are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

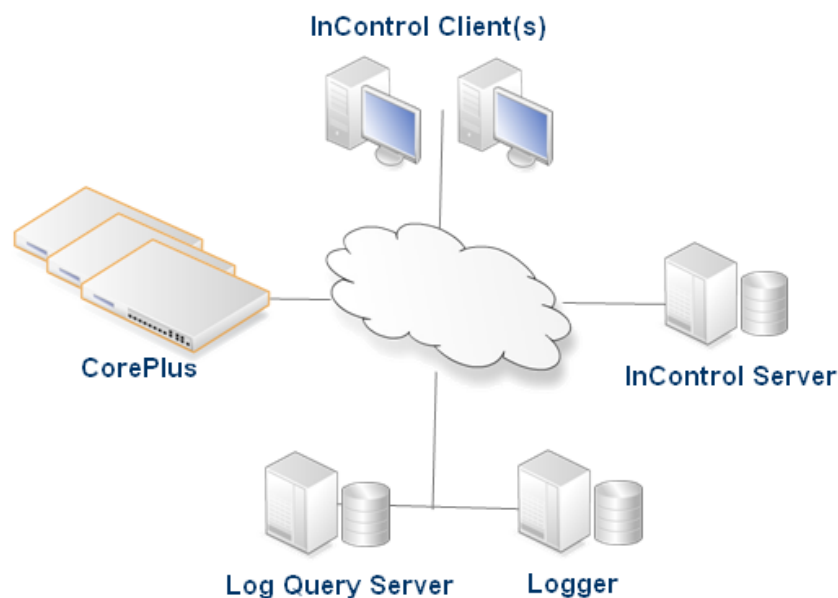
Chapter 1: InControl Overview

Introduction

Clavister InControl is a software product for the monitoring and centralized administration of one or multiple Clavister Security Gateways. The product provides an intuitive graphical client which runs on a standard Windows based PC under Windows XP or later version. This PC will sometimes be referred to in this document as the *client workstation*.

The Client/Server Architecture

InControl consists of two parts: the InControl client and the InControl server. One or multiple InControl client workstations communicate with an *InControl server* which runs as a Windows service on the same or different computer.



The server acts as a repository for all CorePlus configuration data and mediates all management communication between clients and Clavister Security Gateways. The diagram below illustrates a possible deployment of InControl with various software components distributed on separate servers connected by the Internet.

Key Tasks Performed by InControl

The following key tasks can be performed for a Clavister Security Gateway by InControl clients:

- Controlling CorePlus management communication.
- Creating, modifying and removing CorePlus objects and security policies.
- CorePlus configuration version control.
- CorePlus license management.
- CorePlus status and performance monitoring.

Uploading Multiple Configurations

An important benefit of using InControl is the ability to upload common configuration elements to large numbers of Clavister Security Gateways in a single operation. This feature is vital to reducing the complexity of managing large numbers of Clavister Security Gateways in a complex network topology and is a key reason for using InControl instead of the web interface built into CorePlus.

Comparison with the Web Interface

InControl can perform all the functions of the web interface plus many more. In many cases the web interface look and feel is duplicated in InControl as is the way configuration information is displayed. This duplication, however, forms only a subset of InControl's complete feature set.

The most important difference with the Web Interface is that a single Web Interface browser window can be used to manage one Clavister Security Gateway at a time. The Web Interface does not therefore provide the ability to share configuration objects between security gateways and define objects that are common to a number of gateways.

Various other features are also not provided by the Web Interface and include InControl's version control.

Restricting Management Privileges

Not all InControl clients need to have the same management privileges. A single, primary administrator with the username *admin* that has, by default, full administrative privileges. Other administrator user accounts can be created that have varying degrees of lesser access privileges. A new client account may be defined, for example, that is allowed to only perform real-time monitoring tasks.

The InControl SDK

InControl provides the option to write third party applications which take over the role of the standard Clavister InControl client and provide customized functionality. This is done using the *InControl SDK*. The SDK provides an *Application Programming Interface (API)* that allows source code to directly access the functions of the InControl server and to manage the security gateways connected to the server.

This manual does not discuss the SDK further. More information on this topic can be found at <http://www.clavister.com> and the separate *InControl SDK Guide* describes this product in depth. The API is based on the *Windows Communication Foundation (WCF)* interface which allows code

development to be done with a variety of languages and platforms.

Chapter 2: Installing InControl

This section describes the installation of InControl for the first time.

InControl Installation Files

The complete set of InControl installation files can be found on the CorePlus CD-ROM delivered to customers. Alternatively, it can be downloaded directly from the Clavister *Customer Web*.

These installation executable (.exe) files consist of one executable for the InControl client installation and a separate executable for the InControl server installation.

Installation of the InControl client and server should be on either the same Microsoft Windows based PC or different PCs. These two installations will also be referred to in this manual as the *client workstation* and the *server computer*. When installing InControl for the first time it is recommended that the simplest installation is performed which is the client and server installed on the same computer.

CorePlus Versions

InControl can only be used for management of Clavister Security Gateways running CorePlus version **9.10.03 or later**.

An error message will appear when trying to add a new security gateway to InControl if the gateway is running an earlier version of CorePlus that is incompatible. Upgrading CorePlus to a compatible version will solve this problem.

The Minimum Configuration

The minimum hardware configuration for both the client and the server hardware is as follows:

- Microsoft Windows XP or later.
- 1 Gigabyte of RAM.
- 100 Mbytes free hard disk space.
- **BOTH THE INCONTROL CLIENT AND SERVER PC SHOULD HAVE PUBLIC INTERNET ACCESS DURING INSTALLATION.**

Windows Administrator Privileges Are Required

When installing InControl, you must be a user which is a member of the Windows *Administrator* group.

Furthermore, all InControl clients must be running under Microsoft Windows as a user which is a member of the Windows *Administrator* group. If a user is a member of a group with lesser privileges, such as *Power Users*, then InControl will start correctly but security gateway management will not function.

Workstation to Gateway Connection

The server workstation must have access to the Clavister Security Gateways to be managed by either being connected to same Ethernet network or being connected remotely across other networks such as the Internet. Similarly, the client workstation needs network access to the server workstation if they are different.

Installation Hardware Should Have Internet Access

As stated in the installation requirement list above, the server and client PCs **SHOULD HAVE PUBLIC INTERNET ACCESS**. This is to allow validation of digital certificates used by the installer. If Internet access is not available, **installation time can extend to around 30 minutes** because of the installer's attempts to access the relevant CA server.

Required .NET Versions

InControl relies on the Microsoft *.NET* framework to run and the installed *.NET* version must be at least 3.5 for the InControl client to run and at least 2.0 for the InControl server to run. Version 3.5 of *.NET* includes version 2.0 so if 3.5 is installed then both client and server can run.

When the InControl installers are run for client and server, the required *.NET* installation can be done automatically so *.NET* need not be installed separately.

Installing InControl

Installation of InControl is performed in two steps:

1. Install the InControl server
2. Install the InControl client



Tip: Installer Error 1158

*With too many other processes running the InControl installer can occasionally produce a general error condition with the error number **1158** before halting.*

This is usually caused by a lack of available memory and is resolved by closing some of the currently running processes.

If the error persists, restart Windows in order to free up the required memory.

Using the Same Workstation

The client and server can be on the same workstation or on different workstations. For first time installation, it is recommended that the same workstation is used and subsequent client installations are done on different workstations.

This order of installation indicated above (server then client) is recommended so that the client on the same workstation can make contact with the running server as soon as it starts.

Server Installation

The server is installed by double clicking the *setup.exe* file in the *InControl Server* folder of the installation packet. An installation wizard for setup will then run.

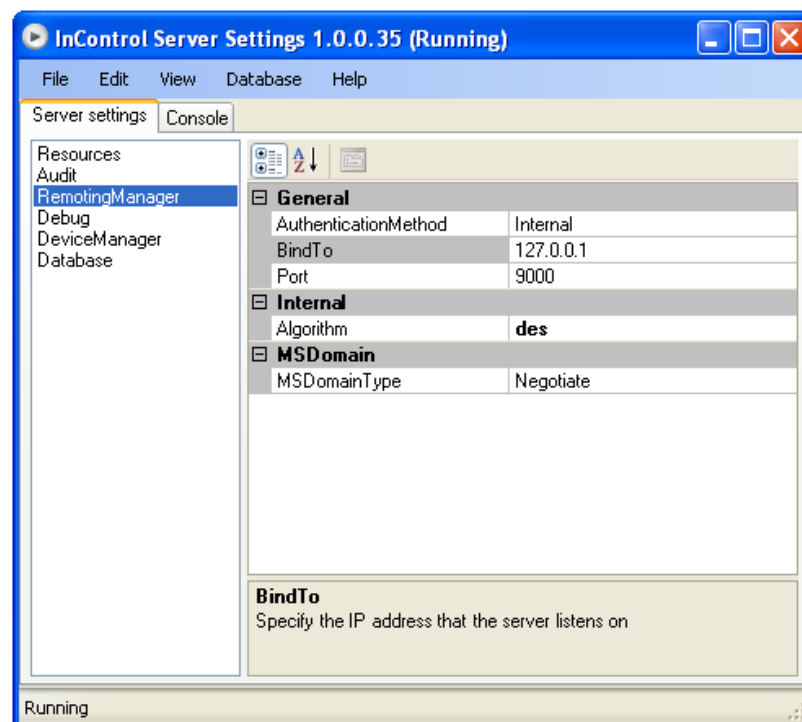


Note: .NET 2.0 is required by the server

The server requires at least .NET version 2.0 to be installed and the installer provides the option to install .NET 2.0 as part of the server installation process.

The server wizard also, by default, installs the Clavister *Log Query Server* (LQS). However, it is possible to tell the wizard to not install the LQS.

The server installation steps consist of standard installation questions and on completion the InControl server will be left running and the server control interface will be displayed, as shown below.



Even if this server interface is closed, the server will continue to run as a Windows service. The server interface will re-appear if the InControl server option is chosen in the Windows start menu.

Three Windows services are installed with the server installation. These appear as shown below when the running system processes are displayed in Windows.

ICS.exe	00	SYSTEM
logger.exe	00	SYSTEM
lqs.exe	00	SYSTEM

When the client is running, the process *ICC.exe* will also appear in the process list.

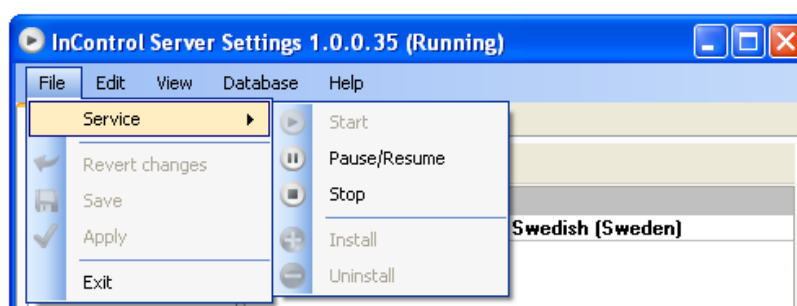


Important: Restrict access to the server hardware

Access to the InControl server user interface is not protected by any security mechanisms. Physical access to the PC on which the server is running also means access to the server interface. It is therefore important to restrict physical access to this computer, preferably by locating it in a secure computer room.

Changing the Server Status

Changing the running status of the server is done by going to the **File > Service** menu in the server interface.



Client Installation

The client is installed by double clicking the *setup.exe* file in the *InControl Client* folder of the installation packet. An installation wizard for setup will then run.

The client installation steps consist of standard installation questions and on completion the complete product is ready to be run. As mentioned previously, the client requires at least .NET version 3.5 to be installed and the installer provides the option to install .NET 3.5 as part of the client installation process.

Start Menu Entries

Following installation, the Windows **Start** menu will contain entries for starting both client and server. The server should be started before starting the client.



Initial Login

When the client is started a username and password will be asked for. The factory defaults for these are **admin** and **admin**. This gives access to the main administration account which has unlimited permissions for changing configuration data and examining system information.

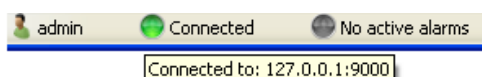
After successfully logging in, the full client interface will be displayed.

Client to Server Connection

When the InControl client is running on the same computer as the InControl server, the client will automatically find and connect with the server. The server should automatically always be running as a process called *ICS.exe* even after computer restarts. At the bottom of the client interface is a connection status icon which is green if server connection has been successful:



If the mouse is moved over the green connection icon, a tooltip appears which shows the IP address (in this case the loopback address) and the port number to which the client has connected:



If connection to the InControl server was unsuccessful then this icon will be red:



If the server appears to be not responding then go into the Windows **Start** menu and select the InControl server option from the Clavister submenu. The InControl server management interface will appear. Now explicitly start the server by choosing the *Start* option from the *File > Service* submenu. The client service status icon should now turn green after one or two seconds.

Upgrading from 8.nn CorePlus

In a situation where a user is upgrading from a CorePlus version 8.nn system, the older FineTune management client can no longer be used with 9.nn versions. From CorePlus version 9.10 onwards, CorePlus can be administered through either the Web Interface, CLI or InControl.

Upgrading from 8.nn can be done in one of two ways:

1. Running the *upgrade.exe* program which is included with the CorePlus distribution package. This executes a special, standalone upgrade wizard.

This wizard is discussed in detail in the separate manual called the *8.nn to 9.nn Migration Guide*.

2. Running the upgrade wizard contained within InControl after the FineTune *Datasources* are first imported into InControl.

This option is discussed in detail later in *Chapter 20, Importing FineTune Datasources*.

Upgrading InControl

From time to time, new releases of InControl will be made available. These can be downloaded from the Clavister *Customer Web* and will be packaged like the original installation as two *.exe* files, one for the client and one for the server. Both should be installed over an existing installation, the server first and then the client.



Important: The client and server should be upgraded together

Although InControl releases include separate installation executables for the upgrade of the client and the server, they should be viewed as a single upgrade. One **should not** be

upgraded without the other since there may exist dependencies between the two.

Before installing, both the client and server user interfaces should be closed. The server installation will automatically stop the relevant service, restart the computer and restart the service with the new version of *ICS.exe*. Any client activity should be suspended during the server upgrade.

The InControl server database is not normally affected by upgrading. Indeed, a complete uninstall of the server will leave the database intact and remaining files must be deleted from the installation directory manually to completely remove the database. In certain, isolated instances the installer may upgrade the database to a new format.

Downgrading CorePlus

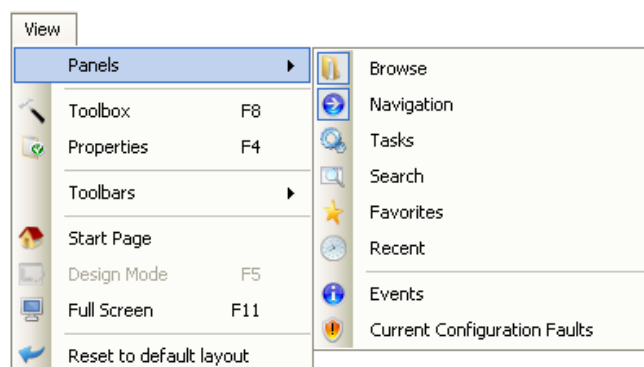
If a security gateway downgrade back to a CorePlus 8.nn system is required, reversing an upgrade, this cannot be done through InControl. Such a downgrade must be done with the standalone *upgrade.exe* program supplied with the Clavister release packages. Despite this executable's name, one of the options that can be chosen from its interface is downgrading.

When the downgrade process is complete, the configuration will have reverted to the one that existed before the upgrade and FineTune can then be used again to administer the security gateway. All configuration changes made with InControl will be lost.

Chapter 3: The Client Interface

The Client User Interface Layout

The main window for editing configurations is divided into a number of panels. A list of these panels can be found in the **View > Panels** menu option.



Not all panels are visible at once but the interface provides tabs to quickly make them visible. In the initial, default display, the left panel consists of a tree providing a complete overview of all the Clavister Security Gateways that can be managed with the different subsets of CorePlus objects. The central panel displays information related to the currently selected object type.

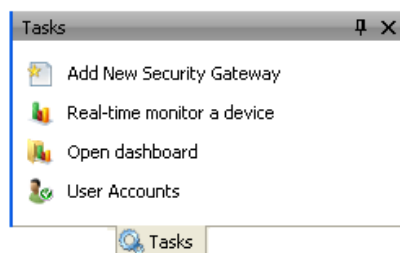
Opening Tabs

When selected, some functions, such as the *License Center* and *Audit Trail* are opened in a new *Tab* in the central area of the user interface. Each tab can be left open, selected or closed as desired.



The Tasks Panel

A special panel called *Tasks* can be opened and this panel provides a shortcut to important functions associated with the currently selected tab. For example, if the *Start Page* panel is open the following will appear in the *Tasks* panel.



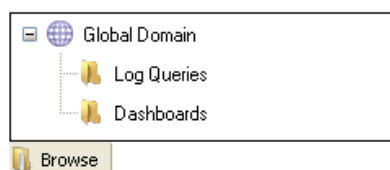
For certain tabs, an extra option will be added in the menubar which lists the same options available in the *Tasks* panel. For example, the *Start Page* tab has an *Object* menu associated with it that appears in the menubar when the tab is selected. This menu is shown below.



If no tab is open then the *Tasks* panel will be empty if it is displayed.

The Browse Panel

The most important panel in the client interface is the *Browse* panel which contains a navigation tree that displays all the *Domains* and *Security Gateways* defined in InControl. After starting InControl for the first time, the *Browse* panel will appear as shown below.



There are a number of important node types that can appear in this tree. These are:

- **Domains**

A *Domain* is a configurable container that can contain many Clavister Security Gateways. The top-level *Global Domain* node in the navigation tree above is an example of a Domain and exists by default.

The purpose of a domain is to share aspects of configuration between multiple Clavister Security Gateways. Objects that exist within a domain can be used by any security gateway within that domain. For instance, all the objects that exist in the default, top-level *Global Domain* can be used by all gateways since everything is contained within this domain.

By double clicking on a domain node, the navigation tree for the domain's objects will open in a new central tab and the tab's name will be the domain's name. The objects types within a domain are a subset of the full object set that are found in a security gateway node.

Domains are more fully explained in Chapter 11, *Creating Domains*.

- **Security Gateways**

A *Security Gateway* node represents an installed Clavister Security Gateway. These may be collected together in a domain so that they can make use of common objects defined within the domain. All security gateways and domains have access to the objects defined in the

Global Domain.

By double clicking on a gateway node, a navigation tree for the gateway's objects will open in a new central tab and the tab's name will be the gateway's name.

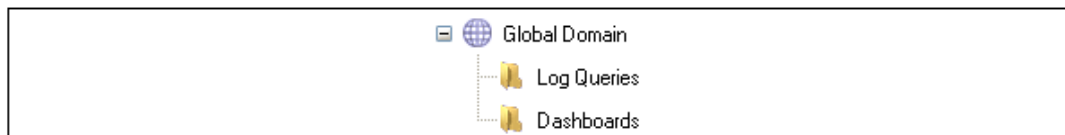
Defining new security gateways is described in Chapter 5, *Adding Security Gateways*.

- **High Availability Clusters**

A *Cluster* node in the *Browse* navigation tree combines two Clavister Security Gateways into a single *High Availability* cluster. The operation of clusters is explained in detail in the separate *CorePlus Administrators Guide*.

The Global Domain

Before any Clavister Security Gateways are defined, the main navigation tree in the *Browse* panel contains only the *Global Domain* node as shown below.

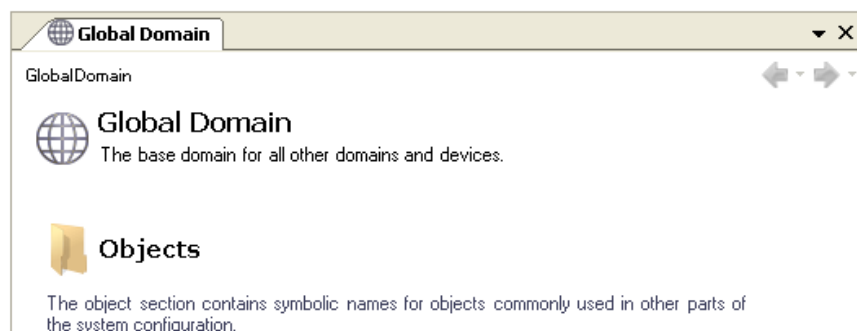


The absence of an icon next to this node indicates that this domain is currently checked in and is available for editing. When the domain is checked out for editing (and therefore locked from editing by other clients), a red dot appears next to it as shown below:



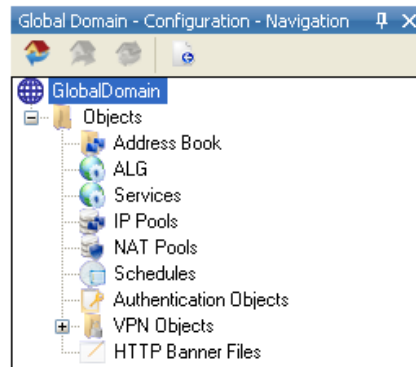
Viewing Objects

By double clicking the Global Domain in the main navigation tree, a navigation tab will open in the central interface panel which shows the various CorePlus objects associated with the Global Domain.



We can now navigate through this domain's objects by clicking on the object types. Notice that in the top right of the tab we have forward and back arrow buttons. These allow us to return to previous views of the domain's objects in the same way that an Internet browser works.

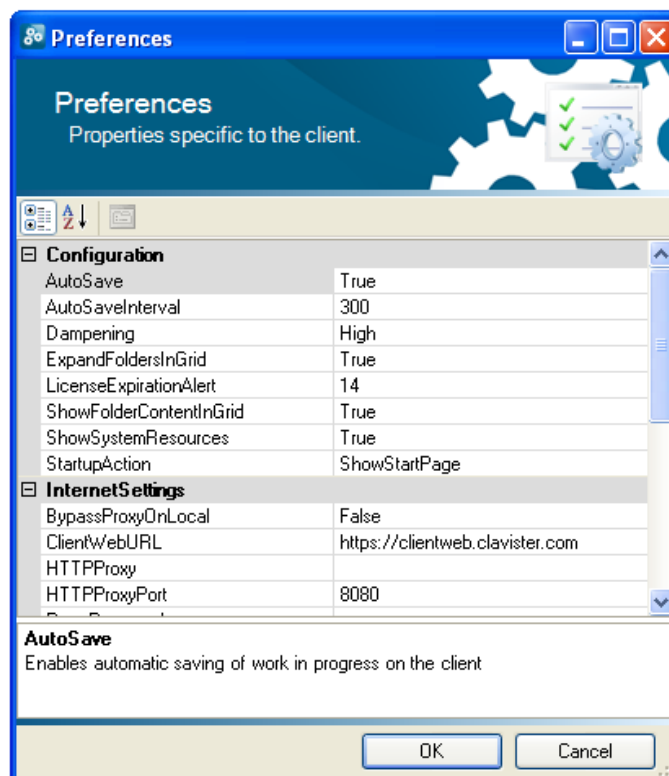
An alternative navigation tree for the objects also opens in a separate *Navigation* panel.



This navigation tree provides an alternative means to reach different objects.

Client Preferences

By choosing the menu option **Edit > Preferences**, the client preferences dialog will appear, allowing a number of general preferences for the client to be changed.



The AutoSave Function

The *Autosave* function in the client preferences dialog provides a way to routinely save any changes made to data in the client to the local disk. Saving means that any work done, for instance, on a checked out configuration is retained even though the client may be closed and then restarted later. If a configuration is checked out then the checked out status will remain between client sessions provided that a save to disk has been performed of the client's status.

If AutoSave is enabled with the *True* setting, the *AutoSaveInterval* value specifies the time between saves.

Chapter 4: Server Management

The InControl server interface provides a number of options for management of the server. These are discussed in this section.

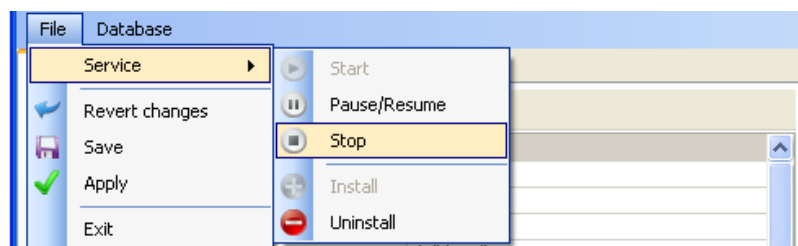
Displaying the Server User Interface

The InControl server runs as a Windows service and appears in the Windows process list as *ICS.exe*. It will be started automatically after initial installation and after hardware restart and will only be stopped by choosing the menu option in the server user interface (or stopping it through the Windows process manager).

Starting the *InControl Server* from the Windows start menu does not affect the running *ICS.exe* if it is already started but just causes the user interface for the server appear. If the *ICS.exe* process is not running then displaying the user interface will have the dual effect of also starting the server service.

Stopping and Pausing the Server

Closing the server user interface will also not affect *ICS.exe*. If the service needs to be stopped then it is recommended that this is done with the **Service > Stop** option in the user interface.



The server may also be paused with the **Pause/Resume** menu option. This option translates directly into a windows service pause. In this state, no updates are performed on the database and it is therefore useful if a backup of the database is to be done using a normal Windows utility instead of through the server user interface. The same menu option can then be selected to resume the server after a pause.

During a database backup initiated through the server user interface (described further below) the server process is automatically paused.

Setting the Audit Level

The *Audit Level* determines which server audit messages are saved to disk as a log. These messages are generated by various server events such as shutdown and startup and are saved in a folder in the server installation directory for analysis through the InControl client. Only server messages that are at or above the set audit level priority will be logged and this level can be different from the general audit level described above.

It's important to remember that the server log messages being discussed here are totally separate from the log messages generated by CorePlus and relate only to server activity, not the activity of connected Clavister Security Gateways.

The server audit files can be viewed with a text editor but should not be edited in any way. Their format needs to be preserved otherwise they cannot be viewed through the InControl client.

Configuring a Syslog Server

By setting the value of the **Syslog** parameter to *True*, server log messages can also be sent to an external Syslog server. The Syslog server's IP address needs to be specified, as well as the desired level of the messages that are sent.

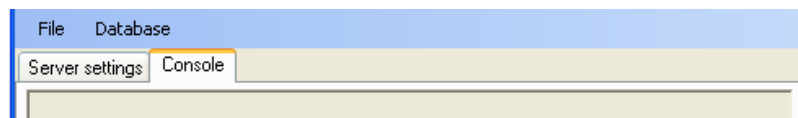
The Transfer Limit

By default, the **Transfer Limit** parameter has a value of 2. This means that after deployment of a new configuration is initiated, the number of concurrent uploads to Clavister Security Gateways will be limited to two.

Should high bandwidth links be available between the InControl server and a large number of Clavister Security Gateways that need to be updated, a higher value for the transfer limit could be chosen.

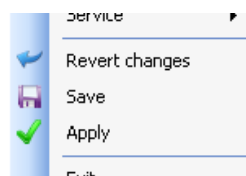
The Server Interface Console

The server interface contains a **Console** tab which gives easy access to log messages generated by the server. By default, only server startup and closedown messages appear in the console.



Applying and Saving Server Changes

After any changes are made in the server user interface, the **Apply**, **Save** and **Revert changes** options become enabled in the **File** menu as shown below:



These options function as follows:

- **Apply**

This option applies any changes to the running server and also saves them to the server configuration file.

- **Save**

This option saves the changes but doesn't apply them to the running server. They will be applied if the server restarts.

- **Revert changes**

Any changes made since the last **Apply** or **Save** are undone by this option. The server interface is updated with the values currently stored in the configuration file.

The configuration file for the server is called *ICS.exe.config* in the server installation directory and this is where server parameter values are stored.

Server Database Backups

The server provides a simple way to perform backups of the entire server database. It should be remembered that all configuration data for InControl is stored in this database so backup is strongly recommended. The default location for the active database is

Backing up does not require that InControl client activity stops. The server will, however, delay client responses until the backup process is complete. This means that client users may experience a slight delay after sending a request to the server during backup.

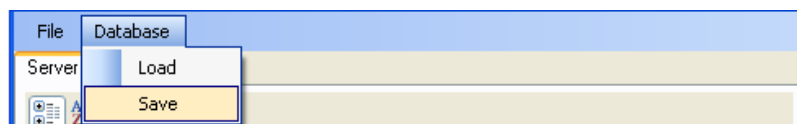
There are two ways of performing a backup:

1. Initiating the backup through the server user interface.
2. Initiating the backup through a Windows console command line.

These are discussed below:

1. Backup initiated through the server user interface.

In the server user interface, selecting the menu option **Database > Save**.



By default, backups are stored in a single file of filetype *.ics* with a filename that shows the date and time when the backup was created. For example, *db2009-01-26_153521.ics* might be the default filename created by the interface, where the filename format is *dbyyyy-mm-dd_hhmmss.ics*.

The file naming convention is, however, not mandatory and can be changed in the file chooser but is recommended as a useful way to keep track of when backup files were created. When a command line is used (as described below) this file naming convention is always used and cannot be changed.

2. Backup initiated through the command line.

It is possible to also create backup files through a Windows console command. The syntax of the command is:

```
Server Settings.exe -backup <directory>
```

If the database backup is being saved to a directory called *backup_1* then the command would be:

```
Server Settings.exe -backup backup_1
```

The command should be issued when the current console directory is the InControl server installation directory. This directory is usually the backup filename used has the default naming format described above and cannot be changed.



Important: The server should be stopped for backups

*The InControl server **must** not be running and should be stopped before performing a backup.*

A key advantage of backing up using a console command is the ability to use Windows to create a scheduled service that will automatically run a *.bat* file containing the command on a regular basis.

Restoring the Database

Restoration of a database backup can be done in the same way as the backup was created, either through the **Database > Save** menu option or through a console command with the syntax:

```
Server Settings.exe -restore <path>
```

When a database restore is complete, the InControl server will restart and any connected clients will be automatically updated to reflect the configuration data in the new version of the database. Database updates or deployments initiated by clients during the restore process will be rejected by the server.



Caution: A restore overwrites the existing database

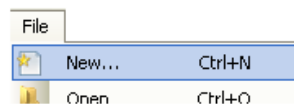
A database restore should be done with caution since the old database contents will be overwritten and completely lost once the restore is initiated.

Moving the Server Between Computers

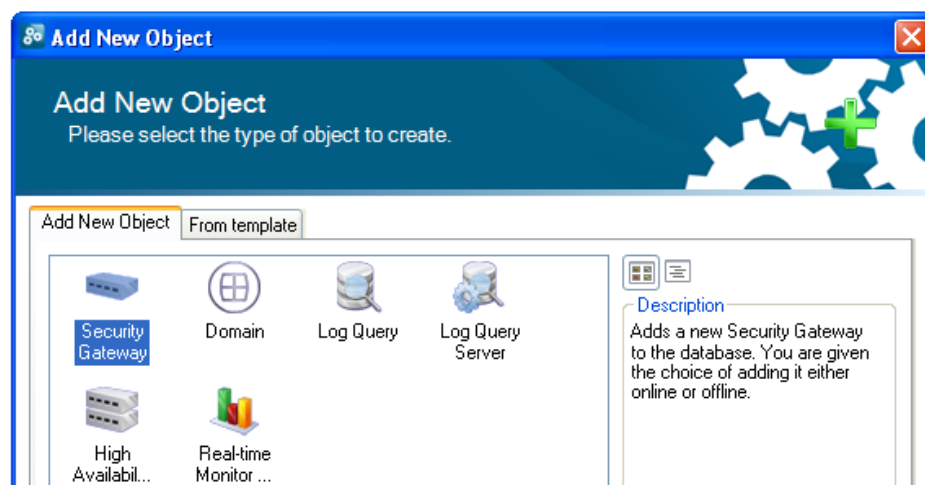
The backup and restore function also allows a server installation to be moved from one computer to another. Once the InControl server is installed on another computer, a database backup can then be restored to that new installation and the default empty database will be overwritten with the restored database backup.

Chapter 5: Adding Security Gateways

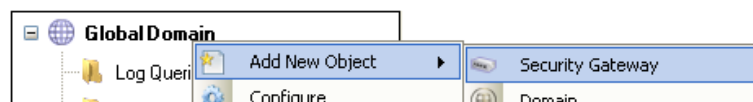
The first, most important task after installation is to have InControl connect to the first Clavister Security Gateway that will be managed. To do this, select the **New...** option from the **File** menu.



The *Add New Object* dialog will be shown. Select the **Security Gateway** option and the *New Gateway* wizard will start.



Alternatively, this step could be done by right clicking the *Global* domain node in the *Browse* panel and choosing *Security Gateway* from the *Add New Object* submenu.



The **New Security Gateway** dialog will now appear.

The name, IP address and secret key of the security gateway now needs to be entered along with a comment. The new gateway doesn't need to be online at this point but it is more straightforward if it is so that any failure to connect can be seen immediately. If the *Offline* option is selected then the model of hardware has to be also specified.

The default parent for a new gateway in the *Browse* panel navigation tree is *Global Domain* but it could be any subdomain that has been previously defined.



Tip

To move between portions of the IP address field, use the right and left arrow keys.

By clicking the icon next to the IP address field, it is possible to instead enter a URL for the gateway.

The *secret key* is the *Netcon key* required by CorePlus for login (*Netcon* is a Clavister proprietary protocol used for management functions). The key can be obtained through the Web Interface or CLI through a series of steps that are explained in Appendix A, *NetCon Key Generation*.

When the key is obtained it is copied to the Windows system clipboard and then pasted into the *secret key* field of the new gateway dialog.

If the security gateway has previously been defined as part of a cluster then a dialog will appear which will ask how to handle this. We can remove create a new cluster object in InControl for this gateway, add it to an existing cluster or remove its cluster membership. If cluster membership is removed then the security gateway can still be added later to a cluster object to again be part of a cluster.

Add Cluster Node

Select action
The Security Gateway is marked as a cluster node, but its parent is not a cluster. Please select action

Automatically create a cluster as parent for this
Cluster Name:

Select a cluster as parent for this

Add as a normal Security Gateway (disable HA functionality)

The next step is registration of the gateway with the Clavister *Customer Web*.

Registration Wizard

Choose Registration Option
Please choose the appropriate registration option.

First-time User
Choose this option if this is the first time you register a product with Clavister.

Existing User
Choose this option if you have previously registered a product with Clavister.

Register Later
Choose this option if you want to register later and run this Security Gateway in demo mode.

If we choose to register now, various customer details will be required.

Registration Wizard

Contact Information
Please fill out the following fields.

Company:

Address:

Zip Code: City:

Country: State:

Phone: E-mail:

Contact:

New registration or registration of an existing user means that InControl can automatically update the *Customer Web* with details of the new device. After this step or after choosing the

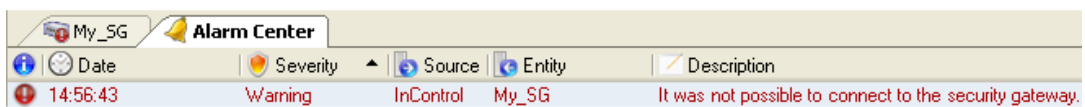
Register Later option, the security gateway is now added to InControl and appears in the *Browse* panel navigation tree.



If there are any alarms that have been generated for the new gateway, an exclamation icon will appear over the gateway node.



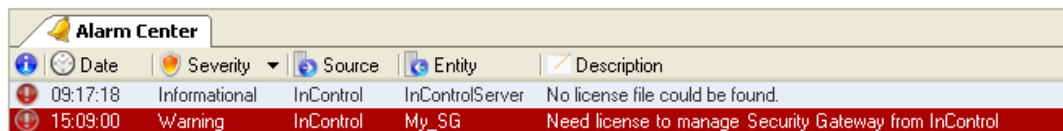
Open the *Alarm Center* by selecting that option in the *Tools* menu to examine any alarms. Below is shown the alarm line that indicates that InControl was unable to connect to the gateway.



Binding a License

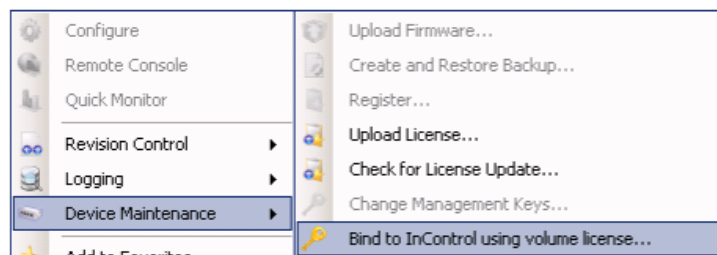
As explained in Chapter 8, *Licensing* there are a number of licensing options for InControl usage.

- If CorePlus is running in the 2 hour demonstration mode, no licensing is needed.
- If CorePlus has a license then the *CENTRALIZED_MANAGEMENT* option in the license has to be enabled. If this is not the case then alarms in the alarm center will indicate this as shown below.



- If neither of the above two options is the case then CorePlus has to have a valid *InControl Server License* (also known as a *Volume License*) bound to it. Additionally, each gateway that doesn't have the *CENTRALIZED_MANAGEMENT* license option enabled must be explicitly be bound to this InControl Server License.

Binding is done by right clicking on the gateway in the navigation tree of the *Browse* panel and selecting the *Bind to InControl Using Volume License* option.

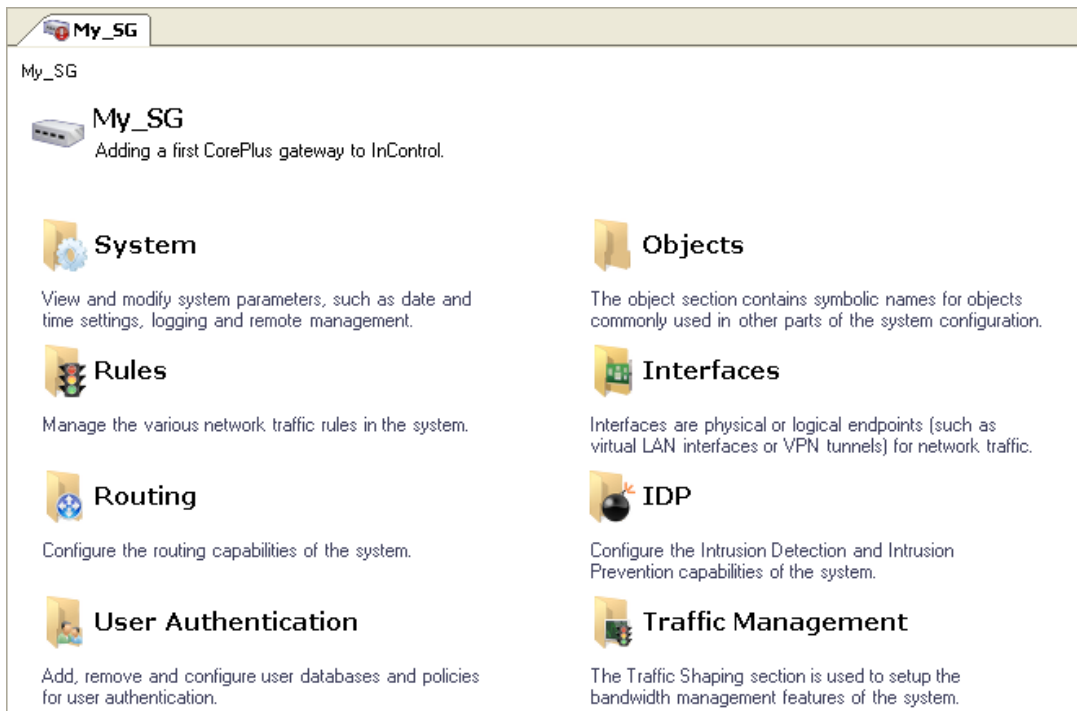


When the gateway is added, an alarm appears in the *Alarm Center* list panel to warn that it is unbound. Binding can also be done by right clicking this alarm in the alarm list and selecting the bind option from the displayed context menu.

Binding gateways to the server license is also discussed in Chapter 8, *Licensing* but is repeated here for emphasis as this step can be forgotten.

Editing the Configuration

By double clicking the new gateway's node in the *Browse* panel, the object navigation tree for the new gateway opens as a new tab in the central part of the InControl interface.



Additionally, a navigation tree view of the configuration will open in the *Navigation* panel.



Key Aspects of Configurations

The key configuration areas for the gateway now accessible through the gateway tab or the tree in the *Navigation* panel are:

- **The Address Book**

This contains definitions of the symbolic names used by InControl for IP addresses, IP networks and IP address ranges.

The Address Book is filled with a number of default entries.

- **Rules**

This is a list of all *IP Rules* which determine the rules for traffic flow through the Clavister Security Gateway. Each is defined using a *security policy* that describes the traffic it affects in terms of the source and destination interface as well as the source and destination IP address plus a service.

Some default rules exist by default but the default set will not allow anything but management traffic to flow.

- **Services**

This is a list of services with each entry normally being defined in terms of a protocol (TCP or UDP or TCP/UDP) and a port number. These services are then used to define security policies such as those defined in the IP rule set which is described above.

A large set of services is defined by default.

- **Routes**

The routing table(s) determine which networks can be found on which interfaces. By default there is one *main* routing table which contains default routes for all interfaces. This table may need to be expanded and modified.

All of the above features are fully described further in the *CorePlus Administrators Guide*. An example of editing a configuration is described later in Chapter 7, *A First Security Policy*.

Deleting Security Gateways

If a security gateway is to be deleted then this can be right clicking the gateway in the *Browse* panel and choosing *Delete* from the context menu.

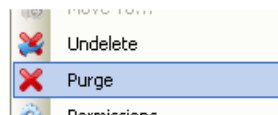
Once deleted, the gateway is removed from the navigation tree but not permanently deleted. The *Show Deleted Objects* button becomes enabled in the top left of the *Browse* panel to indicate there are deleted objects that can be restored.



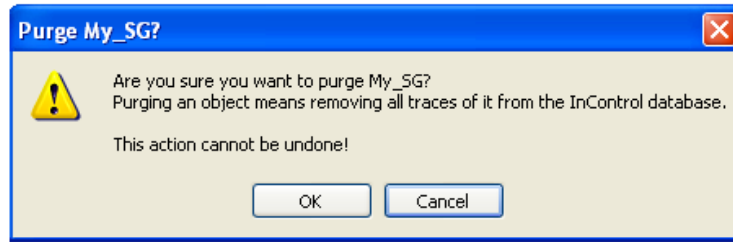
By pressing this we can restore the deleted gateway to its previous position although it remains deleted as indicated by the red cross through it.



To permanently delete this gateway, we can right click it and choose the *Purge* option.



Selecting *Purge* results in complete removal of *My_SG*.



Chapter 6: Revision Management

Revision Management is the ability to save and track changes made to CorePlus configurations and is an important tool for managing Clavister Security Gateways. Revision management allows the administrator to keep track of what was changed in configurations, when it was changed, who made the changes and provides the ability to roll back to older configuration versions. These features are also sometimes referred to as *configuration version control*.

Two key features of revision management with InControl are:

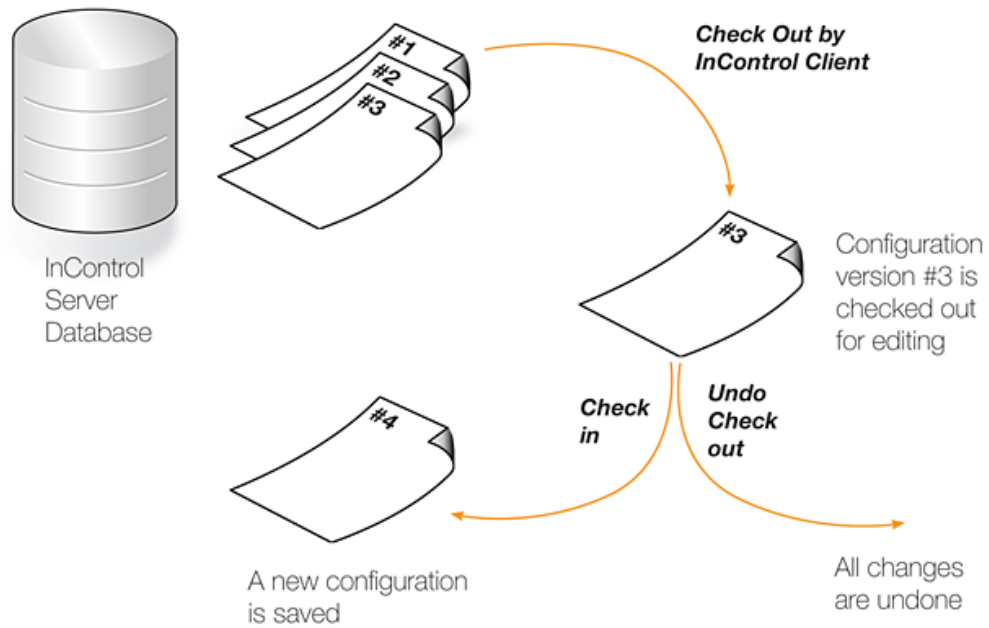
- The ability to archive many configuration versions in the InControl server database, including a record of who made the changes and when they were made.
- The *checking out* and *checking in* of configurations so that only one InControl client is updating a configuration at any one time.

InControl Version Control is Separate from the Web Interface

If version control is performed through InControl then the Web Interface should not be used to upload previously backed up configuration versions since these are completely separate from InControl. Once InControl version control is adopted then it should be continued with.

Check Out and Check In

The version control system revolves around the operations of configuration *Check Out* and *Check In*.

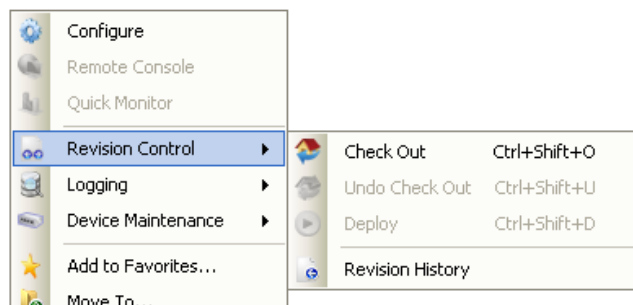


A configuration in the InControl database can be either "checked in" or "checked out". The default is "checked in" and an administrator accessing a configuration in this mode will find that it is read-only and no modifications can be made. Several administrators may access the same "checked in" configuration simultaneously in read-only mode from different management workstations.

Checking Out a Configuration

Whenever an administrator wants to start modifying a configuration, the configuration needs to be checked out.

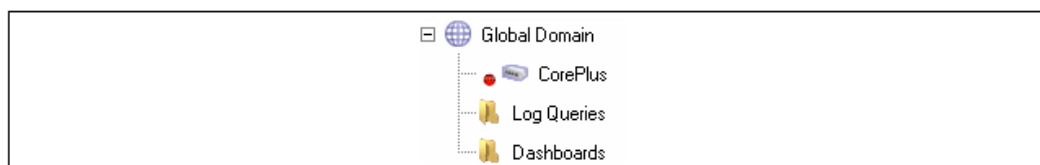
Check Out can be done by right clicking on the Clavister Security Gateway that is the target for the modification in the navigation tree. The following context menu options will appear:



Keyboard Shortcut for Checkout

An alternative to using the menu is to use select the gateway to be checked out and use the keyboard shortcut **Ctrl-Shift-O**.

A red dot will appear next to the Clavister Security Gateway node in the InControl navigation tree after check out as shown below for a Clavister Security Gateway called *CorePlus*:



The administrator who performed the check out now has exclusive write access to the configuration. As long as the configuration remains checked out, all attempts to check out the configuration by other management workstations will fail. This prevents two administrators modifying one configuration simultaneously.

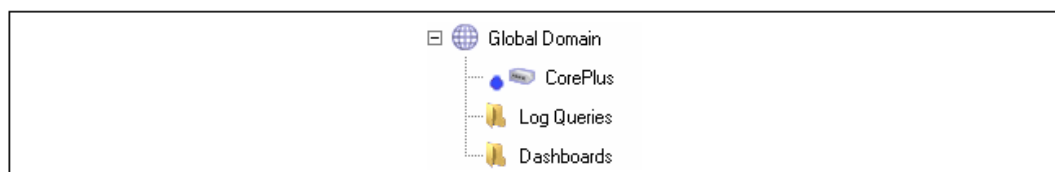
Check Out is a recursive operation. This means that if a domain configuration is being checked out, and the *Automatic Configuration Inheritance* option is enabled for that domain, all underlying configurations will be checked out. The reason for this behaviour is that a modification of the domain configuration can affect underlying configurations inheriting the domain.

The Security Editor will watch for name collisions. When checking out a configuration that contains name collisions, a dialog is shown where these name collisions may be resolved.

In a multi-administrator scenario with multiple InControl clients, best practice is that a configuration should not be "checked out" any longer than is absolutely necessary.

Already Checked Out Security Gateways

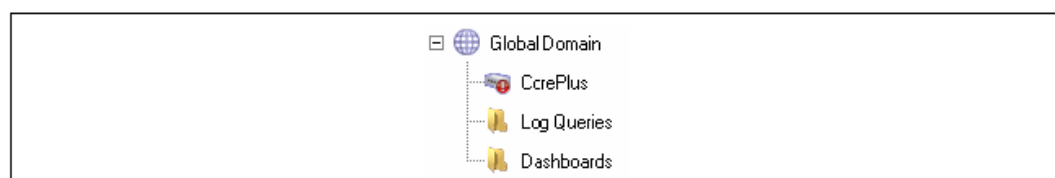
If a security gateway is already checked out by another InControl client, a blue dot icon will appear next to the gateway's icon.



Since check out of a gateway is an exclusive operation, it cannot be done on an already checked out gateway and this option will be disabled in the InControl client interface.

Security Gateways with Error Conditions

If a security gateway has a new alarm associated with it, an exclamation mark icon will appear next to the gateway's icon.



The reason for the alarm could be that the gateway is not responding to the server. Check the *Alarm Center* to investigate this further.

Automatic Check Out

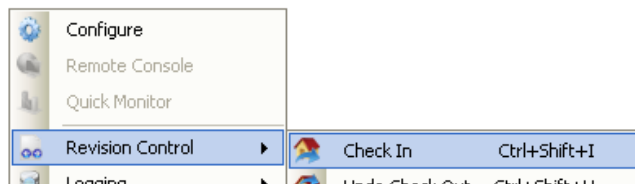
If a security gateway is selected and its configuration changed in some way without explicitly checking out the unit, then the gateway is automatically checked out by InControl. The success of the check out is obviously still subject to the possibility that another client may already have

the gateway checked out.

Checking In a Configuration

When all necessary changes have been made to the configuration, the administrator needs to perform a check in operation in order to commit the changes to the database. The check in operation stores a new version of the configuration in the management database and changes the mode to "checked in", meaning that the configuration once again is read-only.

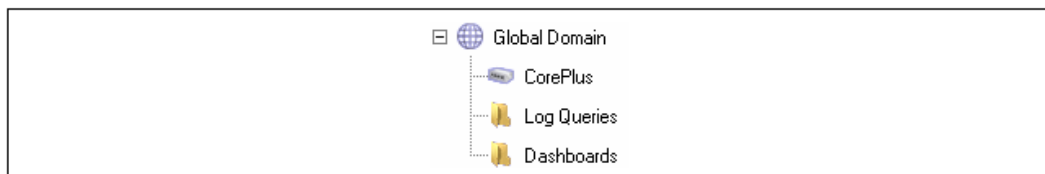
Check in can be done by right clicking on the Clavister Security Gateway that is the target for the modification in the navigation tree. The following menu options will appear:



Note

Check in can also be done by selecting the **Check In** option in the **Tasks** option panel.

After successful check in, the red dot beside the security gateway node in the main navigation tree will disappear and the gateway will appear without an icon as shown below:

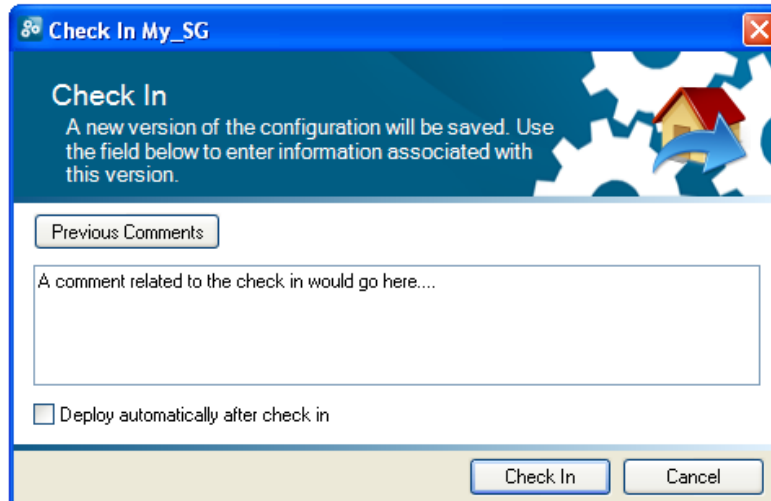


Check Ins are Recursive

A Check In is a recursive operation. This means that if a domain configuration is being checked in, and any underlying configurations are checked out, the Check In operation will cause all those underlying configurations to also be checked in.

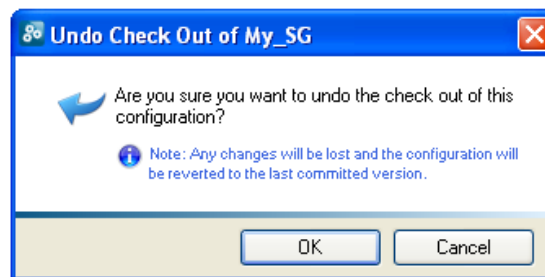
Commenting Revisions

It is recommended that the administrator add a comment each time a new revision is checked in. This provides an easy way to identify changes in the revision history.



Undo Check Out

In the event that a configuration is checked out and changes are made but the changes are to be discarded while the checkout is reversed, the *Undo Check Out* function can achieve this. The following dialog is displayed if this option is chosen:




Deploying Changes

It must be remembered that the check in operation only copies updated configurations to the InControl server database. The changed configuration must be next *deployed* to the physical Clavister Security Gateways. This can be done by pressing the deploy button (shown below) on the toolbar.



Using the deploy button will cause all configuration changes between check out and check in operations to be deployed to the relevant Clavister Security Gateways. The progress of the actual upload of configurations to the hardware units is indicated by progress bars in the bottom right panel of the InControl client interface. A screenshot of the upload progress to a Clavister Security Gateway called *CorePlus* is shown below:

Action	Device	Progress	Time remain
Upload firmware pack...	CorePlus	 100%	Done

An alternative to using the deploy button is to choose the **Tools > Deploy...** option from the menubar. This will display a dialog that lists the changed configurations that are yet to be deployed so that individual entries in the list can be selected for deployment. This means that not all configurations need to be deployed at once.

Checking In Domains and Inheritance

Domains such as the Global Domain, can be checked out, modified and deployed just like a security gateway. When checking in a domain one or more security gateway configurations may inherit objects that were altered and this situation needs to be handled by InControl. The possible scenarios are follows:

- The inheriting gateway is not checked out. This means the domain changes that affect the gateway can be checked in straight away and can also be deployed if deployment is requested.
- The inheriting gateway was checked out, perhaps by another client. In this case the check in will be put in a queue by the InControl server. There are then two possibilities for this queued request:
 1. The checked out, inheriting gateway is subsequently checked in. The queued change will now be applied and deployment will take place if that was requested.
 2. The checked out, inheriting gateway is subject to an "undo checkout". The queued change will now be applied and deployment will take place if that was requested.

Revision Numbers

Every time a new configuration version is created and activated, a *configuration revision number* is allocated to the version. This number has two parts and is of the form *nn:mm*. This number appears next to the gateway name in the title of the tab that appears for editing in InControl.

The first part of the number, *nn*, is incremented every time a new configuration is activated through a non-InControl interface such as the Web Interface or CLI. The second part of the number, *mm*, is incremented every time a new configuration is activated through a InControl client. Both numbers will start at **1**. The most recent configuration version is therefore associated with the highest version number from either number.

Whenever a security gateway configuration is changed through a non-InControl interface, any connected InControl server will be automatically notified that there is a configuration change and what the new version number is. All clients connected with the server will then be informed of this change.

Concurrent Changes Made Outside InControl

Even if an InControl client checks out a Clavister Security Gateway configuration, it is still possible that the configuration could be changed by another non-InControl user during the period it is checked out.

By using the CLI or Web Interface, another user could change the configuration outside the direct supervision of InControl. However, when such configuration changes are made, the InControl server will detect them and any InControl client that has checked out that configuration will present a popup warning message to tell the user that something has changed. The popup message gives the user the option to update their view of the configuration and this is the recommended action.

Chapter 7: A First Security Policy

The *IP rule sets* are one of the most important CorePlus components and are used to define the basic *security policies* of a CorePlus configuration. An IP rule set contains *IP rules* which state what traffic is disallowed or allowed to flow between specific interfaces and between specific networks. There can be more than one IP rule set but initially only a single, default rule set exists and this has the name *main*.

This chapter goes through the process of setting up a first security policy by defining an IP rule that allows a Clavister Security Gateway to respond to an ICMP *Ping* request. "Pinging" a security gateway from any computer is a quick and simple way to check if the gateway is up and running. When CorePlus starts for the first time, the default *main* IP rule set is empty and all traffic is therefore dropped including an ICMP traffic.

Example Assumptions

The following names and IP addresses are assumed:

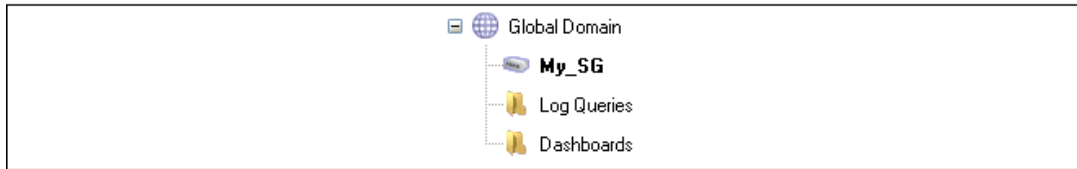
- The interface chosen as the management interface is called *lan*.
- The IP address of interface *lan* is *192.168.101.240* with the netmask *255.255.255.0*. This network is defined as an IP4 address object called *lannet* in the CorePlus configuration.
- The server or workstation running InControl resides on the same subnet and has an IP address of *192.168.101.100*.
- A Clavister Security Gateway has already been defined to InControl and given the name *My_SG* in InControl.



Note

You will have to substitute the information above with the actual interface name and IP addresses of your specific installation.

When InControl is started, the security gateway *My_SG* will appear in the *Browse* panel. If this panel is not visible, it can be opened by selecting the **View > Panels > Browse** menu option. The initial *Browse* navigation tree is shown below.



All ICMP Traffic is Initially Dropped

Let us show that the initial CorePlus configuration drops all traffic and will therefore drop any ICMP traffic such as a *Ping* request.

To do this, open a standard command console on the Windows management workstation and leave InControl running. At the command prompt, given the assumptions explained above, type:

```
> ping 192.168.101.240
```

The command should return output similar to that below.

 A screenshot of a Windows command prompt window titled 'C:\WINNT\system32\cmd.exe'. The prompt shows the command 'ping 192.168.101.240' and its output:

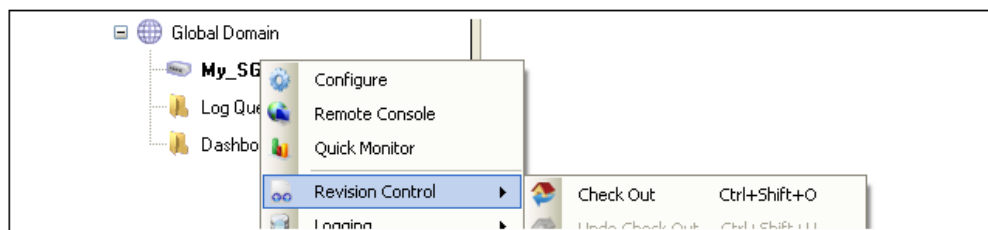

```
C:\>ping 192.168.101.240
Pinging 192.168.101.240 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.101.240:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

This output shows that CorePlus is ignoring the ICMP protocol packets, and the *Ping* command returns the *Request timed out* message.

Adding an IP Rule

Now we will add an IP rule so that CorePlus responds to *Ping* requests. The steps to do this are:

1. Right click the Clavister Security Gateway *My_SG* in the *Browse* panel and choose *Check out* from the *Revision Control* submenu.



Providing no other InControl client has *My_SG* checked out, the check out will succeed and a red dot will appear next to the gateway.



The exclamation mark indicates that there is an alarm active and this can be seen by opening the *Alarm Center*.

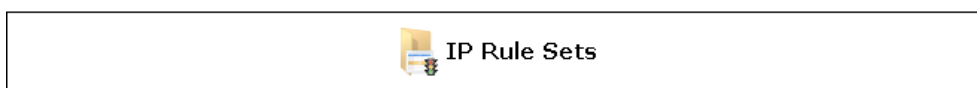


By default, check out alarms are sent to all interested clients but the *Severity* of the alarm is *Informational* and it can therefore be ignored. Alternatively, the alarm can be cleared by right clicking the alarm line and selecting *Clear* or *Acknowledge*.

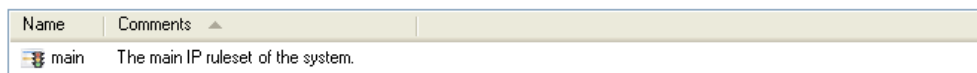
A check out event is also logged in the *Audit Trail*.



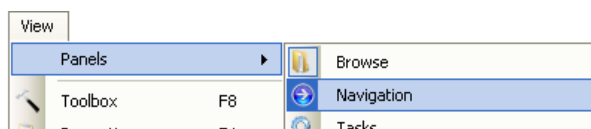
2. Now we need to select from the configuration objects for *My_SG*. This can be done in one of two ways:
 - Double click the *My_GW* and a list of configuration objects will appear in a central *My_GW* tab. Select *Rules* and then select *IP Rule Sets*.



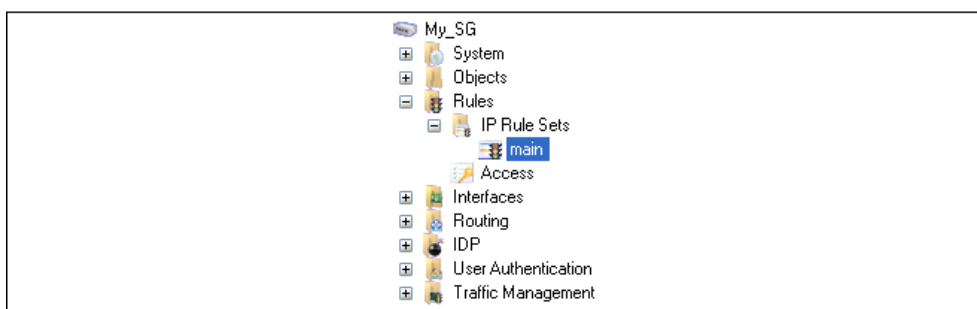
A list of IP rule sets is now displayed with only *main* as the initial member.



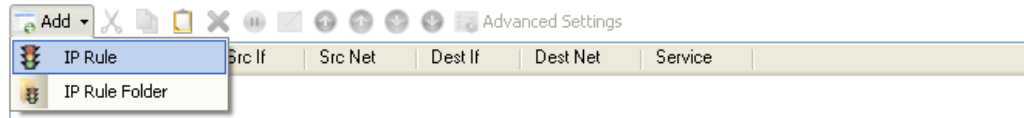
- Alternatively, after double clicking *My_GW*, open the *Navigation* panel.



This will open a tree view panel of the objects for *My_SG* and the *main* IP rule set can be opened from there.



- By selecting the *main* IP rule set we get a list of IP rules which is initially empty (equivalent to dropping all traffic). By pressing the *Add* button for this rule set we can define a new rule to allow *Ping* requests.



- Now we can define the IP rule that will allow traffic. First we define the *General* parameters of the rule. Any suitable name can be specified, in this case we use *MgmtPing*.

Name:	MgmtPing
Action:	Allow
Service:	all_icmp
Schedule:	(None)

The *Action* is *Allow* since we want to allow traffic to flow. The service is *all_icmp* which is one of the predefined services in CorePlus. The *Schedule* parameter can be used to specify specific times when the rule is to be active but is not needed here as the rule will be active all the time.

- Next, we specify the *Address Filter* of the rule which says where the affected traffic is coming from and where it is going to. These filtering parameters are common to most of the security policies that can be defined in CorePlus.

Source		Destination	
Interface:	lan	Interface:	core
Network:	lanet	Network:	all-nets

Notice that the *Destination Interface* is defined as *Core* which means that the ICMP *Ping* request is directed at the security gateway itself and it is CorePlus that will respond.

- If required, we can enable the sending of log messages for when this IP rule is triggered. This is done by selecting the *Log Settings* tab.

Enable logging:	<input checked="" type="checkbox"/> Enable logging.
Severity:	Default



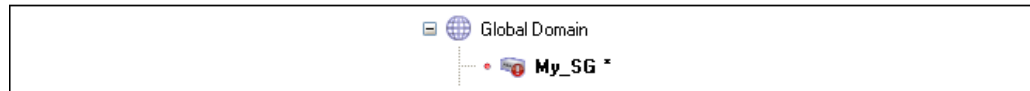
A log receiver needs to be defined

It is important to remember that no logging of IP traffic or any other CorePlus events will be done unless at least one Log receiver is first defined in CorePlus.

- Next, press the *OK* button to save the new IP rule. The rule will now appear in this IP rule set although the rule does not become active until the new configuration is *deployed* in the next step.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	MgmtPing	Allow	lan	lan_net	core	all-nets	all_icmp

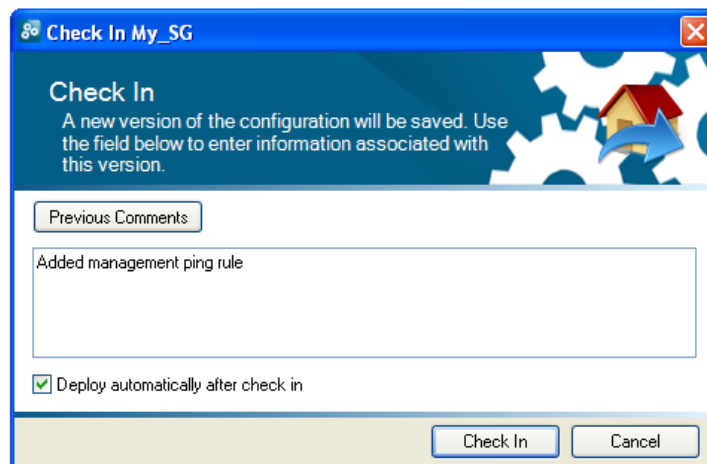
When anything in a configuration changes and needs deployment, an asterisk "*" appears next to the gateway in the *Browse* panel. This is shown below for *My_SG*.



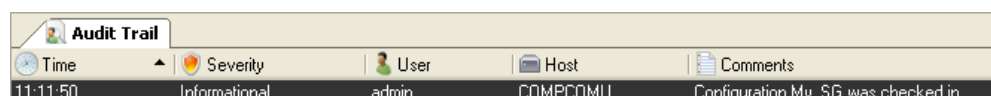
8. Finally, we must deploy the new configuration to the security gateway as well as check the configuration back in. This can be done in one of two ways:
 - Both the check in and deployment can be done in one operation. First, select the check in option after right clicking the gateway.



A dialog appears for entering a comment with the check in and includes a checkbox to specify that deployment should also be done.



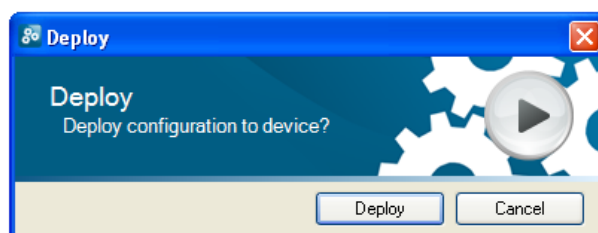
A check in will not produce an alert but will create a message in the audit trail.



- Alternatively, deployment and check in could be done separately. We can choose to deploy without checking in.

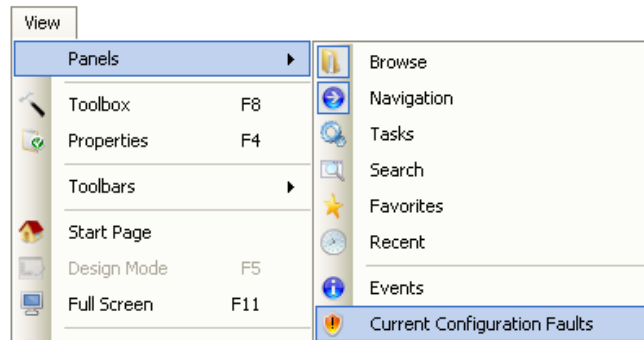


InControl will ask for confirmation before performing the deployment.

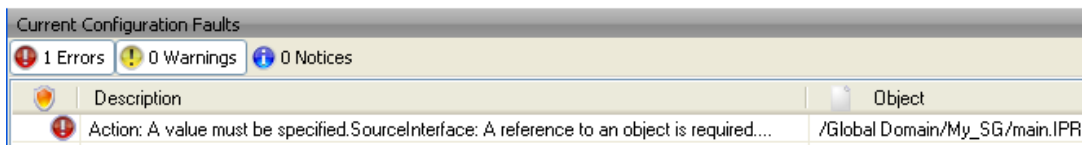


Checking for Configuration Faults

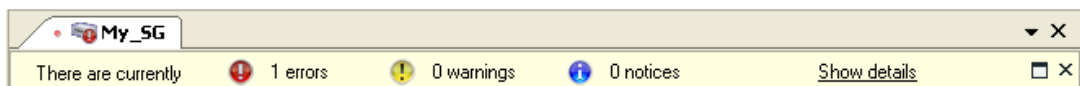
As the configuration is being modified, various configuration faults can be detected by InControl and also by CorePlus when these modifications are deployed. These faults are listed in the *Configuration Faults* panel which can be shown by selecting the option from the **View > Panels** menu.



The panel contains a list of any faults found in the configuration and these are grouped into *Errors*, *Warning* and *Notices*.



Any *Errors* that appear in the list must be fixed before a new configuration can be deployed. When InControl detects any configuration errors it also shows this in the top of the tab.



Verifying that Ping Works

Now verify that CorePlus doesn't drop all traffic and the security gateway replies to ICMP *Ping* requests. At the Windows command prompt in a console window, type:

```
> ping 192.168.101.240
```

The command should now result in output similar to that shown below.

```
C:\WINNT\system32\cmd.exe
C:\>ping 192.168.101.240
Pinging 192.168.101.240 with 32 bytes of data:
Reply from 192.168.101.240: bytes=32 time=4ms TTL=252
Reply from 192.168.101.240: bytes=32 time=99ms TTL=252
Reply from 192.168.101.240: bytes=32 time=2ms TTL=252
Reply from 192.168.101.240: bytes=32 time=2ms TTL=252
Ping statistics for 192.168.101.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 99ms, Average = 26ms
C:\>
```

If the *Ping* command returns a *Request timed out* message, the InControl connection to the Clavister Security Gateway did not succeed. Refer to Chapter 21, *Troubleshooting Connections* for possible reasons.

Chapter 8: Licensing

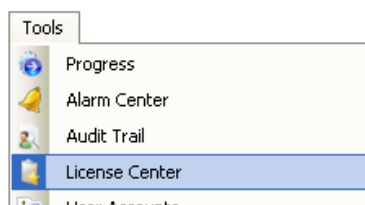
InControl Licensing Options

This chapter will first discuss the licensing options for InControl itself. There are three ways InControl can be used:

- A. In demonstration mode without licensing.**
- B. With per security gateway licensing.**
- C. With an InControl server license.**

The InControl License Center

The three options listed above are described next but first it should be noted that all licensing is managed through InControl using the *License Center*. This is selected from the *Tools* menu.



The *License Center* displays in a central tab and shows details of current licenses. An example of this is shown below (the registration keys are for illustration only).

Registration Key	Object Name	Status	Issue Date	Expiration Date
3422-1587-6868	InControl Server	OK	2009-04-30 11:25:33	2010-12-31 00:00:00
3422-1587-6868	/Global Domain/HA_Cluster/Slave	OK	2009-04-30	2010-12-31
3422-1587-6868	/Global Domain/Domain/SubDomain/CorePlus	OK	2008-09-29	2010-12-31
3422-1587-6868	/Global Domain/HA_Cluster/Master	OK	2009-04-30	2010-12-31

A. Demonstration Mode

InControl can be used without any licensing if it only manages unlicensed Clavister Security Gateways that are running in the standard 2 hour CorePlus demonstration mode. In this scenario, InControl will have full functionality for any number of Clavister Security Gateways. If we add a Clavister Security Gateway called *My_SG* to InControl we will see the following lines after

opening the *License Center* in the client.

Registration Key	Object Name	Status	Issue Date	Expiration Date
	InControl Server /Global Domain/My_SG	DemoMode		

The registration code is blank since these lines represent demonstration modes where a license is not required.

B. Per Security Gateway Licensing

Each individual Clavister Security Gateway can have a CorePlus license that allows management by InControl and this is the usual way that InControl is licensed. No special license for the InControl server is needed and InControl clients can manage any correctly licensed Clavister Security Gateway.

After purchase, the CorePlus license file is downloaded from the Clavister *Client Web* in the normal way and contains the license parameter *CENTRALIZED_MANAGEMENT*. The license can be purchased with or without this parameter enabled. If a license that allows management by InControl is purchased, the parameter is assigned a date which is when the feature expires. For the standard purchase agreement, the expiry date is normally 3 years from the date of purchase.

If a gateway doesn't have a valid license for InControl management, it can still be defined and added to InControl and will appear in the *Browse* panel navigation tree with an exclamation mark over its icon. It will not be possible to examine and edit the gateway's configuration and a line in the *Alarm Center* will indicate the missing license.

Date	Severity	Source	Entity	Description
09:02:05	Warning	InControl	My_SG	Need license to manage Security Gateway from InControl

C. InControl Server Licensing

With larger populations of Clavister Security Gateways, administering each individual CorePlus license to allow InControl management can be time consuming. A better, alternative option is to purchase an *InControl Server License* (also known as an *InControl Volume License*) from Clavister which then allows a single InControl server to manage a specified maximum number of Clavister Security Gateways through a specified maximum number InControl client sessions.



Note: Discuss this option before purchase

InControl server licensing often needs to be adapted to an organisation's specific needs so the purchase options should be discussed with your Clavister product representative.

With a server license, the CorePlus licenses of the individual Clavister Security Gateways being managed do not then need to have the *CENTRALIZED_MANAGEMENT* option enabled.

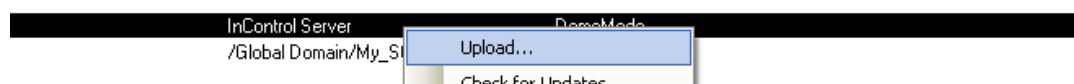
An InControl server license file is structured in a similar way to a CorePlus license and contains the following two key parameters:

1. *PROP_CLIENTSESSIONS* - How many simultaneous InControl client sessions can be opened at any one time.
2. *PROP_DEVICES* - The maximum number of security gateways that can be managed by an InControl server (and therefore by any InControl client connected to that server).

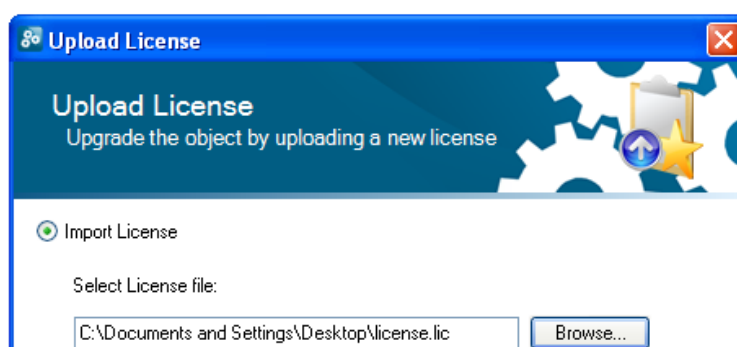
The *PROP_DEVICES* parameter value does not include any Clavister Security Gateways which

already have the license described in the previous option, which explicitly allows management by InControl. For example, if the value of *PROP_DEVICES* is 100 and one Clavister Security Gateway already has a license with the *CENTRALIZED_MANAGEMENT* parameter enabled then the InControl server can, in fact, manage that gateway plus another 100 gateways (making a total of 101).

A server license can be downloaded from the Clavister *Customer Web* and then uploaded to the server by right clicking the server license line in the *License Center* and selecting *Upload*.



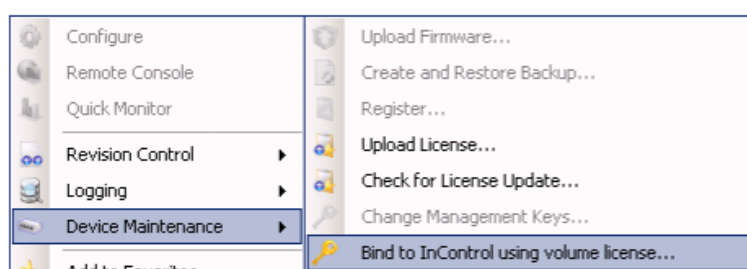
A dialog then appears to allow the license to be selected.



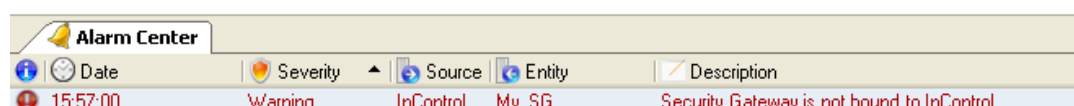
The server license can alternatively be automatically retrieved by the server from the Clavister *Customer Web* and this is discussed in a section below.

Binding an InControl Server License

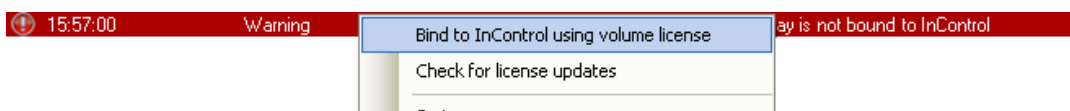
If an InControl server license is being used for managing a Clavister Security Gateway then it is important to remember that once the gateway is added to InControl then **the final step should be binding the gateway to the license**. This can be done by right clicking the gateway in the navigation tree of the *Browse* panel and selecting the *Bind to InControl Using Volume License* option.



When a new gateway is added to InControl, an alarm appears in the *Alarm Center* to warn that it is unbound as shown below.



Binding the gateway to the server license can alternatively be done by right clicking this alarm in the alarm list and selecting the bind option from the displayed context menu.



Older CorePlus Licenses and InControl

Any CorePlus licenses that were purchased before the release of CorePlus version 9.10.03 will automatically have the *CENTRALIZED_MANAGEMENT* parameter option enabled at no extra charge.

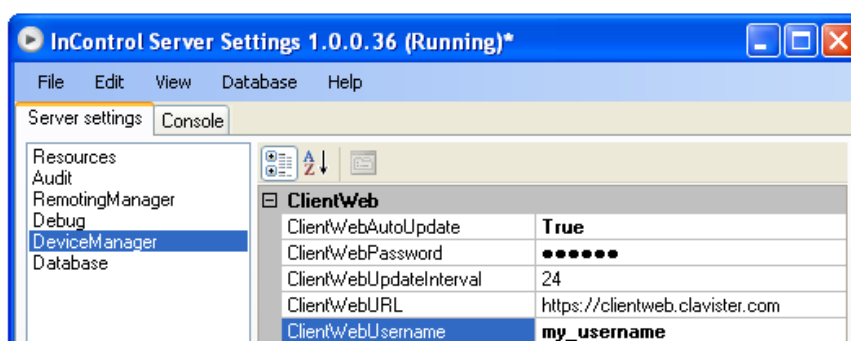
Obviously, the *CENTRALIZED_MANAGEMENT* parameter will not already appear in an older license file downloaded before 9.10.03 so the licensee should download a new license file from the Clavister *Customer Web* and upload it to the Clavister Security Gateway. The new license file will have a standard 3 year period specified for the *CENTRALIZED_MANAGEMENT* parameter **starting from the date of InControl's initial version 1.0 release** in June, 2009. When that period expires, a new InControl license should be purchased to extend InControl administration of the gateway.

All new CorePlus users will have to purchase one of the two licensing options described in the list above if InControl is to be used without restrictions.

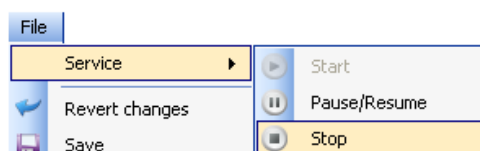
Automatic Retrieval of InControl Server Licenses

The InControl server has the ability to automatically retrieve a server license from the Clavister *Customer Web*.

To do this, open the server user interface by selecting the server from the InControl program group in the Windows Start menu. Select *DeviceManager* from *Server Settings* and change the *ClientWebAutoUpdate* option to be *true*. Next enter the username and password used for web access to the Customer Web. In the example shown below, *my_username* has been entered as the username.



The server must be restarted for the license to be retrieved. Do this by selecting *Stop* from the *Service* submenu.



Restart the server by selecting *Start* from the *Service* submenu.



When the server license is successfully retrieved it will appear in the *License Center* panel. An example of successfully installed server license is shown below.

License Center				
Registration Key	Object Name	Status	Issue Date	Expiration Date
1234-5678-9876	InControl Server	OK	2008-10-10 17:17:17	2010-10-10 12:30:10

CorePlus Licensing

With or without InControl, a Clavister Security Gateway requires a *CorePlus License* in order to function correctly. The license determines the operational capabilities of a CorePlus system as well as protecting against the unauthorized use of Clavister products. As explained above, this license can also specify that InControl usage is allowed, otherwise a separate InControl license must be used and associated with the InControl server.

CorePlus Demonstration Mode

When CorePlus operates without a license, it functions in *demonstration mode*. This means that CorePlus will cease to function after two hours of operation except for allowing management traffic. A restart is then required to continue running the product for another two hours.

No licensing is required for InControl if it is communicating with Clavister Security Gateways operating in demonstration mode.

CorePlus License Uploads

A new CorePlus license can be uploaded to a Clavister Security Gateway at any time. However, this is best done during hours of low system usage or during routine maintenance. A license upload will cause CorePlus to restart and all existing connections will be lost. This is because the new license may require a different allocation of memory, for example if the maximum number of VPN tunnels have been changed.

The Customer Web

Clavister provides a secured web site, the Clavister *Customer Web*, where all licenses can be administered. Furthermore, Clavister InControl includes all functionality needed for license management.

The Customer Web can be found at the URL: <https://clientweb.clavister.com>.

The Registration Key

All Clavister products are shipped without an installed license. For CorePlus, a valid license is retrieved from the Clavister Customer Web using a *registration key* and a MAC address of one of the hardware's Ethernet interfaces. The MAC address can be found on the underside of smaller Clavister hardware models. The key is provided on a *Certificate of Authenticity* which is a card usually included with all Clavister products including the software-only CorePlus product.

The registration process is automated within Clavister InControl, but it can also be performed manually on the Clavister Client Web. When registration is complete, a license is automatically generated and deployed to the installed Clavister Security Gateway or to the InControl server.

The License File

A Clavister license is a single file with filetype *.lic* which can be stored on disk. It is possible to read the file's content with a text editor.

When a CorePlus license is uploaded to the Clavister Security Gateway, it is stored as a file called *license.lic* in the Clavister Security Gateway's local memory. A CorePlus license is bound to the hardware using the *MAC address* of one of the Ethernet adapters.

The license file is created in a similar format for both InControl and CorePlus. After binding, an InControl license is kept with the server in the installation folder

License Expiration Alerts

By choosing the menu option **Edit > Preferences**, the client preferences dialog will appear and the *License Expiration Alert* setting can be changed.

Dampening	High
LicenseExpirationAlert	14
ShowSystemResources	True

This value specifies the number of days before license expiration when an alert about impending license expiration starts to appear. The default value is 14 days (in other words, 2 weeks).

Chapter 9: Alarms

Overview

InControl *alarms* are notifications of certain events that can be sent to InControl clients. Through InControl, the administrator can define what kinds of alarms are of interest, to whom notification should be sent and how they should be managed.

An Alarm's Components

An alarm has the following attributes:

- **A Source**

The *source* is the software that created the alarm. In most cases, this is an InControl server.

- **An Entity**

The *entity* is the device which is the subject of the alarm. In most cases this will be a particular Clavister Security Gateway.

Alarm Actions

A single alarm can be subject to the following processes:

- Triggering

An alarm is triggered by the *entity* associated with it. Triggering means that that a state has occurred that should be notified. For example, InControl might notice that it is unable to contact a particular security gateway.

- Acknowledgement

An alarm can be acknowledged by an InControl client user. Acknowledgement can be done by applying an *action* to an alarm. An alarm can have one or many actions associated with it.

If an alarm is acknowledged by one client, it becomes automatically acknowledged for all clients.

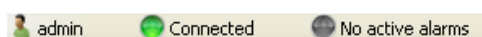
- Clearing

The clearing of an alarm is done by the alarm's source. For example, an alarm that indicates a particular security gateway is unreachable could be cleared when that gateway becomes reachable again.

An override feature for the user to clear the alarm manually is provided but this should not normally be needed.

The Alarm Indicator Icon

Every InControl client display includes an alarm indicator icon at the bottom of the client interface. If there are no active alarms, the indicator appears as shown below:



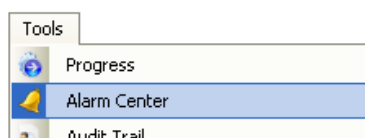
When any alarms are active, this icon changes as shown below:



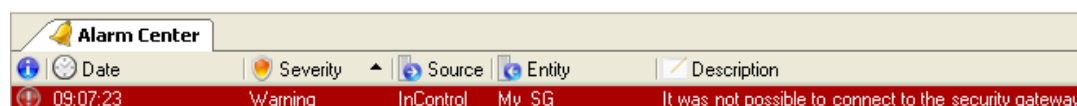
In this example, the display indicates there are two active alarms for this InControl client.

The Alarm Center Display

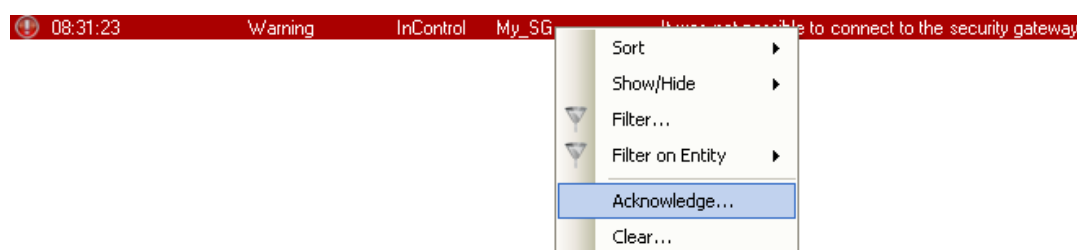
The *Alarm Center* in the InControl client interface displays information about all alarms, including alarms that have been triggered but not yet cleared. It can be opened by selecting the *Alarm Center* from the *Tools* menu.



InControl will now display a summary of alarms for this client:



Right clicking an alarm will cause a context menu to appear from which a number of actions can be chosen:

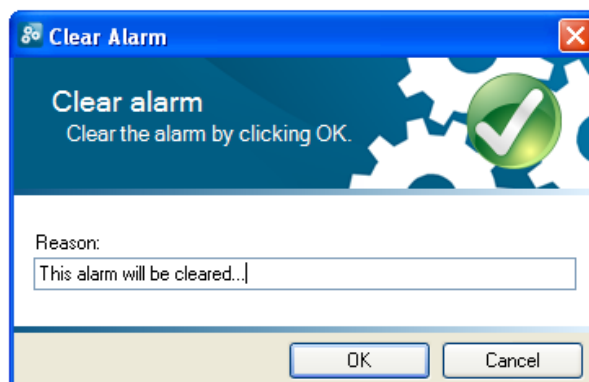


Clearing Alarms

If the *Clear* option is chosen, this means the user is saying "I have seen the problem and it is fixed".

Many alarms will be eventually be cleared by InControl itself. For example, if the alarm is caused by a failure to connect to an offline security gateway then when the gateway comes back online InControl will clear the alarm itself.

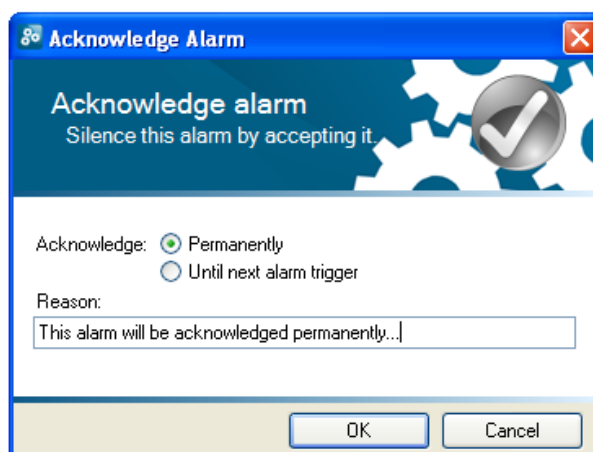
After choosing the clear option, a dialog is shown so that a reason for clearing the alarm can be given and stored in the alarm history.



When an alarm is cleared, either by InControl itself or explicitly by the user, it is removed from the standard alarm list and stored in the *Alarm History*.

Acknowledging Alarms

When an alarm is acknowledged, the user is saying "I know about this but it isn't fixed". If this option is chosen, an acknowledge dialog is shown so that a reason for acknowledgement can be given.



The acknowledgement dialog includes two further options:

- **Acknowledge Permanently**

This means that an alarm will not reappear if the same alarm occurs again.

- **Acknowledge Until Next Alarm Trigger**

This means that the alarm will disappear from the *Alarm Center* list but if the same alarm occurs again, it will have its state changed back to unacknowledged and reappear in the alarm list.

Note that the phrase *same alarm* means that the responsible source and event are unique, as explained later.

Acknowledged alarms are not stored in the *Alarm History* but will be stored by InControl until they are eventually cleared, even though they aren't displayed.

An acknowledged alarm must be cleared before it disappears into the alarm history and this can happen due to a clear being done by InControl. Alternatively, the user can clear the alarm explicitly by using the filtering option in the client to display find it and then applying a clear operation to it.

Alarm Uniqueness

Alarms in the list of active alarms are unique. The combination of alarm type, source and entity must be unique for each entry in the list. Although an alarm might trigger repeatedly, for instance every few minutes if a security gateway is unreachable, the triggering will always update the same entry in the alarm center list.

The Alarm History

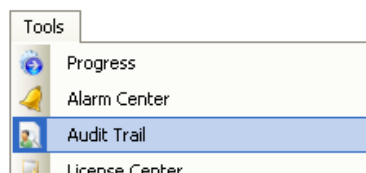
CorePlus retains an audit trail of all alarms that are triggered. When an alarm is cleared, it is removed from the active alarm list and placed into the alarm history. This history can be searched from the alarm center based on the search criteria listed below:

- Time when first triggered.
- Time when first triggered.
- Time when last triggered.
- The source.
- The entity that the alarm refers to. For example, a security gateway.
- The acknowledgement state of the alarm.
- The user that acknowledged the alarm.
- Time when the user acknowledged the alarm.
- User provided comment from user.
- If alarm has been cleared.
- The user that cleared the alarm.
- Time when alarm was cleared.
- The alarm type.
- The alarm source.
- The ID that uniquely identifies the alarm from all alarms with the same source type.
- The name.
- Severity level.
- The default action.

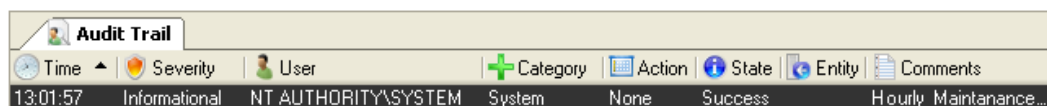
Chapter 10: The Audit Trail

Changes made to Clavister Security Gateway configurations, as well as a variety of other actions performed by InControl clients, are logged on the InControl server and are retained as an *Audit Trail*.

The *Audit Trail* is displayed by choosing the option from the *Tools* menu.

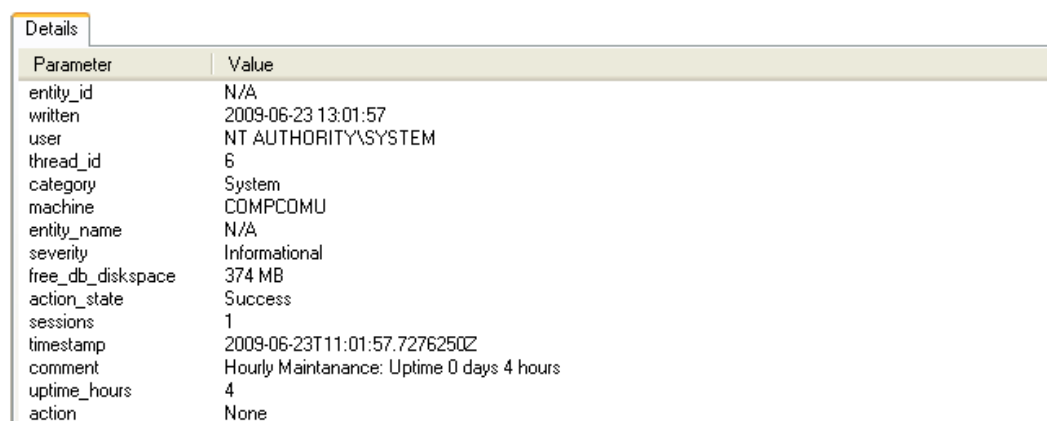


Each entry in the trail shows what action was performed by who and on what. An example of the audit trail display is shown below, showing the entry added by InControl as it performs regular system maintenance.



Time	Severity	User	Category	Action	State	Entity	Comments
13:01:57	Informational	NT AUTHORITY\SYSTEM	System	None	Success		Hourly Maintenance...

By selecting any single line in the audit trail display, the details of that event are shown. Below are the details of the system maintenance event from the image above.

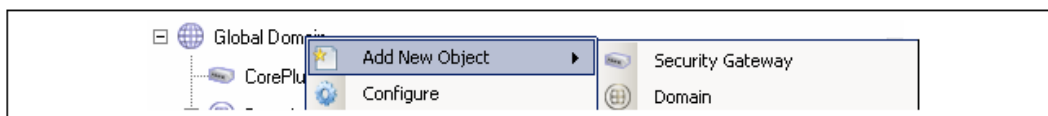


Parameter	Value
entity_id	N/A
written	2009-06-23 13:01:57
user	NT AUTHORITY\SYSTEM
thread_id	6
category	System
machine	COMPCOMU
entity_name	N/A
severity	Informational
free_db_diskpace	374 MB
action_state	Success
sessions	1
timestamp	2009-06-23T11:01:57.7276250Z
comment	Hourly Maintenance: Uptime 0 days 4 hours
uptime_hours	4
action	None

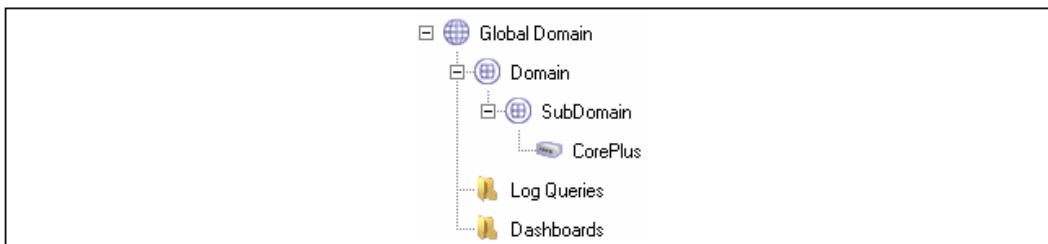
Chapter 11: Creating Domains

It is often the case that a set of configurations objects need to be shared amongst a subset of the security gateways defined to InControl. In this situation, a *Domain* can be defined in the InControl navigation tree.

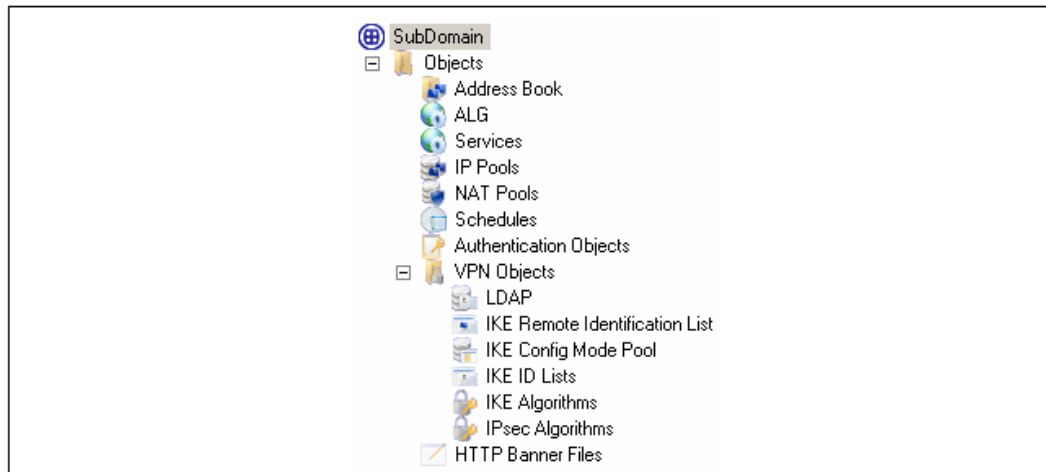
The *Global Domain* always exists in a CorePlus configuration and this is used to share CorePlus configuration objects amongst all security gateways. By right clicking on the global domain, we can choose *Add New Object* from the context menu followed by the *Domain* option in the submenu:



Once the new domain is defined, it appears under the global domain. However, it is then possible to create further domain levels. The screenshot below shows a domain called *subdomain* defined under a domain called *domain* which is itself defined under the global domain. A security gateway called *CorePlus* has been defined under *subdomain*.



Once defined, *subdomain* has a set of objects which are similar to the set found in the global domain. The *subdomain* object set applies only to the security gateways defined within *subdomain*. Below is the object navigation tree that is shown:



The above arrangement means the following:

- The objects in any domain are available to all security gateways within the domain, including any defined within any sub-domains.
- It follows that the objects in the global domain are available to all security gateways.

Name Duplication

CorePlus does not allow the same object name to be used twice in a hierarchy of domains. For example, a *Service* object called *my_service* in the global domain cannot coexist with another *Service* called *my_service* in a domain or security gateway at a lower level.

Checking Domains Out and In

Not only is it possible to check out an individual security gateway, it is also possible to check out a domain and apply version control to its contents.

When a domain is checked out, only the domain itself is checked out. Everything within that domain is not automatically also checked out.

When the domain is checked in, any changes made to objects in the domain that are used by security gateways within the domain are now applied by the InControl server. In other words, the configurations of security gateways affected by the domain changes are automatically updated.

Applying Domain Changes to Checked Out Gateways

If domain changes have to be applied to a security gateway that is already checked out by another InControl user then the changes are queued by the InControl server until the security gateway is checked back in. At that point, the InControl will attempt to apply the queued changes.

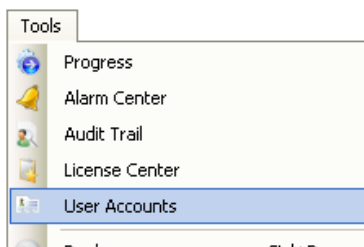


Note: Domains are only available in InControl

The domain concept is only available in InControl. The domain concept is not available if using the Web Interface or the CLI to perform administration tasks. However, it is still possible to administer configurations with either InControl or the other interfaces.

Chapter 12: User Accounts and Groups

By selecting **Tools > User Accounts** the *User Accounts* panel will open and we can create new *Users* as well as *User Groups*.



The *User Accounts* dialog will now appear in the main InControl panel. The top list shows all currently defined users:

Name	Password	Groups
admin	XXXXXXXXXX	Administrator
auditor	XXXXXXXXXX	Auditor

The bottom list shows all currently defined groups to which a user can belong:

Name	System Permissions	R/W Permissions	Local Users
Administrator	All	[root recursive All]	admin
Auditor	Configure, Monitor, ...	[root recursive Read]	auditor

Adding Users

An individual user can be defined by selecting the **Add button** under the user list in the *User Accounts* panel. This starts the *New User* wizard and we begin by giving the user a unique name, for instance *admin2* along with a password (that should be hard to guess).

The screenshot shows a window titled 'New User' with a blue header. Below the header, the text 'New User' and 'Please enter user credentials' is displayed. There are three input fields: 'Name:' with the text 'admin2', 'Password:' with six dots, and 'Retype Password:' with six dots.

In the next and final wizard step, we assign the user to a pre-existing *Group*. A group defines the permissions that a user has. InControl provides two groups by default, the *Administrator* group and the *Auditor* group. In this example we choose the *Administrator* group for *admin2* and the user then inherits its permissions from the group.

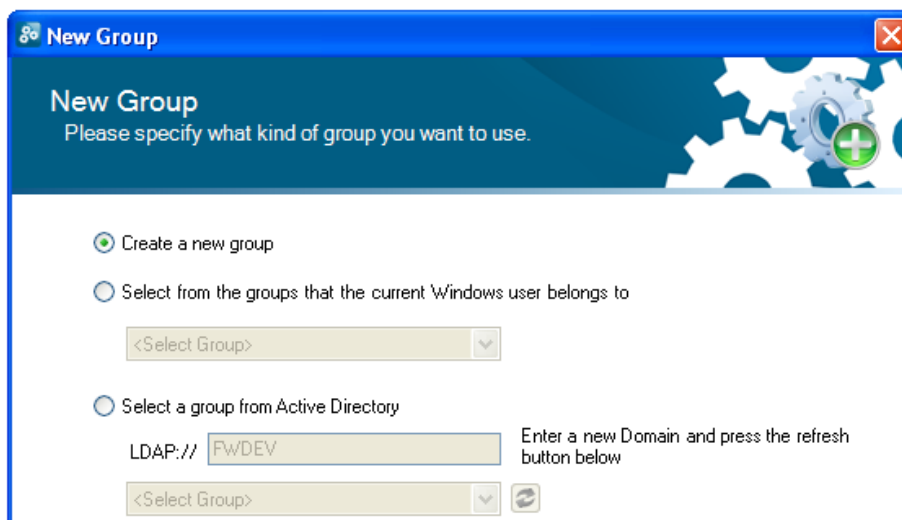
The screenshot shows a window titled 'New User' with a blue header. Below the header, the text 'New User' and 'Select appropriate user groups.' is displayed. There is a table with two columns: 'Group' and 'System Permissions'.

Group	System Permissions
<input checked="" type="checkbox"/> Administrator	All
<input type="checkbox"/> Auditor	None

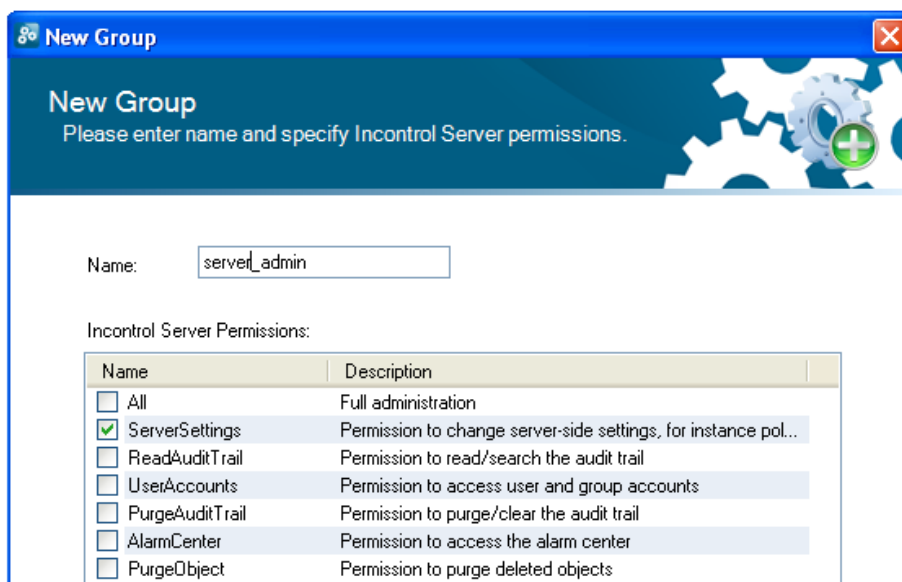
The *Administrator* group allows full access to all functions. The *Auditor* group allows the least permissions which is read only access to certain data. The creation of new groups that have sets of permissions between these extremes is discussed next.

Creating Groups

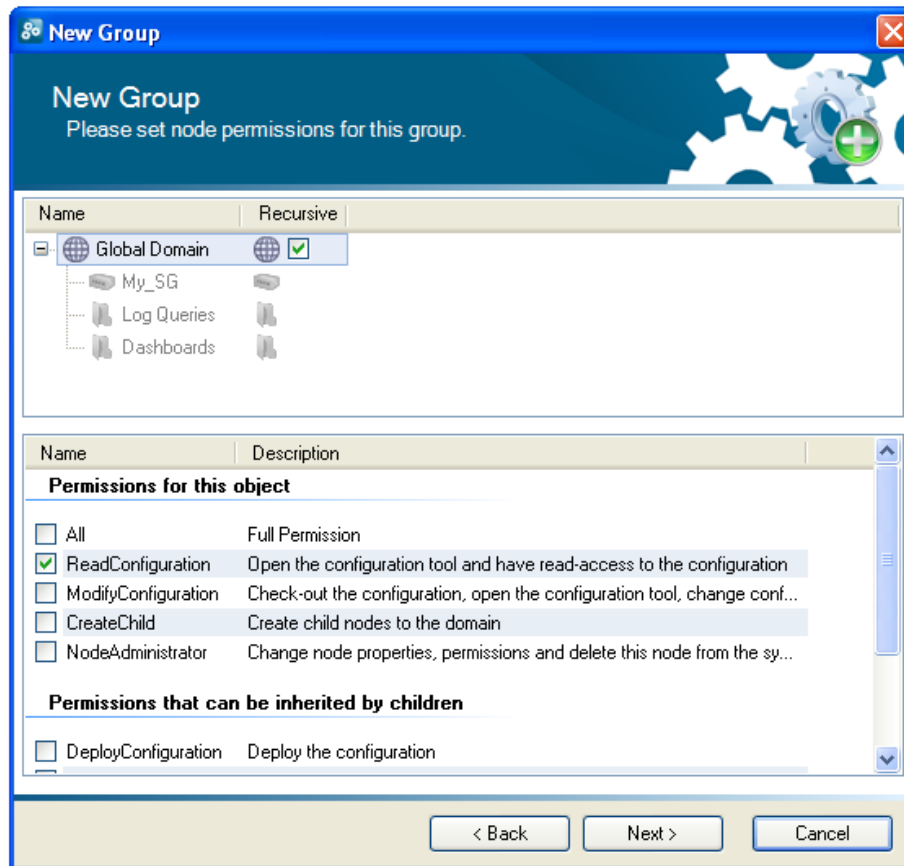
If we now press the **Add** button under the list of user groups, the *New Group* wizard starts and we select the option to create a new group.



Next we specify a name, in this example *server_admin*, along with what *InControl Server Permissions* the group will have. Here, we select the privilege to change server settings.



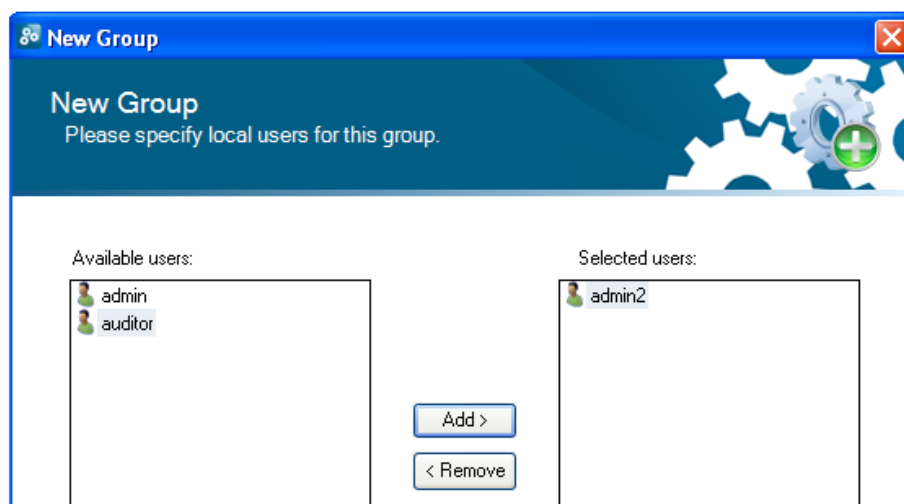
The next step is to specify what permissions this group has in relation to individual Clavister Security Gateways. In the example below, the only permission given to the group is that configurations can be read (but not changed).



Notice that the top panel in this step is used to specify to what security gateways or domains the permissions will apply. By default, the permissions are specified for the *Global Domain* and is specified as *Recursive* which means that permissions apply to all sub-domains and security gateways. Alternatively, the permissions could be applied to a particular gateway or group of gateways.

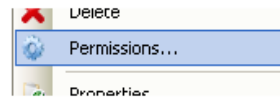
Permissions are divided into two categories, those that are directly applicable to the object selected (in the example, the *Global Domain*) and permissions that are inherited by children when the *Recursive* option is selected.

In the final step, the wizard allows us to move particular local users to be moved into this group. This can be a useful step since we may have created the users before the group was created. On this case we move the *admin2* user into the new group before pressing *Finish*.

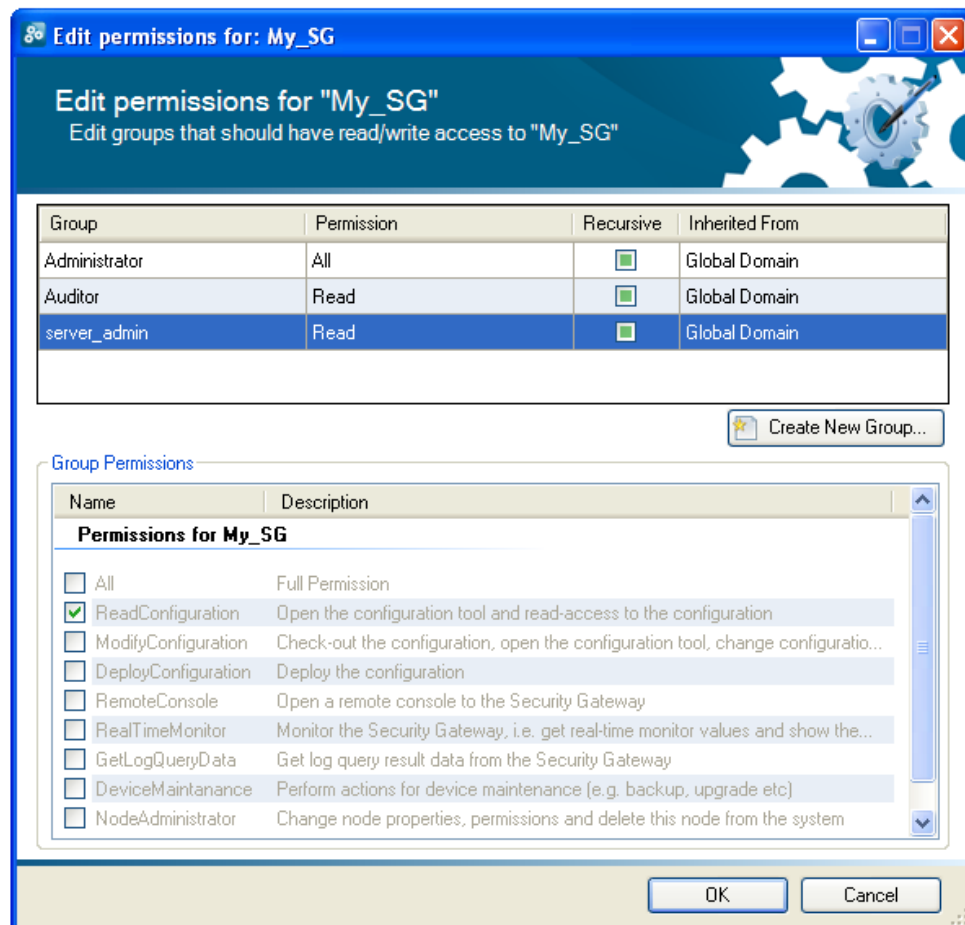


Setting Permissions on Gateways and Domains

By right clicking a security gateway or domain in the InControl navigation tree, the **Permissions** option can be chosen from the context menu.



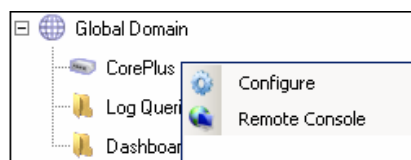
This option displays a dialog which indicates which user groups affect the gateway and allow changes to be made regarding the group membership.



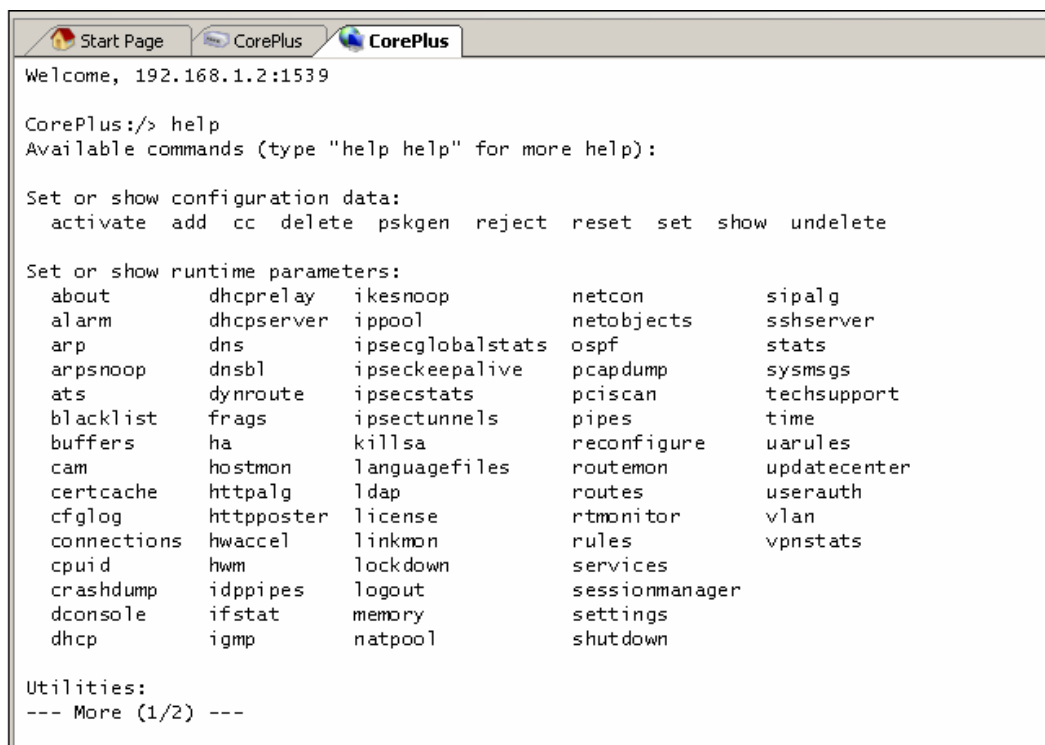
Chapter 13: Remote Console

This chapter describes the Remote Console feature of InControl, which is used to access the CLI in CorePlus from within the InControl environment.

A console can be opened by right clicking a security gateway in the navigation tree. The following context menu will appear:



If the *Remote Console* option is chosen, a new tab will open that contains the console session. In the screenshot shown below, a security gateway called *CorePlus* has a console opened for it:



The console can be used for issuing CLI commands just as a Secure Shell (SSH) console or a local

console attached to the hardware RS232 port can be used for doing this.

The remote console can be often be used to troubleshoot problems. Below is an example of the *ipsecstat* command being used to show the status of IPsec tunnels:

```

Cmd> ipsecstats -ipsec

--- Active child SAs:

VPN Tunnel      Local Address    Remote Address    Remote GW
-----
IPSecTunnel_TEN  0.0.0.0/0        10.20.10.43       10.20.1.106
IPSecTunnel_TEN  0.0.0.0/0        10.20.10.37       10.20.1.106

Cmd> ipsecstats -u

--- Active child SAs:

1 IPsec Tunnel   : IPSecTunnel_TEN
  Endpoints      : 0.0.0.0/0 <-> 10.20.10.43
  Remote Gateway : 10.20.1.106
  Protocol       : ESP: AES HMAC-SHA1
  SPI (in)      : 0x9c515412
  SPI (out)     : 0xid289c40

  Counters:
  Packets in    : 30
  Packets out   : 29
  Kilobytes in  : 2
  Kilobytes out : 2

2 IPsec Tunnel   : IPSecTunnel_TEN
  Endpoints      : 0.0.0.0/0 <-> 10.20.10.37
  Remote Gateway : 10.20.1.106
  Protocol       : ESP: AES HMAC-SHA1
  SPI (in)      : 0x9c515414
  SPI (out)     : 0xa3585795

  Counters:
  Packets in    : 2364
  Packets out   : 2763
  Kilobytes in  : 160
  Kilobytes out : 226

```

For a complete list of CLI commands, refer to the separate *CLI Reference Guide*.

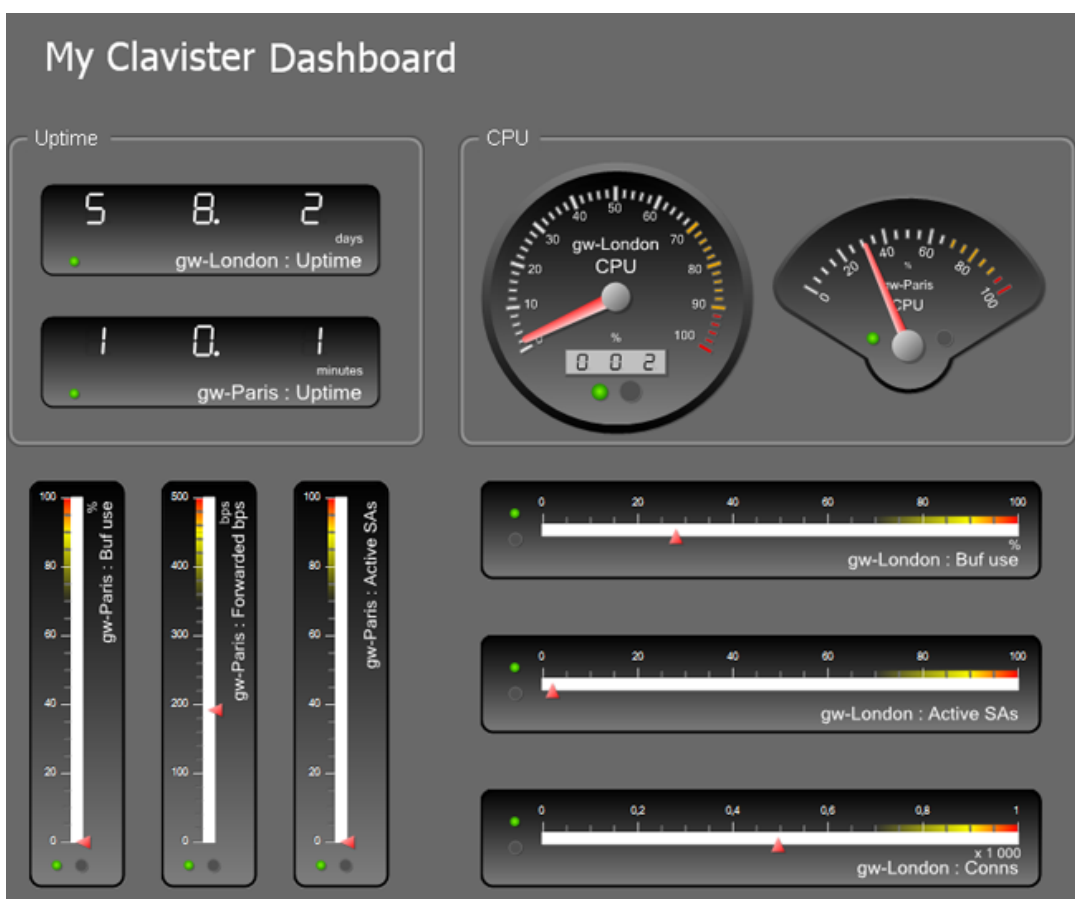
Multiple Console Sessions

It is possible that multiple InControl clients as well as multiple SSH clients could be changing a single CorePlus configuration at the same time. This is allowed by CorePlus and the when a CLI console session saves and activates its changes then those changes are at that point in time applied to the current configuration.

Chapter 14: Real-time Monitoring

Monitoring Overview

InControl *Real-time Monitoring* allows monitoring of one or more Clavister Security Gateways using a variety of *controls* arranged in the style of a *Dashboard*. Two examples of typical dashboards are shown below to illustrate what is possible with this feature.



The image above illustrates a dashboard consisting of *Gauge* monitoring controls in various styles. Each Gauge is monitoring a single parameter in a CorePlus installation.

The image below shows a dashboard consisting of a *List* control at the top, a *Bar Chart* in the middle, with a *Line Chart* control at the bottom. The List and Chart are each being used to monitor a number of different parameters in a CorePlus installation at the same time.



Real-time Monitoring Components

When using Real-time Monitoring, the essential components are:

Monitoring Controls

Monitoring Controls are graphical displays which can show the current value of a CorePlus operating parameter for a Clavister Security Gateway. Some controls monitor only one parameter (Gauge), some can monitor multiple parameters (Chart or List). A range of control styles are available and almost any style can be associated with any CorePlus parameter.

Dashboards

A *Dashboard* is a set of one or more controls that are displayed together for monitoring a group of CorePlus parameters. Different controls in a single dashboard can monitor just one or many Clavister Security Gateways. Monitoring controls of any type can be placed anywhere on a dashboard and they can be scaled to any size.

Dashboard Templates

A pre-defined set of *Dashboard Templates* are provided with InControl. These consist of pre-defined sets of monitoring controls that are already associated with a CorePlus parameter. Using the editor, a Template can be opened, possibly changed, associated with a Clavister Security Gateway, and then saved as a normal user-defined dashboard.

Monitoring Control Types

The following types of Monitoring controls are available:

Generic Monitoring Controls	These fall into two categories:				
	<table> <tr> <td>Gauges</td> <td>A <i>Gauge</i> is a graphical display which can show the current value of a single CorePlus operating parameter on a single Clavister Security Gateway. A range of Gauge styles are available and any style can be associated with any CorePlus parameter.</td> </tr> <tr> <td>Chart and List</td> <td>As an extension of a Gauge, the <i>Chart</i> and <i>List</i> are Gauges that can display multiple parameters in a single graphical unit and provide a simple means to do comparisons. A Chart is available in two forms: a <i>Bar Chart</i> and a <i>Line Chart</i>.</td> </tr> </table>	Gauges	A <i>Gauge</i> is a graphical display which can show the current value of a single CorePlus operating parameter on a single Clavister Security Gateway. A range of Gauge styles are available and any style can be associated with any CorePlus parameter.	Chart and List	As an extension of a Gauge, the <i>Chart</i> and <i>List</i> are Gauges that can display multiple parameters in a single graphical unit and provide a simple means to do comparisons. A Chart is available in two forms: a <i>Bar Chart</i> and a <i>Line Chart</i> .
Gauges	A <i>Gauge</i> is a graphical display which can show the current value of a single CorePlus operating parameter on a single Clavister Security Gateway. A range of Gauge styles are available and any style can be associated with any CorePlus parameter.				
Chart and List	As an extension of a Gauge, the <i>Chart</i> and <i>List</i> are Gauges that can display multiple parameters in a single graphical unit and provide a simple means to do comparisons. A Chart is available in two forms: a <i>Bar Chart</i> and a <i>Line Chart</i> .				
Pre-defined Controls	InControl includes special controls that have been created to monitor specific CorePlus parameters. The <i>Web Content Filtering</i> control is an example of this.				
Layout Controls	These consist of the <i>Label</i> control for adding text and/or images to a dashboard, and the <i>Group</i> control for creating groups of related controls within a dashboard.				

Design Mode and Monitor Mode

Real-time Monitoring functions in one of two modes:

Design mode	In this mode, the editor is used to create individual dashboards which can be saved and re-edited later. Real-time monitoring is not activated while in Design mode.
Monitor mode	In this mode, a specific dashboard associated with one or more Clavister Security Gateways is used for live monitoring. This mode can optionally be full-screen using F11 to toggle between normal and full-screen.



Tip

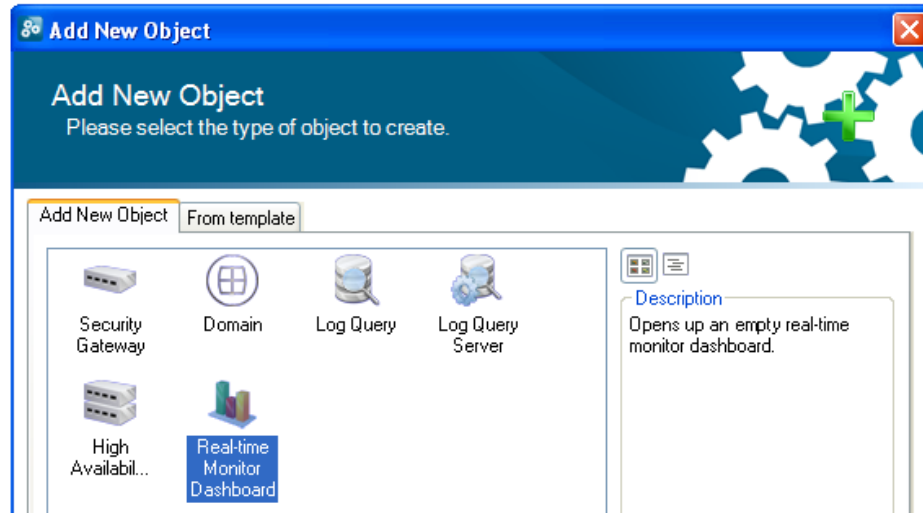
Toggling between the design and monitor modes can also be done with the **F5** function key.

Creating Custom Dashboards

By using the *Design mode* editor, custom dashboards can be created which contain the *Monitoring controls* that are desired for managing particular CorePlus installations. An initial empty editor screen is shown below with no controls yet added.

Starting a New Dashboard

To begin a new dashboard, select the *New* function from the *File* menu. In the resulting dialog, select the *New Monitor Dashboard* option.



A new tabbed design area in the central part of the user interface will be created.

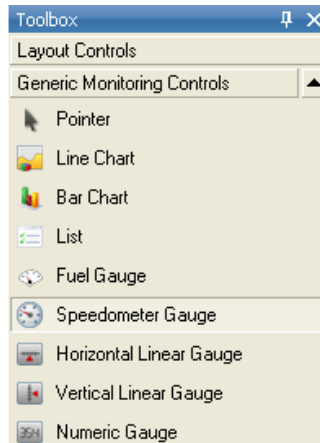


The main area used in Design mode is a graphical workspace for defining the appearance of a dashboard. The *Toolbox* to the right is used to define new controls in the dashboard along with their *Properties*.

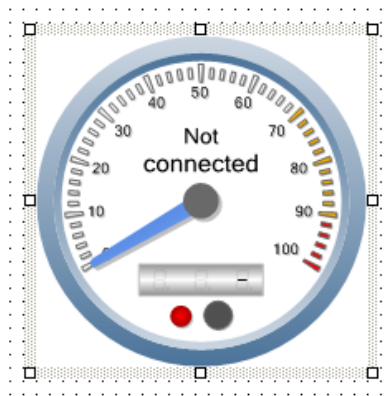
Monitoring controls may be added, moved around, resized, grouped together and annotated on the dashboard. Using the tabs at the top of the editing area, several dashboards can also be edited simultaneously and Monitoring controls can be cut and pasted between them.

Monitoring Controls

InControl provides a range of Monitoring controls in different styles. Any style can be used to measure a CorePlus parameter and it is up to the administrator to decide the style that best suits their presentation needs. If it's preferable to have a single control monitor more than one parameter, a Bar Chart, Line Chart or List control can be used. Otherwise a Gauge control may be the most appropriate.



By selecting the *Speedometer Gauge* from the control list and then dragging out a rectangle on the editor area to define the control's size, a *Speedometer Gauge* like the one below will be added to the dashboard editor area. Alternatively, it's possible to drag the control from the Toolbox menu directly into the editor window, in which case a standard size is used for the control.




All Monitoring control styles can be scaled to a smaller or larger size by dragging their edges at the marked points and their positions can be changed by dragging their borders.



Note

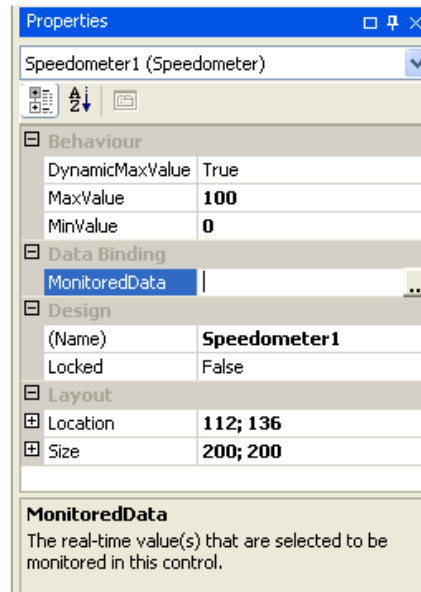
The text "**Not Connected**" appears in the control to indicate that a Clavister Security Gateway and the CorePlus parameter it will monitor on that gateway have not yet been selected for the control.

Cursor Styles

The editor cursor shows a crosshairs style when the mouse is to be dragged to define a new Monitor control. To switch out of this mode select the **Pointer** option, indicated with the  icon.

Monitoring Control Properties

Once selected, any of the *Properties* of this control can be set using the Properties display shown below:



For each control, both the lower and maximum value of the monitored quantity can be specified. For some controls that can monitor several parameters, such as a Bar Chart or List, several parameters can be defined and the parameters can be for different Clavister Security Gateways.

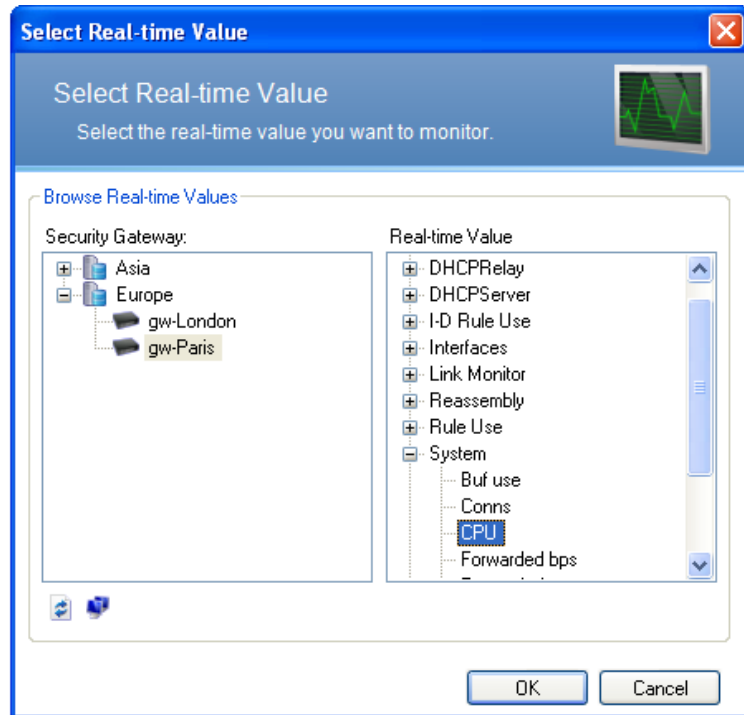
Dynamic Maximums

Sometimes it can be difficult to predict the maximum value of a parameter and if this is the case then the *Dynamic Maximum Value* can be set to **True**. This will mean that the control will extend its range and repaint itself automatically if the upper limit is exceeded (conversely it will reduce its range if the value falls back below the upper limit).

The Data Binding

One of the Properties that must be set for a control to perform monitoring is the *Data Binding*. This is the combination of a Clavister Security Gateway plus the CorePlus parameter within that gateway that is to be monitored.

Selecting the Data Binding property will cause the dialog shown below to appear. On the left of the dialog are the Clavister Security Gateways which have been located automatically by InControl, on the right are the individual CorePlus parameters which can be monitored in each gateway.



Once the control is associated with a parameter, the parameter's name will appear on the control as shown below.



Note

CorePlus provides a extensive set of parameters which can be monitored. If a Monitoring control is not associated with one of these CorePlus parameters it won't do anything in Monitor mode.

Changing Design Mode to Monitor Mode

In order to have a dashboard become "live" and start monitoring Clavister Security Gateways, it is necessary to switch from *Design Mode* to *Monitor Mode*. The *Design Mode* option in the View menu acts as a toggle between the two modes.



Tip

Toggling between the modes can also be done with the **F5** function key.

As soon as Monitor mode is switched on, the currently displayed dashboard will appear as a live display and begin showing actual values.

Adding Text Captions

Text Captions can be placed anywhere in a dashboard and can contain either text or an image. Their purpose is purely cosmetic and they provide a means to add helpful annotations or graphics such as a company logo to a dashboard. Like Monitoring controls, their size can be dragged larger or smaller, and properties such as the font can be changed.

Defining a Group

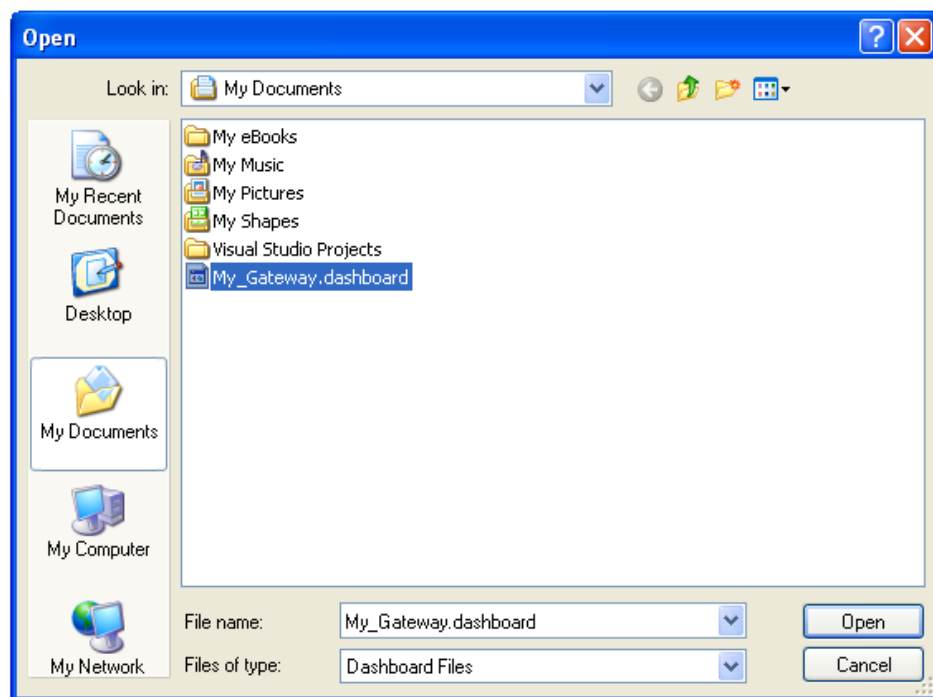
A *Group* is a display area that has a textual caption and several related controls can be placed into a Group's display area. By dragging its corners, a Group display area can be made smaller or bigger. A Group can be similarly dragged around the overall dashboard display area and when this is done all the controls it contains will be dragged with it.

Using Themes

The look and feel of a dashboard or the individual components can often be set by selecting a *Theme*. Themes are purely cosmetic and provide a way to get a color scheme that suits the user.

Saving a Dashboard

Once a dashboard has been created, it can be saved with a user defined name into a file with filetype *.dashboard* anywhere in the file system. Once saved, it can be opened at any time by selecting the *Open* function in the *File* menu and then selecting the dashboard file in a filechooser dialog.



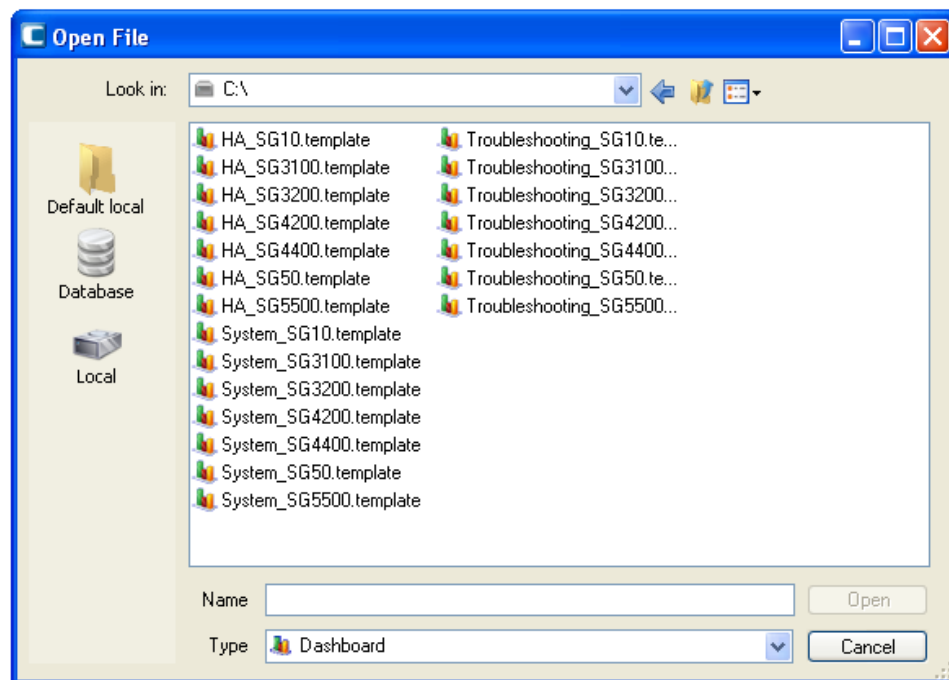
Alternatively, double clicking a **.dashboard** file from Windows will open the dashboard in monitoring mode.

Using Dashboard Templates

The quickest and easiest way to create a dashboard is to select an existing *Dashboard Template*.

Templates are pre-defined dashboards that are already included with InControl and that with pre-defined layouts of Monitoring controls are already connected to a set of parameters. They are designed to provide a quick and easy way to begin monitoring without having to spend time creating a dashboard from scratch.

Dashboard Templates are stored as files and have the filetype **.template**. When selecting **New Dashboard From Template** in the menu the following dialog is displayed.

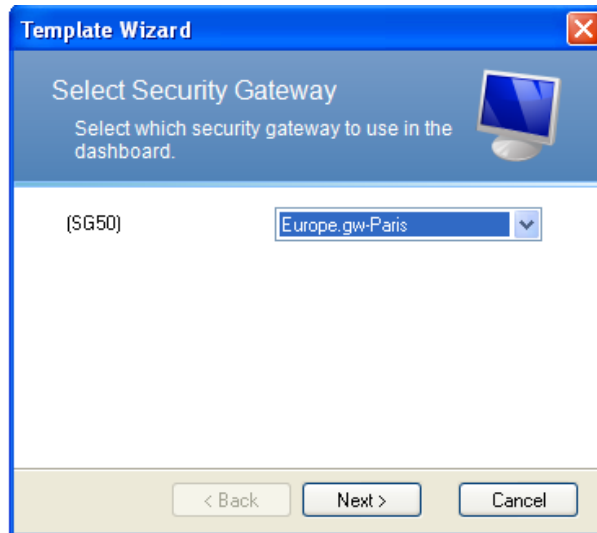


Alternatively, an external template file can be selected by double clicking the file in the Windows file explorer.

The three groups of templates available are:

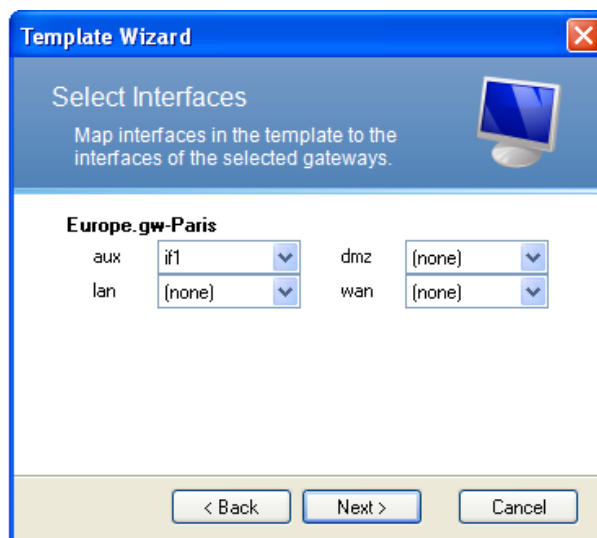
- **System** - A general dashboard suitable for each Clavister Hardware Series.
- **Troubleshooting** - Dashboards designed to help identify problems.
- **HA Cluster** - A dashboard suitable only for High Availability Clusters.

After selection, a template still lacks connection to a Clavister Security Gateway and to define this, the following dialog appears.



In this dialog "**(SG50)**" must be replaced by one of the available Clavister Security Gateways shown in the drop-down box in the right part of the dialog. In this case *Europe.gw-Paris* might be the selected gateway.

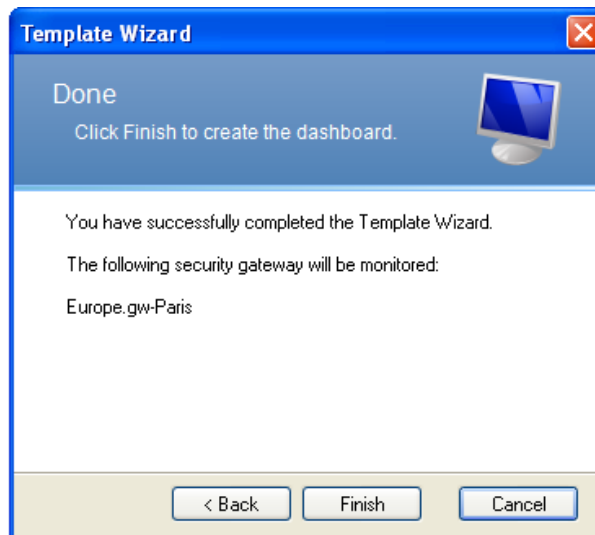
Once the appropriate Clavister Security Gateway is selected there may still be a mismatch between the individual values monitored in the Template and the values in the gateway. These mismatched values are resolved in the following steps.



If the names of the physical interfaces of the gateway have been changed from the default ones in the configuration it is necessary to select which name to use for each interface in the Template.

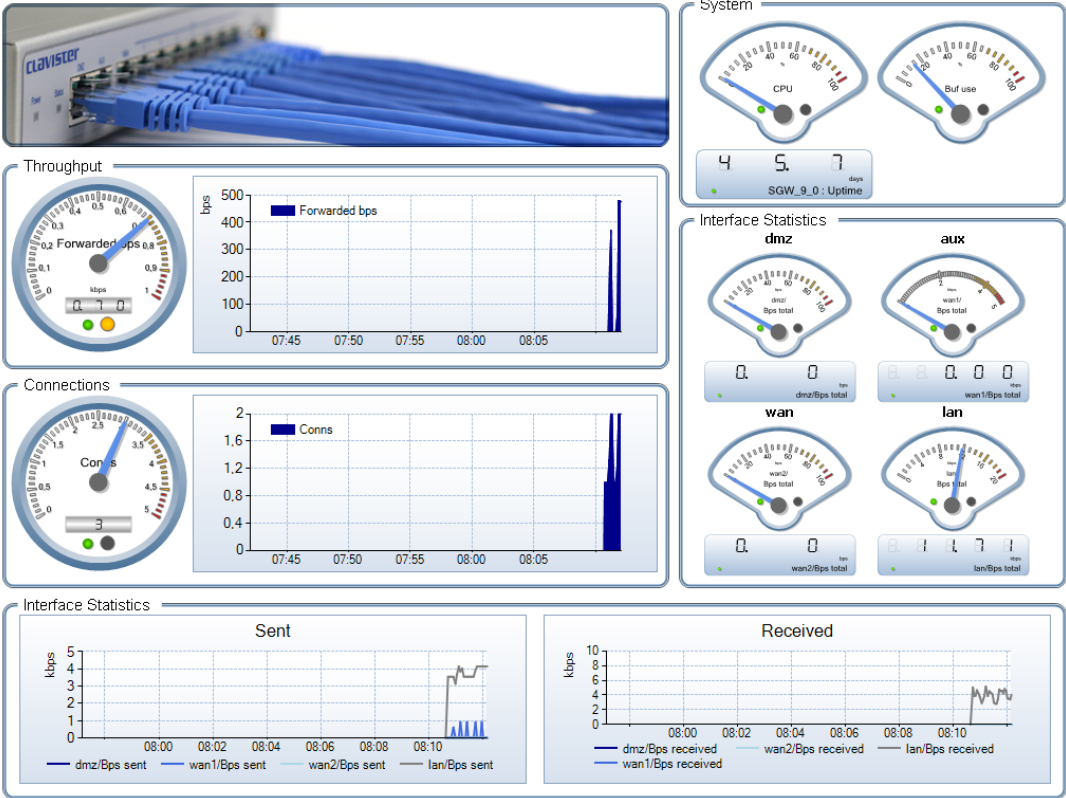


Some Templates use hardware monitoring counters that show values collected from sensors in the Clavister Security Gateway. If these sensors have been configured in the gateway, they can be selected in the next step of the wizard.



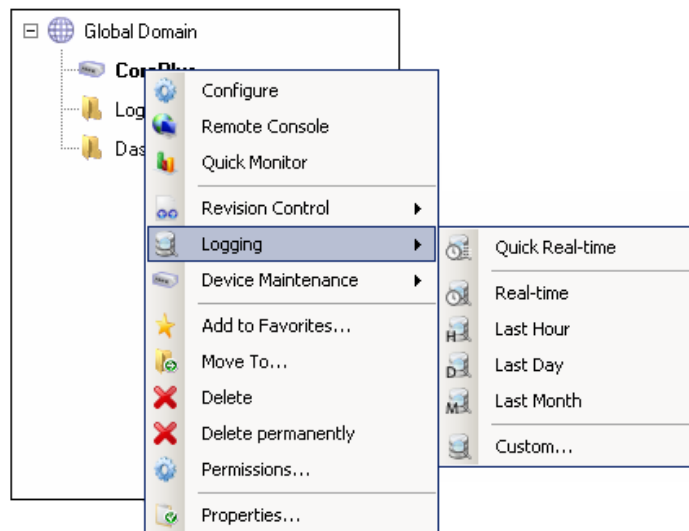
The Template is now opened and can be used as a normal dashboard as well as being able to be saved to a new dashboard file.

The following image illustrates a dashboard that comes from a template.



Chapter 15: Log Monitoring

It is possible in InControl to open a tab which displays, in real-time, the log messages generated by CorePlus. This is done by right clicking the security gateway of interest and selecting the *Logging* option followed by the *Quick Real-time* option in the submenu as shown below:



A tab is then opened with the same name as the security gateway and the log messages are displayed in real-time. An example of this is shown below:



```

Start Page Dashboard* CorePlus
CONN: id=00600004 rev=1 event=conn_open_natsat rule=NAT_DNS conn=open connipproto=UDP connrecvif=lan
connsrrip=192.168.1.2 connsrport=1025 conndestif=wan conndestip=194.165.224.190 conndestport=53
connnewsrrip=10.4.4.22 connnewsrport=3539 connnewdestip=194.165.224.190 connnewdestport=53
CONN: id=00600004 rev=1 event=conn_open_natsat rule=NAT_All conn=open connipproto=TCP connrecvif=lan
connsrrip=192.168.1.2 connsrport=1790 conndestif=wan conndestip=209.85.129.104 conndestport=80
connnewsrrip=10.4.4.22 connnewsrport=3188 connnewdestip=209.85.129.104 connnewdestport=80
CONN: id=00600001 rev=1 event=conn_open rule=NetconBeforeRules conn=open connipproto=UDP
connrecvif=lan connsrrip=192.168.1.2 connsrport=1791 conndestif=core conndestip=192.168.1.1 conndestport=
999
CONN: id=00600002 rev=1 event=conn_close action=close rule=NetconBeforeRules conn=close connipproto=UDP
connrecvif=lan connsrrip=192.168.1.2 connsrport=1785 conndestif=core conndestip=192.168.1.1 conndestport=
999 orisnt=124 termsent=0
CONN: id=00600001 rev=1 event=conn_open rule=Ping conn=open connipproto=IGMP connrecvif=wan connsrrip=
10.4.0.241 connsrport=0 conndestif=core conndestip=239.255.255.100 conndestid=0
IP_PROTO: id=07000014 rev=1 event=ttl_low action=drop ttl=1 ttlmin=3 rule=TTLonLowMulticast recvif=wan srrip=
10.4.4.106 destip=239.192.83.80 ipproto=UDP ipdatalen=40 srport=21328 destport=21328 udptotlen=40
CONN: id=00600002 rev=1 event=conn_close action=close rule=Ping conn=close connipproto=IGMP
connrecvif=wan connsrrip=10.4.0.241 connsrport=0 conndestif=core conndestip=239.255.255.100 conndestid=0
orisnt=28 termsent=0
CONN: id=00600001 rev=1 event=conn_open rule=NetconBeforeRules conn=open connipproto=UDP
connrecvif=lan connsrrip=192.168.1.2 connsrport=1793 conndestif=core conndestip=192.168.1.1 conndestport=
999
CONN: id=00600002 rev=1 event=conn_close action=close rule=NetconBeforeRules conn=close connipproto=UDP
connrecvif=lan connsrrip=192.168.1.2 connsrport=1786 conndestif=core conndestip=192.168.1.1 conndestport=
999 orisnt=124 termsent=0
IP_PROTO: id=07000014 rev=1 event=ttl_low action=drop ttl=1 ttlmin=3 rule=TTLonLowMulticast recvif=wan srrip=
10.4.4.212 destip=239.255.255.250 ipproto=UDP ipdatalen=109 srport=1711 destport=1900 udptotlen=109

```

This output reflects the log messages that are being stored in the *Memlog* which are the messages saved in the security gateway's local memory.

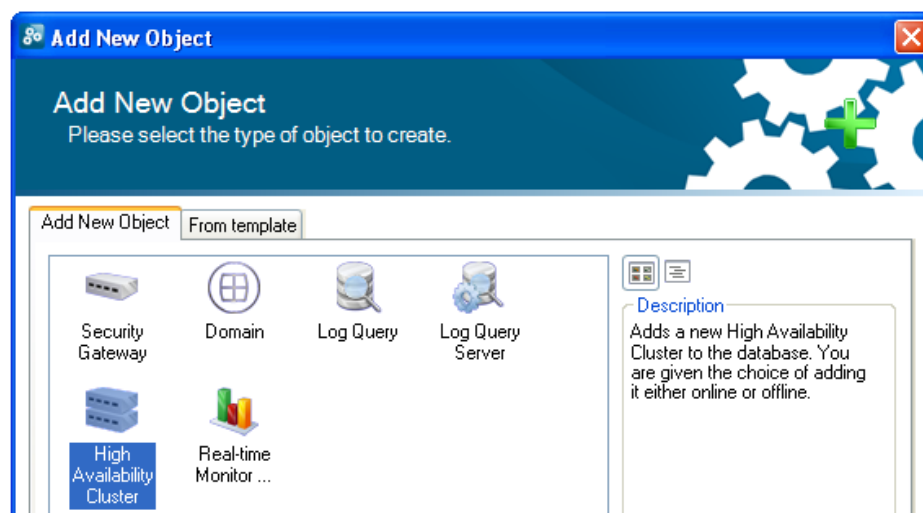
Chapter 16: High Availability

CorePlus *High Availability* allows two Clavister Security Gateways, a *master* and a *slave unit*, to operate as a single security gateway in an *HA cluster*. If the master unit ceases to function, the slave will detect this and a *fail over* occurs in which the slave takes over the master's functions. This implements hardware redundancy and provides extremely high system availability. HA is more fully explained in the *CorePlus Administrators Guide*.

An HA cluster can easily be set up in InControl and does not require great effort by the administrator.

Creating a New HA Cluster

To create a new HA cluster, the administrator should first create an *HA cluster* object using the *New* option in the InControl *File* menu.



The *HA Cluster* wizard will start and the cluster can be defined. The screenshot below shows the wizard step where the cluster name and method of deploying configurations to the cluster can be set.

The configuration deployment options are:

- **Nodes are kept synchronized**

With this option InControl uploads a new configuration to first one and, after a delay, to the second unit. When deployment is initiated by the administrator, InControl asks which gateway should be deployed to first using the dialog shown below.

Deploying first to the inactive node means that there will be a minimum of service interruptions since only one failover is required. Deploying to the active node first means that there is an increased interruption to traffic since more than one failover is required but also means that the currently active unit remains the active unit after deployment.

The time delay before uploading to the second unit can also be selected (deploying to both gateways at the same time should never happen).

- **Automatic synchronization**

With this option, a new configuration is uploaded to just one of the security gateways in the cluster and the gateways themselves then share and synchronize the new configuration. The administrator can select the security gateway for deployment.

When this option is selected, the *Sync* flag of the cluster is set to *Enabled* and it cannot then

be changed through any management interface.

- **Manually**

This option means that the administrator has complete control over configuration deployment and must explicitly deploy the configuration to each security gateway in a cluster before both have the same configuration. The administrator manually deploys a new configuration to one gateway and then does the same to the other.

The deployment option chosen can be changed later in the *Properties* dialog for the cluster tree node.

Adding Gateways to the Cluster

Once the HA cluster object is created, security gateways can be added to the cluster by:

- Adding an existing security gateway to the cluster. This can be done by simply dragging the gateway's node in the navigation tree and dropping it into the cluster node.

OR

- Define the new gateway with the new gateway wizard and add it to the cluster in the wizard.

Selecting the Master and Slave

Although the two security gateway in an HA cluster are peers, CorePlus designates one to be the *master* gateway and the other to be the *slave*. With InControl, the first security gateway added becomes the *master* unit and the second added becomes the *slave*.

Matching Interfaces and Selecting Sync

Whenever a second security gateway is added to an HA cluster, the wizard asks the administrator to match interfaces and to select the interfaces on each unit which will be the *sync* interface.

The *Sync* interface on the master and slave in an HA cluster are used to synchronize the two Clavister Security Gateways. Only one matching interface on each unit is chosen to be the *Sync* and is dedicated to this purpose. The *CorePlus Administrators Guide* should be consulted for a full explanation of *Sync* interface operation.

Adding an Existing HA Cluster to InControl

If a security gateway is already configured to be part of an HA cluster outside of InControl then it is possible to add the cluster so it can then be managed By InControl.

To add an existing cluster to InControl, the following actions should be performed:

1. Create a new HA cluster object in InControl.
2. For this new cluster object, select the action **Add New Node > New Security Gateway** and add the security gateway which is configured as the *master* unit in the original cluster.



Important

The master must be added to the InControl cluster object first.

3. Repeat the above step but this time add the security gateway which is the *slave* in the original cluster.

Removing a Gateway from a Cluster

To remove a gateway from a cluster is simply a matter of dragging the gateway in the InControl navigation tree out of the HA cluster object. When it is disconnected, it automatically reverts to a standalone unit.

Wizard Finalization

When the HA wizard completes a summary of the final HA cluster configuration is displayed, as shown in the screenshot below:

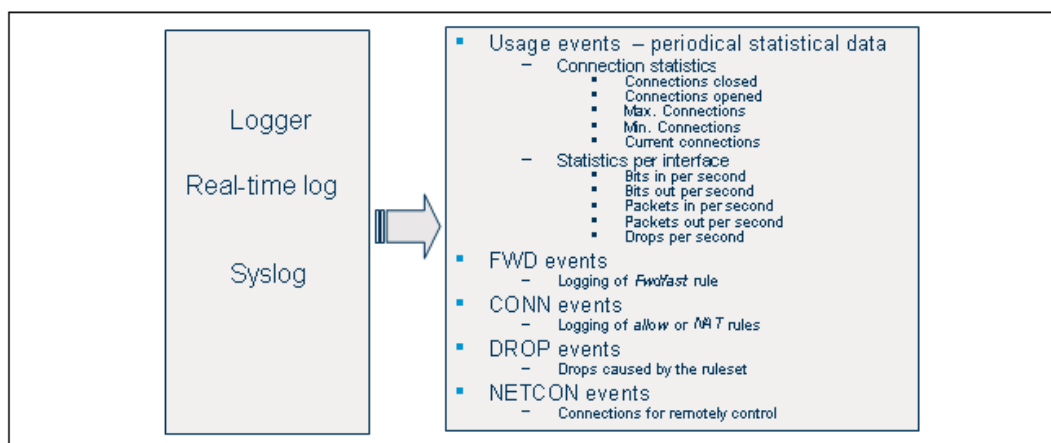
Name	HA_Cluster	Created	2009-04-28 16:18
Parent object	Global Domain	Version	9.10
Sync mode	InControl keeps the node configurations synchronized (deploys to both)		
Comments	Virtual CorePlus		

Open Configuration tab on successful add

< Back Finish Cancel

Chapter 17: The Log Query Server

The complete CorePlus logging features are more fully described in the *CorePlus Administrators Guide*. These features are summarized in the diagram below.



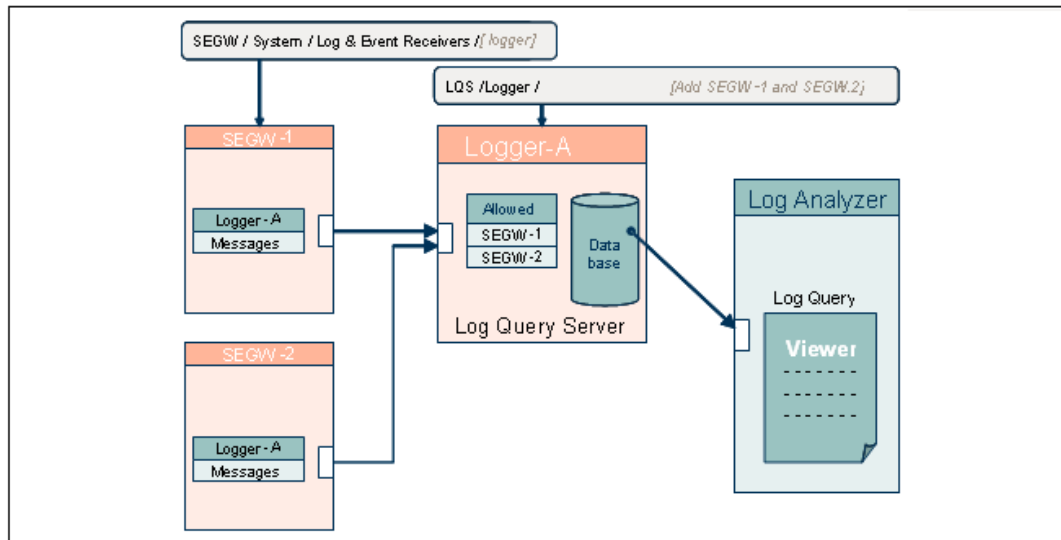
This chapter examines the log analysis capabilities of the proprietary Clavister *Log Query Server*.

FWLogger and LQS

The *FWLogger* database is a Clavister proprietary log server database. It stores log messages in its own format and a query feature called the *Log Query Server* (LQS) is provided which can be accessed through the InControl interface.

Log Analysis

The arrangement of the *FWLogger* database, LQS and InControl access is illustrated below.



Installation

The FWlogger database and LQS are installed by default with the standard InControl server installation. It is possible, however, to specify to the installation wizard that only the logging software is to be installed or that InControl is to be installed without the logging software.

The logging software can therefore be installed on the same PC as the InControl server or on a different PC. More than one installation can be fed by messages coming from a Clavister Security Gateway. In the example used here, only one logging installation is used and it is installed on the same PC as the InControl server.



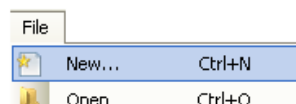
Note

The LQS must be installed on the same PC that is used for storing the FWLogger database.

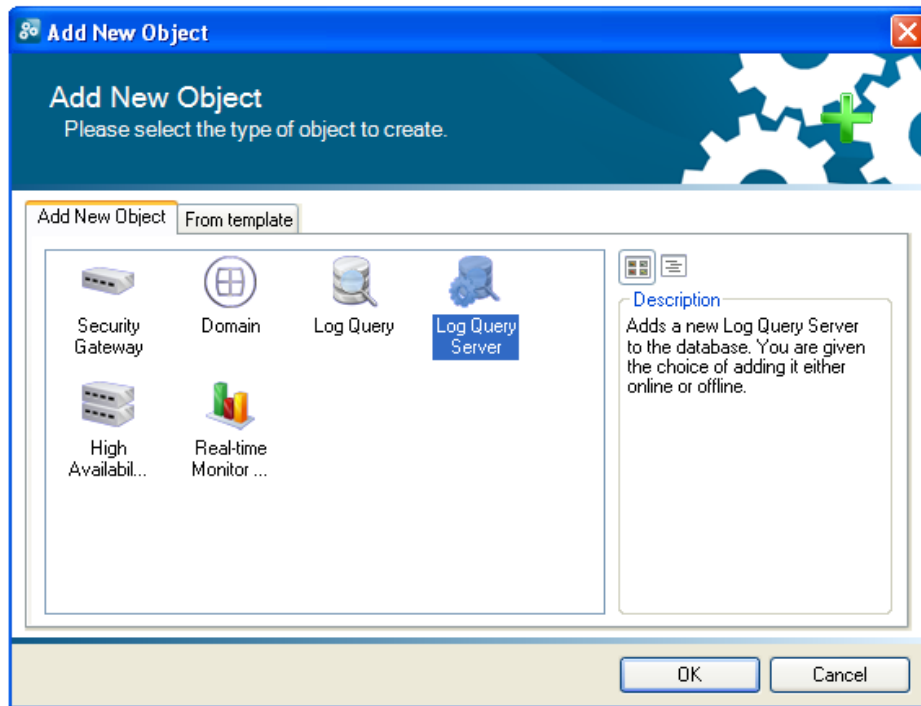
Using LQS

LQS runs as a windows service and will start automatically after installation.

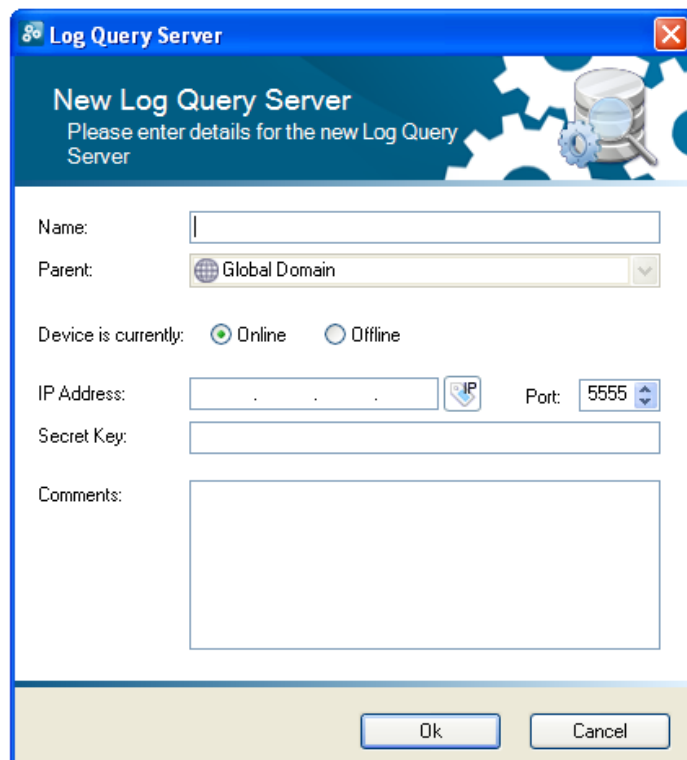
To be able to use the LQS it must be first added to the *Global Domain* of the InControl client. First open the *Add New Object* dialog by selecting the **New** option in the **File** menu.



Select the *Log Query Server* object in the *Add New Object* dialog.



The *New Log Query Server* wizard will start.



The *Secret Key* in the above dialog is the NetCon key used for the communication between InControl and LQS. This key can be found in the file in the InControl installation directory and has the parameter name *SharedKey*. This key needs to be copied and pasted into the key field in the dialog. An example of how the key appears in the *Lqs.xml* file is shown below:

```
SharedKey="DBC2A65220E2D3753149EDED524FC1A140CDA6810FA68E2A78FCD2684A04
8A708A1D97B6B10BE90FD52AA39634830E1EEE1F406B812CC550EB CDDCC447307C8E"
```

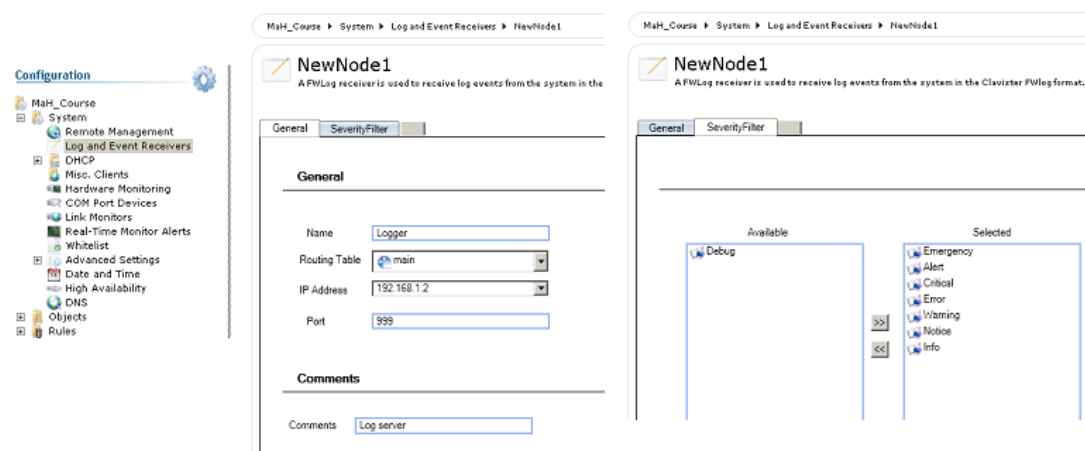
If LQS is running on the same PC as InControl, the IP address for access is *127.0.0.1*.

4. The *Log receiver location* should be the same as the directory for the *logger.exe* executable.
5. Add one or more Clavister Security Gateways to the logger.

The added list contains the Clavister Security Gateways from which messages will be stored in the logger database.

Configure the Clavister Security Gateways for Logging

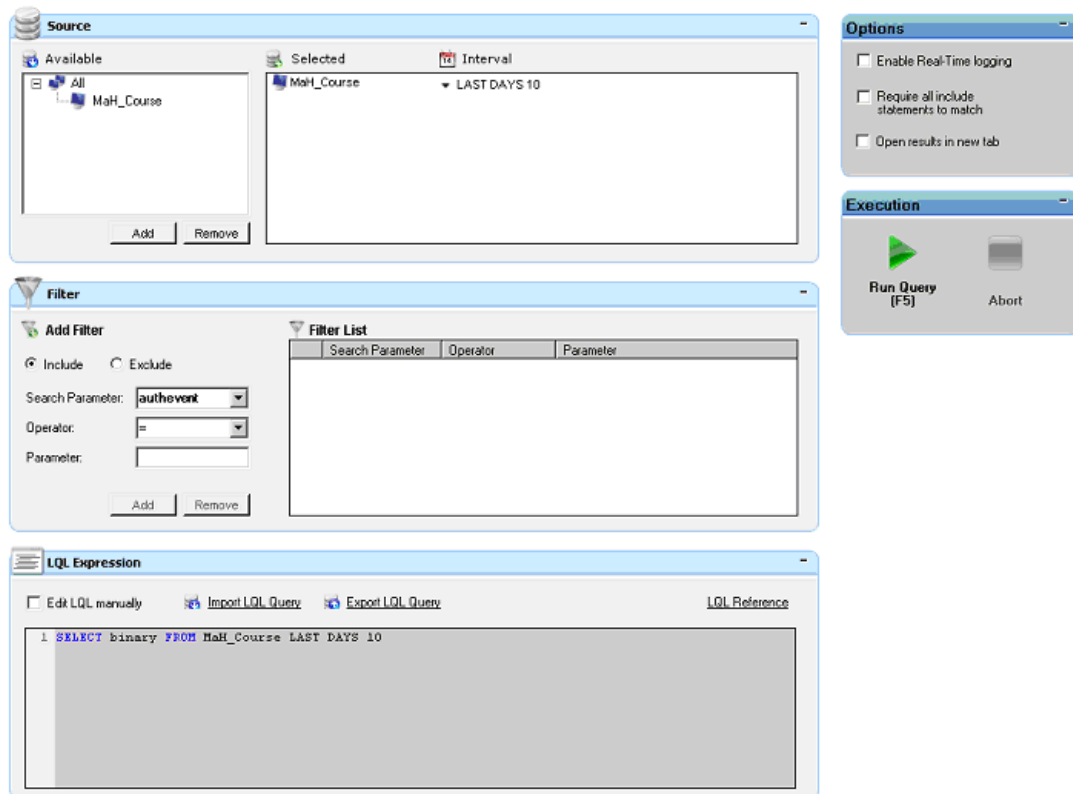
Each Clavister Security Gateway must now be configured with entries that specifies which loggers to send messages to and which messages to send. Below is the dialog to define a log receiver.



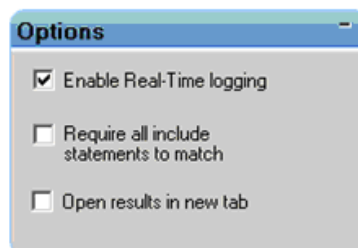
Here, the IP address of the logger is specified and a name if given. Syslog servers may also be specified. A maximum of 8 log servers can be specified.

Running the Log Analyser

Select the menu option **Tasks > Run Log Query** to open the log analyzer.



The *Source* is the Clavister Security Gateway is question and this must be selected. Several types of filtering are possible. Real-time log message output can also be activated.



Below is a typical example of log analyzer output.

Results								
Time	Device Time	Name	Message ID	Rule	Severity	Category	Event	Action
2008-10-23 16:05:39	2008-10-23 16:05:31	MaH_Course	02300001		Info	NETCON	init_complete	
2008-10-23 16:05:39	2008-10-23 16:05:31	MaH_Course	03202000		Notice	SYSTEM	startup_normal	
2008-10-23 16:05:41	2008-10-23 16:05:33	MaH_Course	00600001	NetconBeforeRules	Info	CONN	conn_open	
2008-10-23 16:05:41	2008-10-23 16:05:33	MaH_Course	02300503		Notice	NETCON	netcon_connect	
2008-10-23 16:05:41	2008-10-23 16:05:33	MaH_Course	03200607		Notice	SYSTEM	bidr_ok	
2008-10-23 16:05:41	2008-10-23 16:05:33	MaH_Course	02300504		Notice	NETCON	netcon_disconnect	
2008-10-23 16:05:41	2008-10-23 16:05:33	MaH_Course	00600002	NetconBeforeRules	Info	CONN	conn_close	close
2008-10-23 16:05:44	2008-10-23 16:05:36	MaH_Course	03202001		Notice	SYSTEM	startup_echo	
2008-10-23 16:05:46	2008-10-23 16:05:38	MaH_Course	06000060	LocalUndelivered	Notice	RULE	unhandled_local	drop
2008-10-23 16:05:50	2008-10-23 16:05:42	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:05:50	2008-10-23 16:05:42	MaH_Course	06000060	LocalUndelivered	Notice	RULE	unhandled_local	drop
2008-10-23 16:05:55	2008-10-23 16:05:46	MaH_Course	03202001		Notice	SYSTEM	startup_echo	
2008-10-23 16:06:58	2008-10-23 16:06:50	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:07:00	2008-10-23 16:06:52	MaH_Course	00600002	NetconBeforeRules	Info	CONN	conn_close	close
2008-10-23 16:08:07	2008-10-23 16:07:58	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:09:15	2008-10-23 16:09:07	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:10:23	2008-10-23 16:10:15	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:11:31	2008-10-23 16:11:23	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:12:40	2008-10-23 16:12:31	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop
2008-10-23 16:13:49	2008-10-23 16:13:41	MaH_Course	06000051	Default_Access_Rule	Warning	RULE	ruleset_drop_pack	drop

Record 1 of 234

Event Details | Packet Dump | References

Chapter 18: Remote Management

The NetCon Protocol

All remote management of Clavister Security Gateways, including configuration, monitoring and upgrades by InControl is secured through 128-bit encryption and authentication. The protocol used for the remote management is called *NetCon*, and is based on the CAST128 encryption algorithm. The NetCon protocol uses both TCP and UDP as a transport protocol on destination port 999.

The NetCon protocol is not used when accessing a Clavister Security Gateway through the Web Interface using a web browser.

NetCon Management Keys

NetCon uses a pair of pre-shared keys for NetCon authentication. These *Remote Management Keys* are unique for each Clavister Security Gateway, and are generated using a strong cryptographic number generator when a new Clavister Security Gateway is initially configured using the Web Interface.

Preconditions for InControl Access

To be able to access a Clavister Security Gateway from InControl, there are 3 requirements:

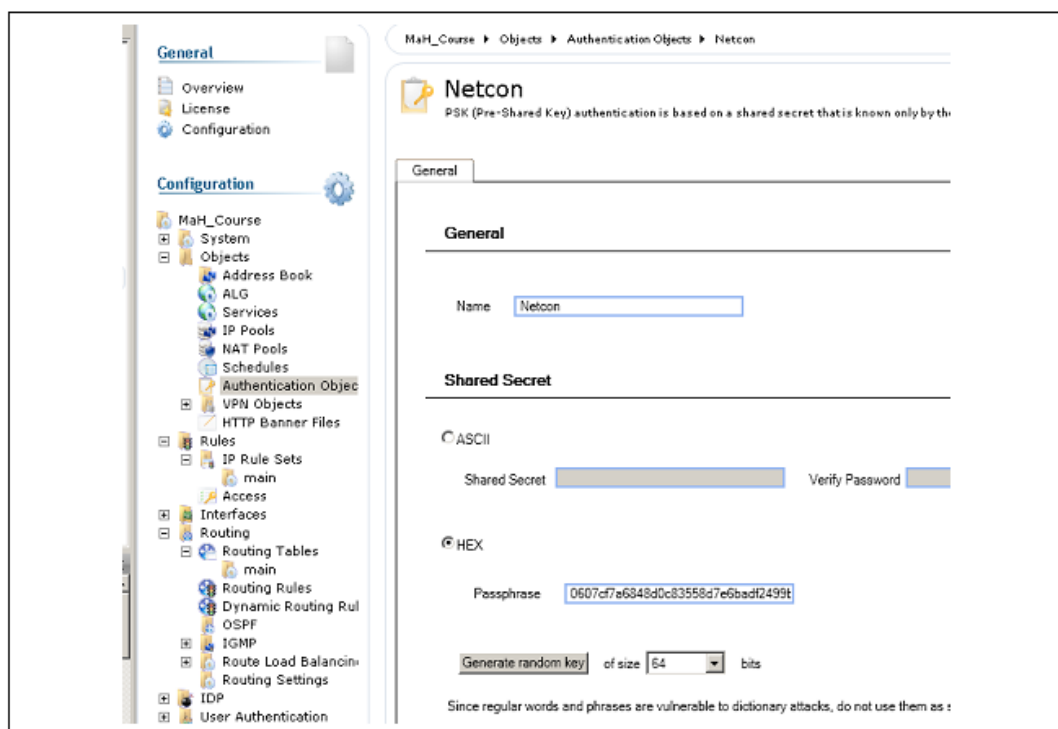
1. The NetCon Remote Management Keys of the Clavister Security Gateway have to be entered into InControl. These are retrieved using the Web Interface as described in Appendix A, *NetCon Key Generation*.
2. The PC running the InControl server has to belong to a network that has been granted administration rights.
3. The NetCon connections from the InControl server to the Clavister Security Gateway have to be received on a specific interface on the gateway.

Management Keys Storage

The NetCon management keys are stored on the InControl server PC in the file `Server > db > Data > ics_data.xml`.

It is much simpler to access the keys through the InControl client by going to: **Objects >**

Authentication Objects > NetCon. Shown below is the dialog displayed.



Changing NetCon Management Keys

Once communication with a Clavister Security Gateway is established from InControl, the NetCon keys can be changed by going to: **Tasks > Change Management Keys.**

Levels of Access Permissions

There are three levels of access to the Clavister Security Gateway which can be granted to other InControl clients. These are:

- **Configure**
This is the highest level and at least one client should always have this access since it allows full control of a Clavister Security Gateway.
- **Console**
This level allows only CLI access.
- **Uptime Poll**
This level allows the Clavister Security Gateway to be polled to check that it is alive.

Access permissions are set using the InControl dialog shown below. The *Access Filter* settings determine from which network and interface access is allowed.

The screenshot displays a network configuration interface. On the left is a 'Configuration' tree with a gear icon at the top. The tree is expanded to show 'System' > 'Remote Management'. The right pane is titled 'General' and contains the following settings:

- General**
 - Mode:
 - Idle timeout:
 - PSK:
- Access Filter**
 - Remote access is granted from the following interface and network.
 - Interface:
 - Network:
- Comments**
 - Comments:

Chapter 19: Certificate Requests

Some security features in CorePlus require the use of X.509 certificates. For instance, this is one of the ways of securely setting up VPN tunnels based on IPsec.

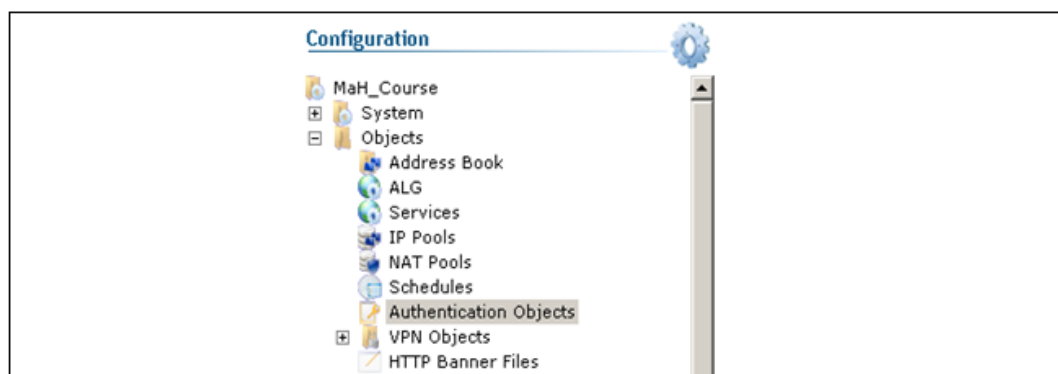
One of the ways to receive certificates from a *Certification Authority* (CA) is to send the CA a *certificate request* and InControl provides a feature to generate these requests. The certificate received can also be imported and deployed to the Clavister Security Gateway through InControl.

The sequence of steps with certificates is:

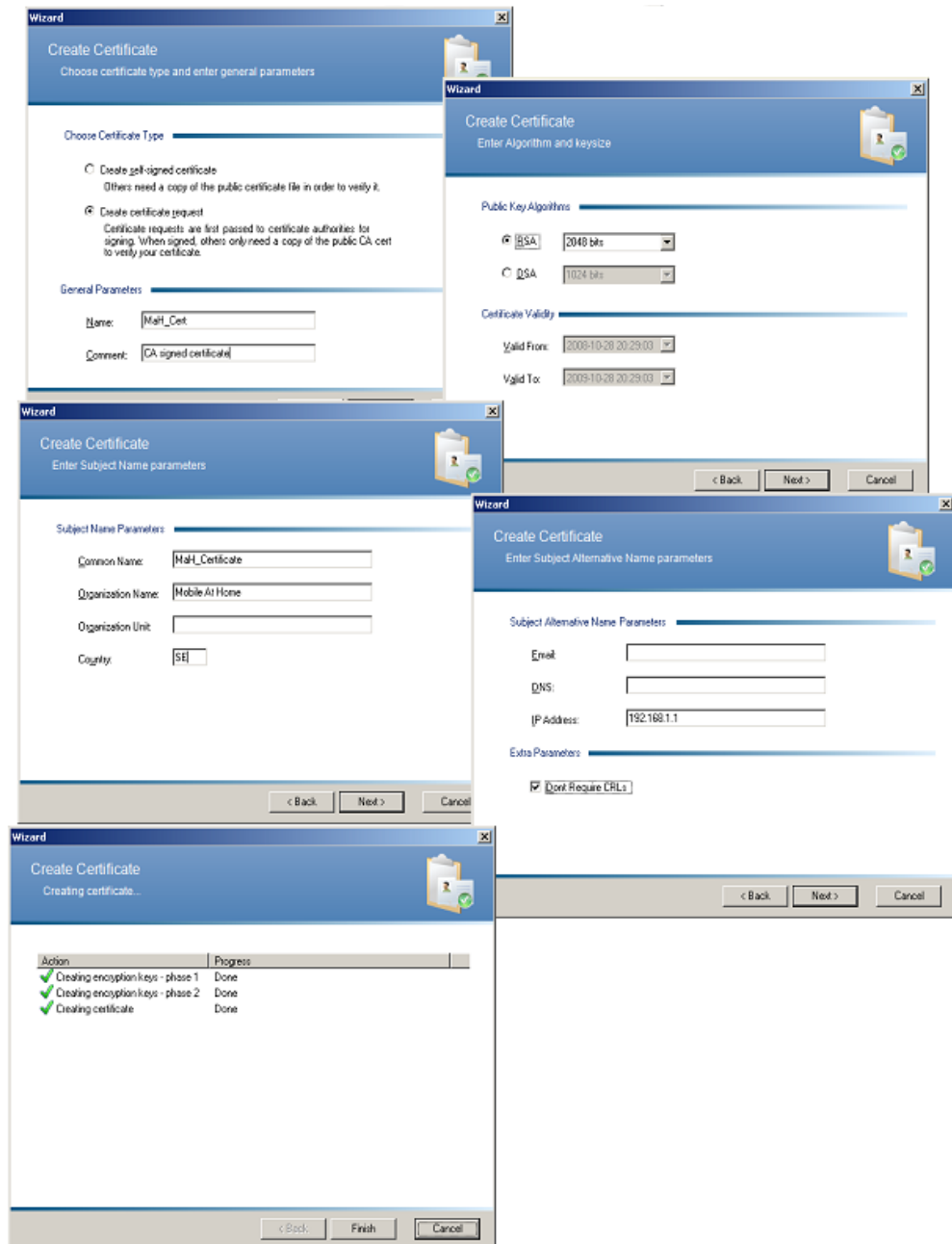
1. Create a certificate request.
2. Export and send the request to the CA.
3. Import the certificate sent by the CA.
4. Associate the certificate with a VPN tunnel.

1. Create a certificate request

To do this, go to: **Objects > Authentication Objects > Add > Certificate**. Choose **Create New** which will activate a wizard to create the certificate request.



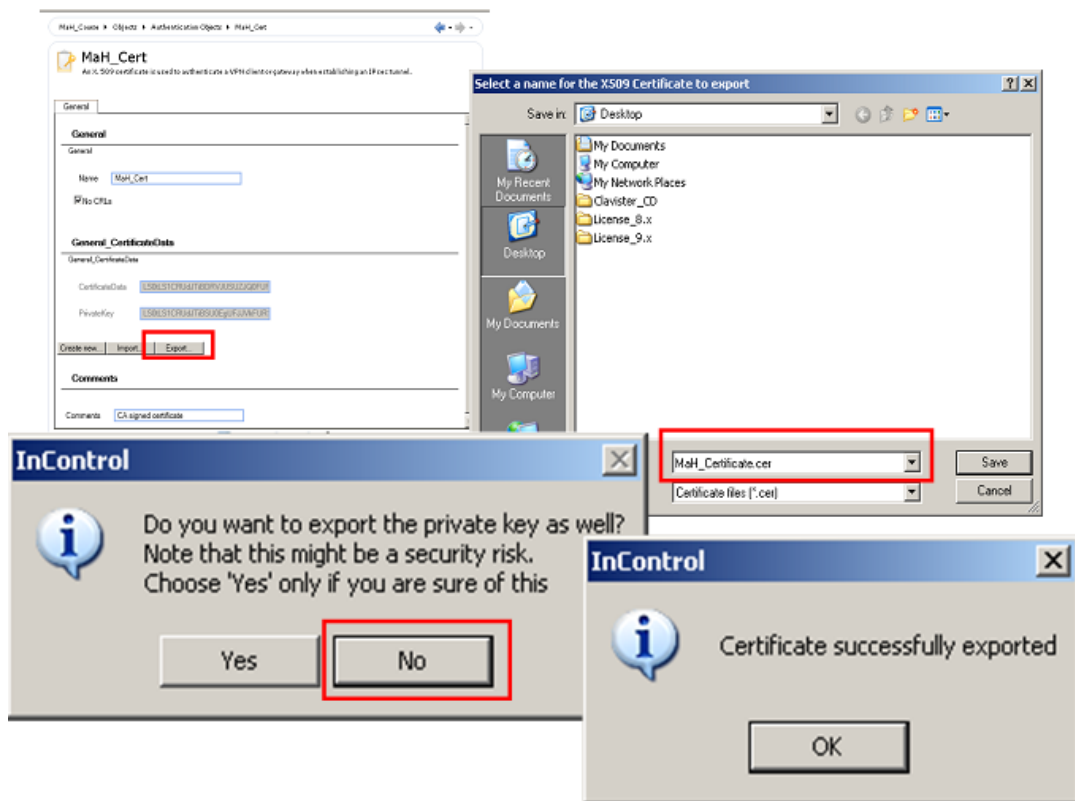
Follow the wizard steps as illustrated in the composite image below.



2. Export and send the request to the CA

To export the request, first create a new folder on the InControl client workstation called, for example, *Certificate Request*. Now click the **Export** button in the certificate properties dialog.

Answer *No* when asked if the certificate should include the private key. The private key should not be included since this should never be transmitted to third parties. The dialog sequence is illustrated below.

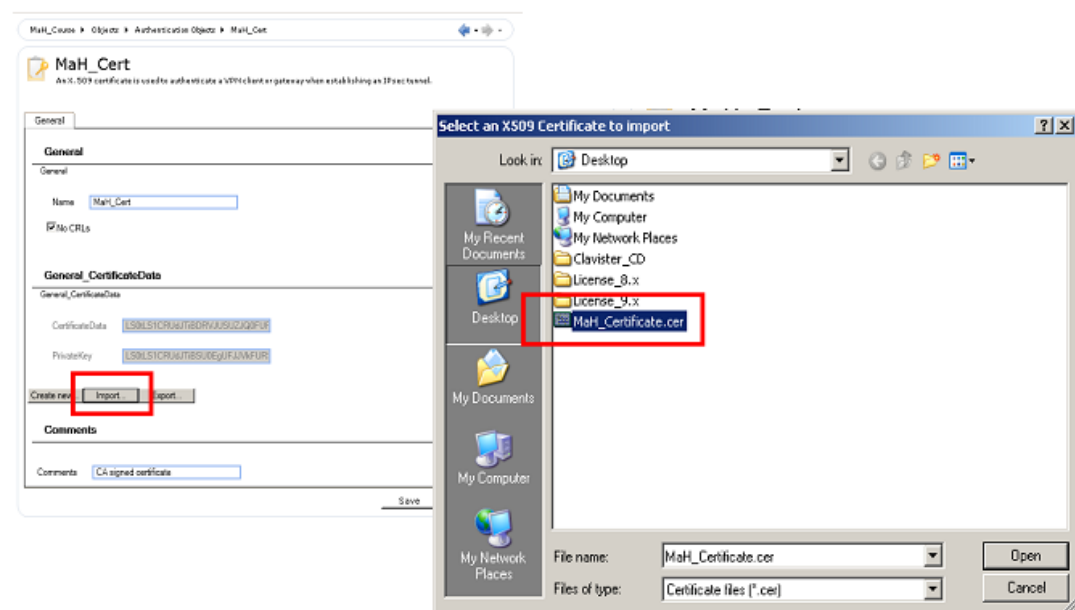


After generating the request file, the filetype extension of the file should be set to *.req* before it is sent to the CA.

3. Import the certificate sent by the CA

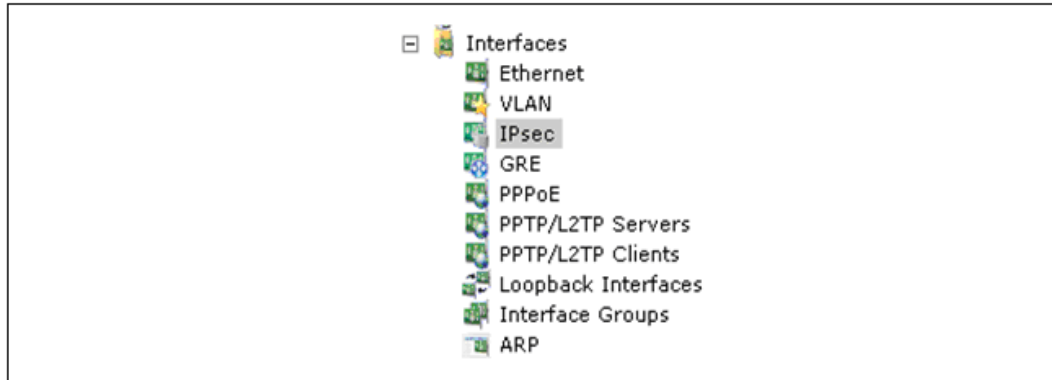
The CA will send back the server certificate (gateway certificate). Store this in the *Certificate Request* folder created previously.

Now import the certificate into InControl. Screenshots of example dialogs are shown below.

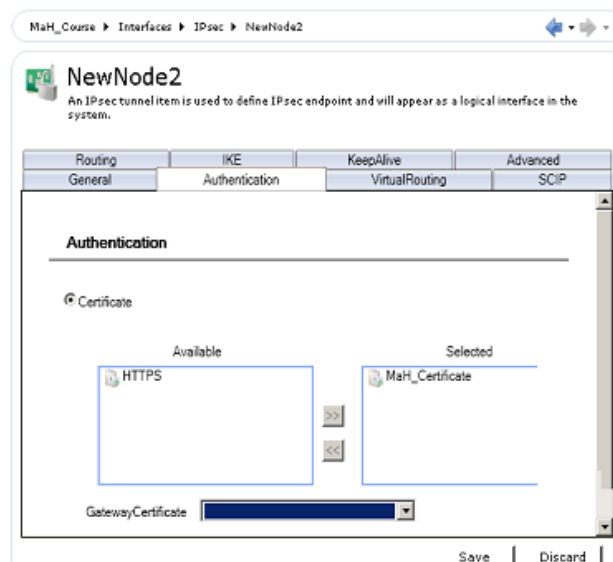


4. Associate the certificate with a VPN tunnel

The final step is to associate a certificate with a VPN tunnel. With IPsec, this is done by opening the *IPsec Tunnel Properties* as shown below.



Now add the certificate from the *Available* list to the *Selected* list.



Using an Internal CA

A certificate request can be sent to an internal CA. The Windows server series includes a internal CA server in many versions and this can be used to generated the certificate from the CA request.

Chapter 20: Importing FineTune Datasources

When upgrading an 8.nn CorePlus system to a 9.nn system that will be administered with InControl, there are two possible approaches:

- Use the standalone CorePlus upgrade wizard program to upgrade to a 9.nn version and then define the upgraded security gateway to InControl. Wizard usage is described in the separate manual called *8.nn to 9.nn Migration Guide*.
- Import and upgrade the security gateway directly from within InControl.

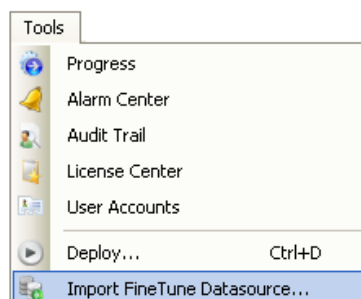
As discussed previously in *Chapter 2, Installing InControl*, the recommended method when using InControl is the second, and this is done within InControl in two distinct steps:

- Define the security gateway within InControl by importing the old configuration data from the 8.nn FineTune datasources.
- Still within InControl, upgrade the CorePlus version of the newly defined security gateway to a 9.nn version.

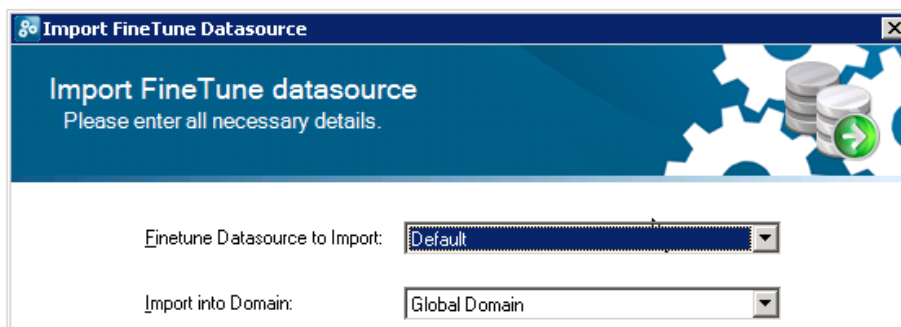
These two steps are discussed in detail next.

Importing Datasources

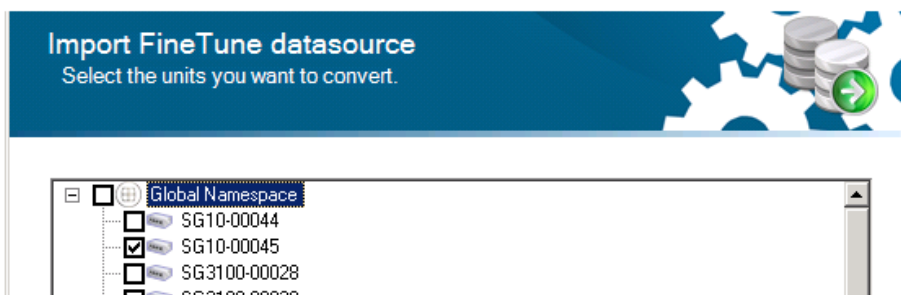
This is done by choosing the InControl menu option **Tools > Import FineTune Datasources**.



Choosing this option starts a simple three step wizard which lists all the datasources found on the local PC and allows importation of the configurations selected by the administrator. First of all, the wizard asks for the datasource to be identified.

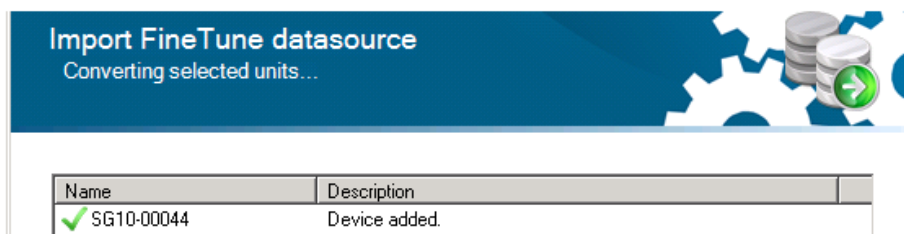


Once the datasource is selected, all the security gateways within the datasource are displayed and the ones to be imported can be individually selected.



The wizard provides the choice of selecting and importing the global namespace from the old FineTune datasource or not importing it. If the global namespace is not imported then any objects in this namespace which are referred to in a configuration are copied as local objects into the configuration created in InControl. If the global namespace is imported then this doesn't need to happen and the original FineTune structure is recreated in InControl.

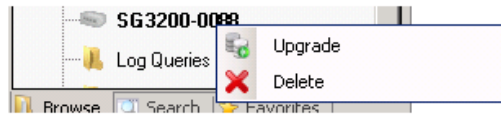
After selecting the units to import, the final wizard screen shows that the import has succeeded. In the screen shot below, a security gateway called *SG10-00044* has been successfully imported.



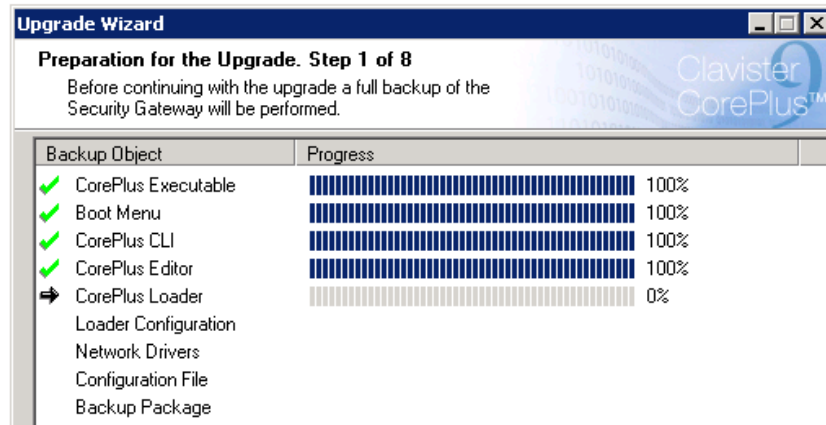
Upgrading the CorePlus Version

Once the FineTune Datasources are imported into InControl, the related security gateways are defined within InControl but cannot be managed by InControl since they are still running a 8.nn CorePlus version.

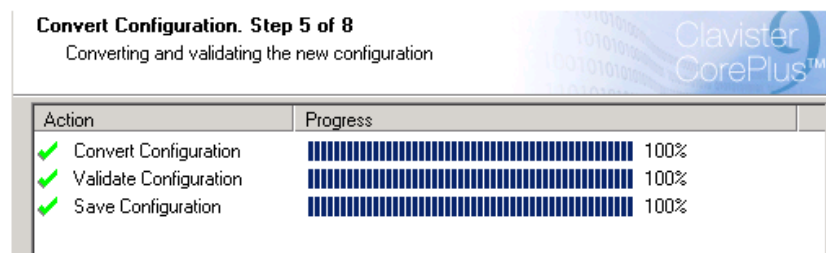
The next step is therefore to run InControl's inbuilt upgrade wizard to upgrade the Clavister Security Gateway itself to a later 9.nn version of CorePlus that can be managed by CorePlus. This is done by right-clicking on the security gateway in InControl's tree-view and selecting the **Upgrade** option from the context menu (the only two options at this stage are *Delete* or *Upgrade*).



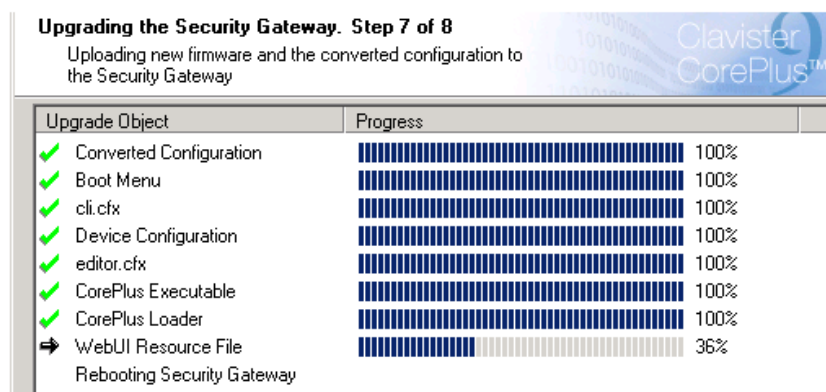
The upgrade wizard that runs is almost identical to the wizard used for defining a new security gateway, with the addition of some extra steps at the beginning and at the end. The wizard initially takes a backup of the configuration before it begins the upgrade and displays the backup progress.



After using the wizard to define the security gateway to InControl like a normal new unit, the actual upgrade is performed.



The final step is to upload the new, upgraded configuration to the security gateway.



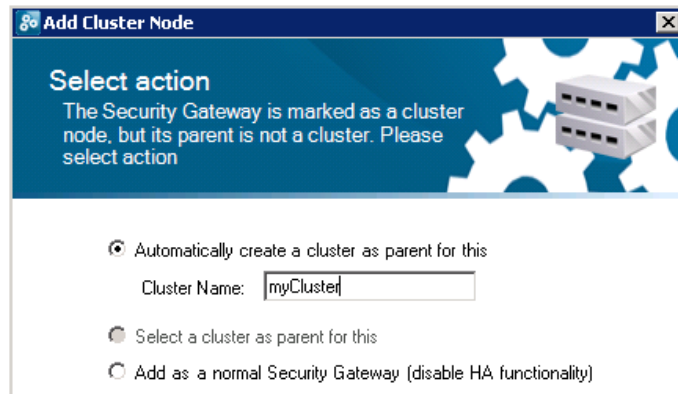
At this point, the security gateway can be fully managed through InControl.

Importing High Availability Clusters

CorePlus HA clusters running an 8.nn version should not be imported into InControl as described

above. Instead, perform the following steps:

- Upgrade the individual cluster members using the *Clavister Upgrade Wizard*. This will result in a working cluster running a 9.nn CorePlus version.
- Add the *master* cluster member as a new security gateway in InControl using the *New Gateway wizard*. The wizard will detect that the added gateway is part of a cluster and an additional wizard step appears, shown below.



Here, we can define a new cluster object to InControl, in this example calling it *myCluster*, and the new gateway will automatically become part of this cluster. Note that we are simply defining an existing cluster to InControl and the cluster itself is unaffected.

If there is an existing but empty cluster object already defined in InControl, the *master* unit could alternatively be added to it at this step.

- Now perform the same procedure on the *slave* unit of the cluster. When the *New Gateway wizard* detects the unit is a cluster member and the cluster options appear, we specify that the unit is added to *myCluster*, which was defined in the previous step.

This results in the cluster being completely defined to InControl.

Chapter 21: Troubleshooting Connections

If there are initial problems with communication between the Clavister Security Gateway and InControl then this section outlines a number of possible problems.

1. Check Communication Between InControl Client and Server

Remember that the InControl client communicates with the InControl server which then communicates with the Clavister Security Gateway. This section assumes they are initially running on the same PC. If they are on different computers then the client will indicate if it can't communicate with the server.

The remaining points in this list assume that the client and server are communicating. They relate to the communication between server and Clavister Security Gateway.

2. Check IP addresses

Make all the correct IP addresses have been entered for the Clavister Security Gateway.

3. Check InControl communication isn't blocked

Make sure another device in the network isn't blocking UDP port 999 TCP port 999. These are used by InControl to communicate with a Clavister Security Gateway.

4. Check connections with Ping

ICMP Ping can be used to check communications to the Clavister Security Gateway.

- Try pinging the gateway from the InControl management workstation.
- Try pinging a host on the management network from the local console on the gateway by using the serial cable.

5. Check management interface connections

There may be a physical connection problem:

- Check the link indicators of the network interface you have selected as the management interface. If there is no link indication, there might be a cable problem.

- Is the Clavister Security Gateway directly connected to a router or another host? In this case, an "X-ethernet" cable will be needed to connect the Clavister Security Gateway to that unit. Using the wrong cable type may result in the link indicators indicating link failure.

6. Routing problems

Look for routing problems:

- If connection to the Clavister Security Gateway is via a router, is the default gateway setting correct in both the Clavister Security Gateway and InControl?

7. CLI Diagnostics

Should none of the above be of any assistance, check the statistics information for the management interface by issuing the CLI command **ifstat** on the Clavister Security Gateway console. This could be done remotely using a Secure Shell (SSH) connection or on a console connected directly to the hardware's RS232 port.

```
Device:/> ifstat ifN
```

This will display a number of counters for the network interface and these are divided into two sections, one for hardware and one for software. To observe the interface behaviour, repeatedly issue the *ifstat* command.

If the **Input** counters of the hardware section are not increasing, then the error is likely to be in the cables. However, it may simply be the case that the packets aren't getting to the Clavister Security Gateway in the first place. This can be verified by attaching a packet sniffer to the network in question.

If the **Input** counters of both the hardware and software sections of the *ifstat* output are increasing, then the interfaces may be attached to the wrong physical networks. There may alternatively be a problem with the routing specified in the connected hosts or routers.

Another test can be performed by running the command **arpsnoop** on the Clavister Security Gateway console. It will dump ARP packets heard on selected interfaces. Arpsnoop is a convenient method of verifying that the correct cables are attached to the correct interfaces.

```
Device:/> arpsnoop -all
```

```
ARP snooping active on interfaces: if1 if2 if3 if4
ARP on if2: gw-world requesting ip_if2
ARP on if1: 192.168.1.5 requesting ip_if1
```

Appendix A: NetCon Key Generation

Overview

For setting up communication with a Clavister Security Gateway, InControl requires a *Netcon* key to be pasted into the *Secret Key* field in the dialog for defining a new gateway. This key can be obtained from CorePlus with the following steps:

- A. Create a new 512 bit Pre-Shared Key object.
- B. Enable the NetCon management protocol with the created key.
- C. Save and activate the new configuration.



Note: The NetCon protocol

The **NetCon** protocol is a proprietary Clavister protocol that uses CAST-128 encryption between the InControl server and Clavister Security Gateways. It uses AES-256 (Rijndael) encryption between clients and the server.

The above steps can be performed in one of two ways:

- Through the Web Interface.
- Using the CLI.

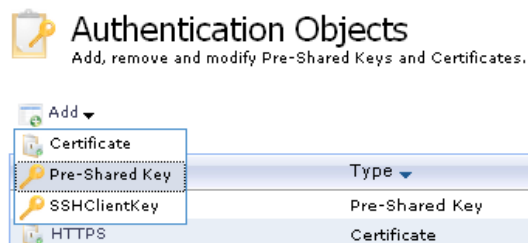
These two methods are now described in detail.

Using the Web Interface

When the Web Interface is used, the steps to obtaining the key are as follows:

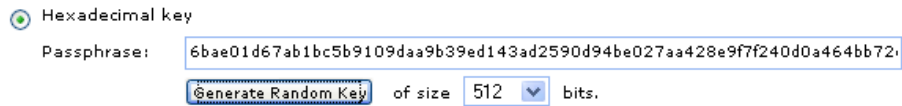
A. Create a new 512 bit Pre-Shared Key object.

1. Open a browser window to the CorePlus Web Interface of the Clavister Security Gateway which is to be defined with InControl.
2. Go to **Objects > Authentication Objects > Add Pre-Shared Key** and the page for creating a Pre-Shared Key object will be presented.



3. Select a suitable name for the key, for example *my_key*.
4. Select *Hexadecimal Key*.

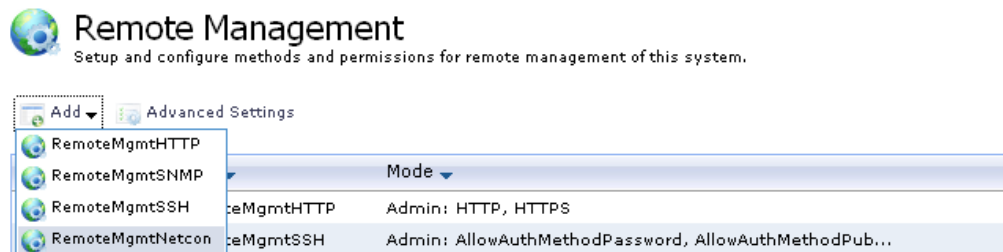
- Select 512 from the bit size choices and press the *Generate Random Key* button.
- A key will be generated and will appear in the *Passphrase* field. Right click this and select **Copy** to copy the key text to the Windows system clipboard.



- Press the *OK* button.

B. Enable the Netcon management protocol with the created key.

- Still in the Web Interface, go to **System > Remote Management > Add > RemoteMgmtNetcon** and the page for Netcon management will appear.



- Set the *PSK* field to the key called *my_key* created previously.
- Select the interface and network where the InControl workstation is located.

General

Mode:

Idle timeout:

PSK: i The Netcon PSK must be 512 bits long.

Access Filter

Remote access is granted from the following interface and network.

Interface:

Network:

- Press the *OK* button.

C. Save and activate the new configuration with the changes.

- In the toolbar, go to **Configuration > Save and Activate** to activate the new configuration.



- Now close the Web Interface browser window.

At this point, the required key is in the system clipboard and ready to be pasted into the InControl new gateway dialog.

Using the CLI

When the CLI is used, connection can be from a Secure Shell (SSH) client or directly via a console attached to the Clavister Security Gateway's RS232 port. The steps for obtaining the key are as follows:

A. Create a new 512 bit Pre-Shared Key object.

1. Using the `pskgen` we generate a new PSK object called `my_key` with a 512 bit key.

```
Device:/> pskgen my_key -size=512
```

If `my_key` already exists, then this command will set its key to be the one generated.

2. Using the `show` command to display the key created.

```
Device:/> show PSK my_key
```

Property	Value
Name:	my_key
Type:	HEX (Hexadecimal key)
PSKHex:	b2c8b532ba54f5da6040a05c3176b06a32beb547 acd199477e8a47b768ab3b31ab6a9e0539094f7d 35d7948041a6ef85b734c130cc20220c7cd4a8b6 d0cfc734

3. The PSK will now be displayed as shown in the example above and can be copied to the Windows system clipboard and later into the InControl new gateway dialog.

B. Enable the Netcon management protocol with the created key.

1. We will assume that management by InControl is to be enabled for the `lan` interface. The CLI command would be:

```
Device:/> set RemoteManagement RemoteMgmtNetcon
                Key=my_key
                Interface=lan
                Network=all-nets
```

The network on which the InControl workstation is located is specified above as being `all-nets`. It would be more secure to give a more specific network address.

C. Save and activate the new configuration with the changes.

1. Activate the configuration changes.

```
Device:/> activate
```

Then immediately commit the new changes (otherwise they will be automatically undone 30 seconds after the `activate` command).

```
Device:/> commit
```

At this point, the required key is in the system clipboard and ready to be pasted into the InControl new gateway dialog.

Appendix B: Keyboard Shortcuts

The following keyboard shortcuts are available when using InControl.

F1	Display the user guide.
F4	Toggle properties window.
F5	Toggle to design mode.
F11	Toggle to full screen mode.
F12	View the current preferences.
Ctrl+N	Add new object.
Ctrl+O	Open.
Ctrl+F4	Close.
Ctrl+S	Save.
Ctrl+Shift+S	Save all.
Alt+F4	Exit InControl.
Ctrl+Z	Undo last change.
Ctrl+Y	Redo last undone change.
Ctrl+X	Cut and place the contents into the clipboard.
Ctrl+C	Copy to the clipboard.
Ctrl+V	Paste the contents of the clipboard.
Ctrl+A	Select all.
Ctrl+D	Deploy...
Ctrl+Shift+R	Remote Console.
Ctrl+Shift+M	Quick Monitor.
Ctrl+Shift+O	Check Out.
Ctrl+Shift+I	Check In.
Ctrl+Shift+D	Deploy.
Ctrl+Shift+U	Undo Checkout.
Ctrl+Shift+L	Quick Real-time Log.
PgDn	Jumps to the bottom of the navigation tree.
PgUp	Jumps to the top of the navigation tree.
Arrows Keys	Move the currently selected control in design mode by a grid unit.

Appendix C: LQL Reference

Overview

Clavister *Log Query Language* (LQL) is a query language used to perform searches on the local CorePlus *MemLog* log message database. To perform such queries with InControl, the user can utilize a set of GUI controls to quickly select the desired search criteria without needing to know LQL. InControl converts the selected criteria into an LQL statement before launching it to perform the query.

LQL statements created in this way can be changed before the search is launched. Alternatively, a search can be done by creating the entire LQL statement from scratch. In either case, this appendix describes the syntax of LQL.

In some respects, LQL is similar to the traditional SQL used as a query language in many database products. LQL has, however, a large number of Clavister specific keywords and statements.

LQL Syntax

The basic syntax of an LQL query is as follows:

```
SELECT <output-type> [, <output-type>]
```

```
FROM <gateway_and_time_statement>
```

```
[WHERE <logical_statement>]
```

Each LQL query is expected to start with the SELECT keyword

Directly after the SELECT keyword, one or more output types (see section Output types), separated by a comma, are specified. The integrated log analyzer expects raw binary data, so for queries in the LQL panel of the log viewer, use "SELECT BINARY".

After the FROM keyword, one or more gateway and time statements are specified.

Optionally, the WHERE keyword followed by a logical statement may be specified.

Logical Operators

Logical operators are used to combine different LQL statements to form more complex statements. The following logical operators are defined in the LQL language:

Operator	Usage	Description
NOT	NOT Expression	Negates a Boolean expression.
AND	Expression1 AND Expression2	Combines two Boolean expressions and evaluates to TRUE when both expressions are TRUE.
OR	Expression1 OR Expression2	Combines two Boolean expressions and evaluates TRUE when either of the expressions are TRUE.

The logical operators are listed in precedence order; for example the 'OR' operator has a higher precedence than the 'AND' operator. By using parentheses to enclose parts of the statement the operator precedence can be changed.

Example C.1. Using Logical Operators

```
srcip = '10.0.0.1' and (destip = '192.168.123.1' or destip = '192.168.123.2')
```

Comparison operators

Comparison operators are used to compare search variables with user specified values. The following operators are supported:

Operator	Description
=	Equal to
>=	Greater than or equal to
<=	Less than or equal to
>	Greater than
<	Less than
IN	Range comparison

All user-specified values are expected to be quoted with ' chars.

Example C.2. Using Comparison Operators

```
srcip = '10.0.0.1' and destip = '192.168.123.1'
```

```
srcip IN (10.0.0.1 - 10.0.0.255) and destip IN (192.168.123.1 - 192.168.123.255, 1.2.3.4)
```

Search variables

There are a number of predefined variables that can be used in the logical statements. The table below lists the variables currently defined.

Variable	Value Type	Description
srcip	IPv4 address	Source IP address on the format: a.b.c.d
destip	IPv4 address	Destination IP address on the format: a.b.c.d
hwsrc	Ethernet address	Source ethernet address
hwdesc	Ethernet address	Destination ethernet address
severity	String	Log message severity
category	String	Category of the logged event. Example: SYSTEM, NETCON, USAGE, CONN, DROP
conn	String	Connection event. Example: Open, Close, Closing
srcport	Integer	Source port (0-65535)
destport	Integer	Destination port (0-65535)
ipproto	Integer	IP protocol (0-255 or name). Example: TCP, UDP, ICMP, 99
recviface	String	Receiving interface name. Example: ext, int, dmz
destiface	String	Destination interface name
icmptype	String	ICMP Message Type (0-255. Example: ECHO_REQUEST
arp	String	ARP opcode. Example: Request, Reply, Other
icmpsricip	IPv4 address	Source IP address in ICMP-encapsulated IP packet
icmpdesctip	IPv4 address	Destination IP address in ICMP-encapsulated IP packet
icmpsricport	Integer	Source port (0-65535) in ICMP-encapsulated IP packet
icmpdestport	Integer	Destination port (0-65535) in ICMP-encapsulated IP packet
icmipproto	String	IP protocol (0-255) in ICMP-encapsulated IP packet

Variable	Value Type	Description
description	String	Description of the event
fin	Boolean	TCP FIN flag (0 or 1)
syn	Boolean	TCP SYN flag (0 or 1)
rst	Boolean	TCP RST flag (0 or 1)
psh	Boolean	TCP PSH flag (0 or 1)
ack	Boolean	TCP ACK flag (0 or 1)
urg	Boolean	TCP URG flag (0 or 1)
xmas	Boolean	TCP XMAS flag (0 or 1)
ymas	Boolean	TCP YMAS flag (0 or 1)
enetproto	Integer	Ethernet protocol number (0-65535)
rule	String	Rule name
satsrcrule	String	SAT source rule name
satdestrule	String	SAT destination rule name
enet[index]	Integer	Value at [index] bytes offset from the Ethernet header
ip[index]	Integer	Value at [index] bytes offset from the IP header
tcp[index]	Integer	Value at [index] bytes offset from the TCP header
udp[index]	Integer	Value at [index] bytes offset from the UDP header
almod	String	Name of the ALG module that this log message originated from.
algsesid	Integer	ID of the ALG session that this log message originated from.
authrule	String	Userauth rule name.
authagent	String	Userauth agent. Example: http, xauth
authevent	String	Userauth event. Example: Login, Logout, Timedout, Disallowed
username	String	Username, from login/logout, as well as src/destusername
srcusername	String	The user that originated this connection/packet
destusername	String	The destination user

Output Types

There are a number of output types defined that are used when specifying what data is to be returned by the query.

All output types return data in plain text, except the *binary* type, which will return the data in a binary form used in the query tool. The *binary* output type is the only output type that is allowed when using the query analyzer tool, and it cannot be mixed with the plain text output types.

The following output types are defined:

Name	Description
binary	Binary form output, only used within the query tool.
srcip	Source IP address.
destip	Destination IP address
srcport	Source port
destport	Destination port
hwsrc	Source ethernet address
hwdest	Destination ethernet address
iphdrln	IP header length
ipdatalen	IP data length
iptotlen	IP total length (data + header)
udpdatalen	UDP data length
udptotlen	UDP total data length

Name	Description
gateway	Name of the gateway that sent the data
time	The time when the event took place
recvif	Receiving interface
destiface	Destination interface
ttl	Time To Live field in the IP header
date	The date when the packet arrived at the logger
description	Description of the event
arp	ARP packet type
arphwdest	Destination hardware address in ARP events
arphwsrc	Source hardware address in ARP events
ipproto	IP protocol
icmptype	ICMP type
icmpsrcip	Source IP in an ICMP-encapsulated IP packet
icmpdestip	Destination IP in an ICMP-encapsulated IP packet
icmssrcport	Source port of an ICMP-encapsulated UDP/TCP packet
icmstd	ttl, icmptype, icmpipproto, icmpdestip, icmssrcip and icmpdestport
tcpflags	All TCP flags
enetproto	Ethernet protocol
usage	Interface throughput
connusage	Connection statistics
rule	Name of the rule that this log entry matched
satsrcrule	Name of the SAT source rule that this entry matched
satdestrule	Name of the SAT destination rule that this entry matched
origsent	Amount of data sent by the originator (client end) of the connection
termsent	Amount of data sent by the terminator (server end) of the connection
conn	Conn event type
ack	TCP ACK flag (0 or 1)
fin	TCP FIN flag (0 or 1)
psh	TCP PSH flag (0 or 1)
rst	TCP RST flag (0 or 1)
syn	TCP SYN flag (0 or 1)
urg	TCP URG flag (0 or 1)
ece	TCP EXE flag (0 or 1)
cwr	TCP CWR flag (0 or 1)
category	Category of the logged event
tcphdrln	TCP header length
tcpdatalen	TCP data length
tcptotlen	TCP total length (data + header)
standard	date, time, gateway, category, recvif, srcip, srcport, destip, destport, ipproto and description
tcpstd	tcpdatalen, tcphdrln, fin, syn, rst, psh, ack, urg, ece and cwr
udpstd	udpdatalen
severity	Log message severity
algmod	Name of the ALG module that this log message originated from
algsesid	ID of the ALG session that this log message originated from
authrule	Name of the userauth rule applied
authagent	User authentication agent
authevent	User authentication event
username	Name of the user that logged in/out

Name	Description
usernames	username, srcusername, and destusername
srcusername	The user that originated this connection/packet
destusername	The destination user

Gateway Statements

The LQL *gateway* statement is used to specify the particular Clavister Security Gateway(s) to search for log events.

The syntax of a gateway statement is as follows:

```
<gateway> [, <gateway>] [<time_statement>] [ AND <gateway> [, <gateway> ]
[<time_statement>]]
```

Time Statements

The time statement is used to specify a time interval for the data that is requested.

A time statement can be any of the following statement types:

TIMES yyyy-mm-dd HH:MM:SS TO yyyy-mm-dd HH:MM:SS

LAST DAYS n

LAST FULL DAYS n

LAST HOURS n

LAST FULL HOURS n

(where n is any numerical value in the range from 1 to 1000)

If the *TIMES* statement is used, the date and time have to be specified in ISO standard format, as shown above, and may be terminated at any point. For example, *TIMES 2000-01 TO 2000-02* is a valid time statement.

InControl Glossary

Clavister Hardware Series	The series of Clavister hardware appliances that run the CorePlus operating system.
Clavister Security Gateway	A hardware device which is running the CorePlus operating system.
Clavister Software Series	Versions of the CorePlus operating system which run on generic, non-Clavister hardware.
CLI	The <i>Command Line Interface</i> for CorePlus. CLI commands offer an alternative user interface and can be issued either through a Secure Shell client or through a console connected to the local RS232 port of the Clavister Security Gateway.
CorePlus	A Clavister proprietary software operating system which performs all the functions of a Security Gateway.
Dashboard	A collection of Monitoring controls that are displayed together.
Dashboard Template	A pre-defined dashboard that must have its Monitoring Controls associated with a Clavister Security Gateway.
Design mode	The alternative to Monitor mode. In this mode, dashboards are created, edited and saved, and are not actively monitoring any Clavister Security Gateways.
InControl client	A proprietary Clavister software application that runs on a separate workstation to control one or many Clavister Security Gateways.
InControl server	A proprietary Clavister software application that runs on a Windows based PC that mediates data flowing between clients and the Clavister Security Gateways they control as well as acting as a central repository for all configuration data
Generic Monitoring Control	A graphical control that appears on a dashboard for monitoring one of more CorePlus parameters on a Clavister Security Gateway.
Layout Control	A graphical control used for making cosmetic additions to a dashboard. This might be the addition of a text or images, or alternatively gathering Monitoring controls together into a Group.
Monitor mode	The alternative to Design mode. In this mode, a dashboard becomes "live" and actively monitors the operating parameters of one or more Clavister Security Gateways. Saving of a dashboard can also be done in this mode.
.NET Framework	A software library available as a free download from Microsoft which is necessary for running InControl. Installed automatically with InControl if not already installed.
Netcon	A proprietary secure Clavister protocol used for communication with Clavister Security Gateways by the server and by clients to the server. Encryption is based on CAST-128 for communication between the InControl server and

		Clavister Security Gateways. It is based on AES-256 go communication between clients and the server.
Pre-defined Control	Monitoring	A control which is specifically designed to monitor a particular aspect of CorePlus operation such as Web Content Filtering.
Security gateway		A hardware device which intercepts, monitors and routes IP traffic in order to prevent security attacks against particular computing assets.
Web Interface (WebUI)		Another name for the <i>web interface</i> . A CorePlus management interface made possible by connecting to CorePlus using a normal web browser. The Clavister Security Gateway acts as a web server, delivering web pages to the browser and acting on the administration commands sent back.

Alphabetical Index

Symbols

.NET installation, 11

A

adding security gateways, 24
alarm, 50

- acknowledging, 52
- action, 50
- center, 51
- clearing, 51
- search criteria, 53

API for InControl, 8

architecture, 7

audit trail, 54

B

backing up the database, 22

C

certificate requests, 91

certification authority, 91

checking in, 34

- inheritance, 36

checking out, 32

CLI

- diagnostics, 100
- remote console opening, 62

client

- installation, 13
- interface, 16
- login, 13
- preferences, 19

configuration versions (see revision management)

control properties, 68

cursor styles, 68

custom dashboards, 66

customer web, 48

D

database

- backup, 22
- moving, 23
- restore, 23

data bindings, 69

deleting security gateways, 29

demonstration mode, 44, 48

deploying new configurations, 35

design mode, 70

domains, 17

downgrading CorePlus, 15

dynamic maximums, 69

F

FWLogger database, 82

H

high availability cluster, 78

- adding an existing cluster, 80

I

importing

- FineTune™ datasources, 14, 95

- HA clusters, 97

installation, 10

internal CA servers, 94

K

keyboard shortcuts, 104

L

license center, 44

licenses

- expiration alert, 49
- files, 48

licensing, 44

- CorePlus, 48

- CorePlus license uploads, 48

- InControl, 44

logging, 82

log monitoring, 76

log query language (see LQL)

log query server (see LQS)

LQL, 105

LQS, 82

- installation, 12

N

netcon key generation, 101

P

per gateway licenses, 45

ping, 99

purging objects, 29

R

registration key, 48

remote console, 62

- multiple sessions, 63

revision management, 31

- concurrent CLI, WebUI changes, 36

- revision numbers, 36

S

saving dashboards, 71

SDK for InControl, 8

server

- audit level, 20
- changing status, 13
- installation, 12
- interface, 12
- management, 20
- syslog server config, 21
- transfer limit, 21
- windows process, 12

server license, 45

speedometer, 68

T

templates, 71

- groups, 72
- text captions, 71
- themes, 71
- troubleshooting connections, 99

U

- undo check out, 35
- upgrading
 - CorePlus, 14
 - from 8.nn, 14
 - InControl, 14
- user accounts, 57
 - groups, 58
- user groups, 58

V

- volume license, 45

CLAVISTER®

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
Fax: +46-660-12250

www.clavister.com