



CLAVISTER®

Clavister InControl Administration Guide

Version 1.70.00

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
www.clavister.com

Published 2016-11-24
Copyright © 2016 Clavister AB

Clavister InControl Administration Guide Version 1.70.00

Published 2016-11-24

Copyright © 2016 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. Upgrading InControl	17
4. Server Management	20
5. The Client Interface	26
6. Preparing cOS Core	33
7. Adding Security Gateways	39
8. Revision Management	46
9. A First Security Policy	55
10. Device Maintenance	62
11. Licensing	65
11.1. InControl Licensing	65
11.2. cOS Core Licensing	71
12. Alarms	77
13. The Audit Trail	82
14. Domains	84
15. User Accounts and Groups	89
16. Remote Console	95
17. Real-time Monitoring	98
18. Log Event Monitoring	108
18.1. Memlog Monitoring	108
18.2. The ILA	110
18.3. The Log Explorer	119
18.4. The Query Filter	123
18.5. Log Query Language (LQL)	126
18.6. The Log Analyzer	132
18.7. InControl Reporting	144
19. The Library Browser	151
20. High Availability	154
21. Configuration Object Groups	160
22. Troubleshooting Connections	166
23. MFA Server Administration	168
23.1. Overview	168
23.2. Installation	171
23.2.1. Windows Installation	171
23.2.2. License Installation	172
23.2.3. Adding to InControl	173
23.2.4. The Revision History	174
23.3. Configuration Objects	175
23.3.1. Overview	175
23.3.2. MFA Server Object Configuration	176
23.3.3. User Store Object Configuration	177
23.3.4. RADIUS Server Object Configuration	178
23.3.5. RADIUS Client Object Configuration	178
23.3.6. Self Service Object Configuration	179
23.4. Scenarios	181
23.4.1. Adding a Scenario	181
23.4.2. Password Scenario Configuration	181
23.4.3. Token Scenario Configuration	182
23.4.4. SMS Scenario Configuration	183
23.4.5. SMS Credits	184
23.5. Supported Clients	185
23.6. Self Service Portal	186
23.7. The Authenticator App	188
23.8. System Folders	189

23.9. Logging	190
A. Cube Log Messages	193
B. Netcon Key Generation	198
C. Certificate Requests	203
D. Keyboard Shortcuts	208
InControl Glossary	209
Alphabetical Index	211

Preface

Target Audience

The target audience for this publication is the administrator of one or more security gateways running the cOS Core network operating system. The system may be running on Clavister hardware or non-Clavister hardware and is to be administered via one or more management workstations running the Clavister InControl client 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 emphasized 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.

cOS Core and *CorePlus* are trademarks of Clavister AB.

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

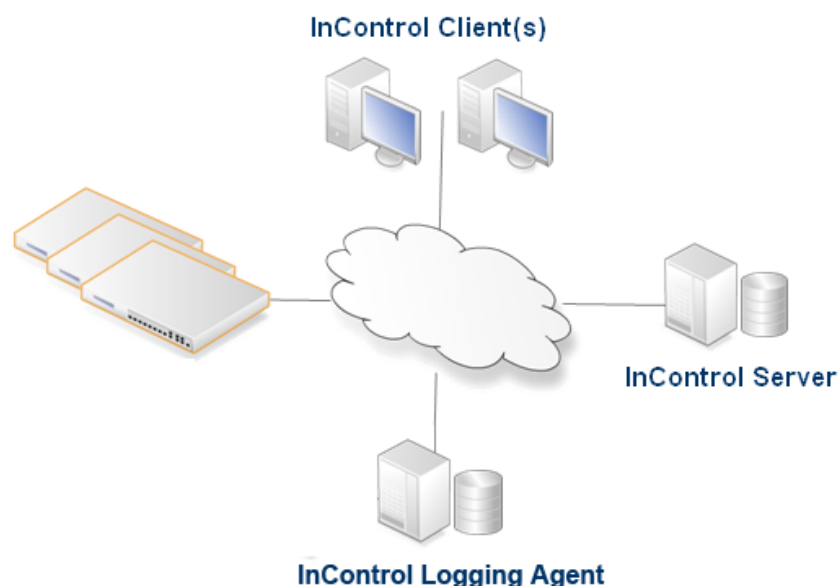
Chapter 1: InControl Overview

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 any Windows™ based computer (Windows 7 SP1 or later). This computer will sometimes be referred to in this document as the *client workstation* or as the *management workstation*.

The Client/Server Architecture

InControl consists of two main software components: 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 cOS Core configuration data and mediates all management communication between clients and security gateways. The diagram above illustrates a possible deployment of InControl with its components distributed across separate computers connected by the Internet. The optional Clavister *InControl Logging Agent* (ILA) component is a cOS Core log server provided with InControl. All InControl components could reside on the same computer.

Management Tasks Performed through InControl

The following key tasks can be performed on a Clavister Security Gateway using the InControl client:

- Controlling cOS Core management communication.
- Creating, modifying and removing cOS Core objects and security policies.
- cOS Core configuration version control.
- cOS Core license management.
- cOS Core 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 cOS Core.

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* always exists that has, by default, full administrative privileges.

Other types of 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. This topic is discussed further in *Chapter 15, User Accounts and Groups*.

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 in the separate *InControl SDK Guide* PDF document. The InControl API is based on the *Windows Communication Foundation* (WCF) interface which allows code development to be done using any one of a number of programming languages and platforms.

Chapter 2: Installing InControl

This section describes the installation of the InControl client and server. Installation of the *ILA* is covered in *Section 18.2, "The ILA"*.

InControl Installation Files

The complete set of InControl installation files can be found on the cOS Core 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, a separate executable for the InControl server installation and another executable for the optional *InControl Logging Agent* (ILA).

There is also a bundled executable which combines all three. ILA installation is covered in *Section 18.2, "The ILA"*. This chains together the installations of the components so that the same question are asked. For example, the question regarding license agreement will still appear once for each component.

Components Can Be Installed On Different Computers

Installation of the InControl client, server and the optional ILA can be on either the same Microsoft Windows based computer or different computers. The client and server installations will be sometimes referred to in this document as the *client workstation* and the *server computer*.

cOS Core Versions

InControl can only be used for management of Clavister Security Gateways running cOS Core version **10.11.00** 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 cOS Core that is incompatible.

Minimum and Recommended Hardware Requirements

The hardware configurations for both the client, server and optional ILA are as follows:

- **Operating system:**
 - i. *Recommended:* Microsoft Windows 7 (SP1) for the client, server or the ILA. Alternatively, Windows 2008 R2 (SP 1) for the InControl server and the ILA.

- ii. At least Microsoft .NET™ version 4.6 is required for the InControl client, server and ILA.

- **Memory:**

- i. *Minimum:* 1 Gigabyte RAM (2 Gigabytes with the 64 bit InfoBright database).
- ii. *Recommended:* 4 Gigabytes RAM.

- **Free disk space:**

- i. *Minimum:* 200 Megabytes for initial client, server and ILA installation.
- ii. *Recommended:* At least 1 Gigabyte for the server or ILA. Both may grow as the database, audit and event logs expand.

- **Processor speed:**

The recommended processor is an *Intel Core i7* processor or a processor with equivalent speed. All InControl components can function with slower processors but *Intel Core i7* speed is optimum.

- **Screen resolution**

For working with the client interface or server management interface, a screen resolution of at least 1280 x 1024 pixels is recommended.

A Local User is Recommended for Running Services

Installation of InControl must be done from a Windows account with *Administrator* privileges. However, using a non-local account could mean that security is compromised by a malicious user logging in across a network.

To enhance the security of the InControl server, it is recommended to create a new, local user account and then log into this account to perform server installation. Such accounts are sometimes referred to as *Service Accounts*. These keep services completely separate from normal user accounts. The same server account should also be used for the ILA server.

Once server installation is complete, the Windows service *ICS.exe* should then be set up in Windows to run under the new, local account (select the **Log On** tab in the properties of the service and specify the account).

To additionally enhance security, InControl server database file access should be restricted to this account only.

Clients Do Not Require Administrator Privileges

InControl clients do **not** need to be running under Microsoft Windows as a user which is a member of the Windows *Administrator* group. A user can be a member of a group with lesser privileges.

InControl Server to cOS Core Communication

The InControl server 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, InControl clients need network access to the server workstation if client and server are

running on different computers.

Required .NET Versions

InControl relies on the Microsoft .NET framework. Version 4.6 of the .NET framework is required for the InControl client, server and ILA.

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

Installing InControl

Installation of InControl is performed in two primary steps:

1. Install the InControl server using the *InControl_Server_Setup.exe* file.
2. Install the InControl client using the *InControl_Client_Setup.exe* file.

A third, optional step is to also install the *InControl Logging Agent* (ILA) using the *ILA_Client_Setup.exe* file. This is described further in Section 18.2, "The ILA".

The ordering of running any of the three installation executables is not important. An alternative to running the installation executables separately is to run the single *InControl_Bundle_Setup.exe* file which runs the three individual files in sequence.

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.

If installed, the ILA can also be on the same or separate computer.

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

Server Installation

The server installation wizard consists of a standard set of installation dialogs which will not be reproduced here.

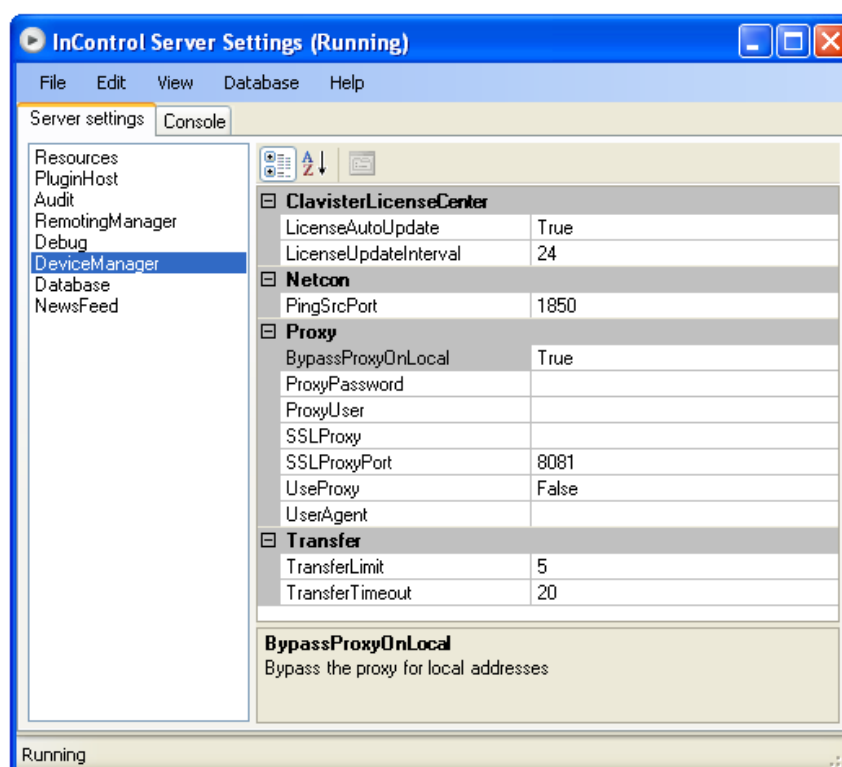


Note: Microsoft .NET version 4.6 is required

Both the InControl server and the ILA require at least Microsoft .NET version 4.6 is installed.

The installer provides the option to install .NET as part of the installation process if it detects that it is not already installed.

On wizard completion, the InControl server will be left running as a Windows service. The server control interface can then 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.

Both the InControl server and, if installed, the ILA run as Windows services. All processes appear when the *Task Manager* is displayed in Windows as shown below.

ICC.exe *32	8608	us	01	57.204 K
ICS.exe *32	11304	SYSTEM	00	30.156 K
ILA.exe	11608	SYSTEM	00	40.160 K
LogReceiver.exe *32	9248	SYSTEM	00	22.808 K

The listed processes listed in the screenshot above are as follows:

- **ICC.exe** - The InControl client.
- **ICS.exe** - The InControl server.
- **ILA.exe** - The ILA query server and log analyzer database builder.
- **LogReceiver.exe** - The ILA log receiver server.

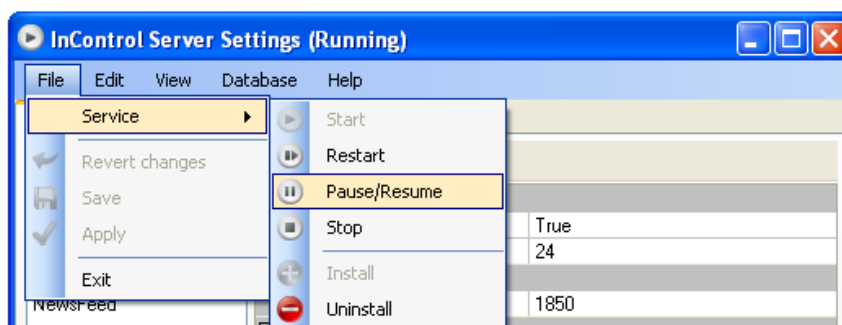


Important: Restrict access to the server hardware

Access to the InControl server management interface is not protected by any security mechanisms. Physical access to the PC on which the server is running also means possible access to the server interface. It is therefore important to restrict access to this computer.

Changing the Server Status

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



The **Install** and **Uninstall** options in this menu are for installing and uninstalling *ICS.exe* as a Windows service.

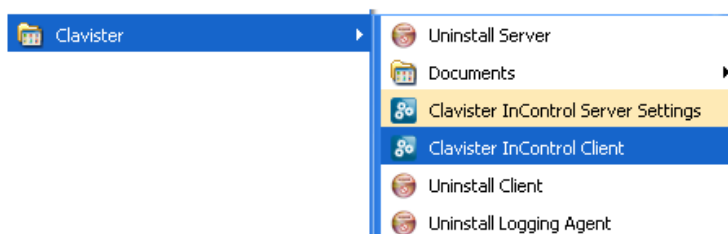
Client Installation

The client installation wizard steps consist of a sequence of standard installation dialogs. As mentioned previously, the client requires at least Microsoft .NET version 4.6 is installed and the installer provides the option to install this as part of the client installation process.

Following installation, the client is ready to run.

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.

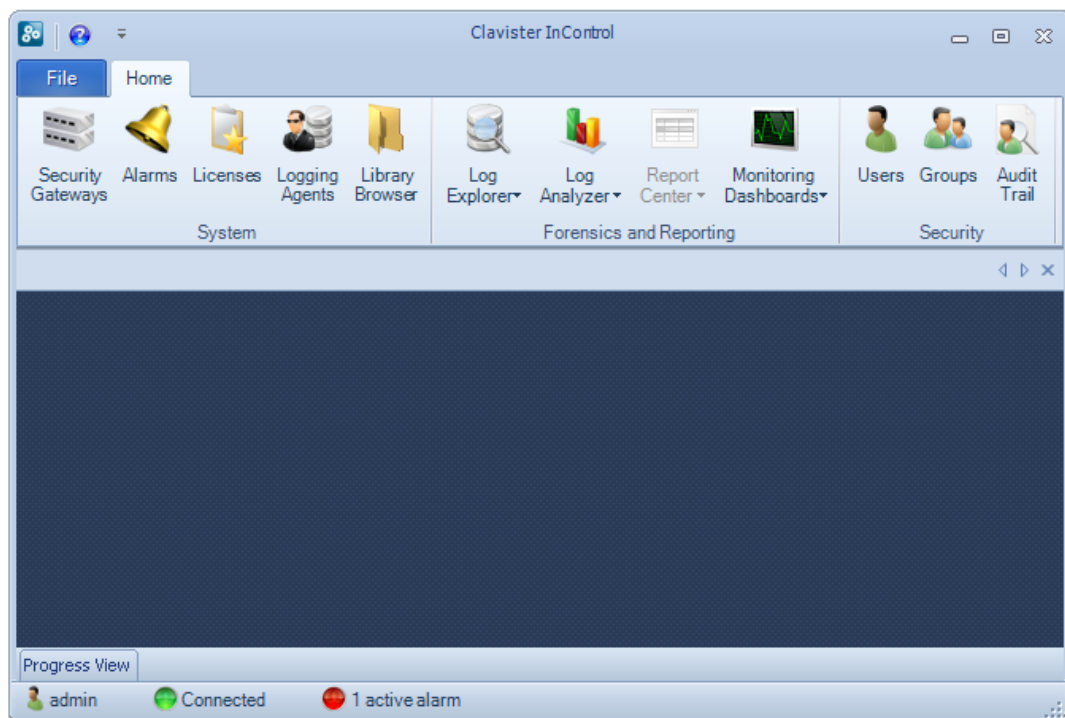


Initial Login

When the client is started a username and password will be asked for. The initial 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.



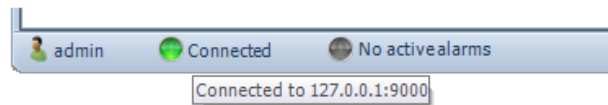
Client to Server Connection

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 and the port number to which the client has connected. In the example shown below, the IP address is the local loopback address since the client and server are on the same computer.



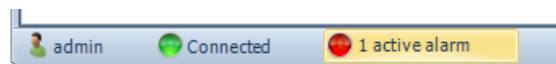
If connection to the InControl server was unsuccessful then this icon will be red:



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, start the server by choosing the **Start** option from the **File > Service** submenu. The client service status icon should now turn green after a brief interval to indicate successful server connection.

The rightmost icon shows if any *alarms* are active. Alarms provide informational, warning or error messages.



As shown above, the alarm icon also acts as a button. When it is pressed the *Alarms* tab is displayed and further action to deal with alarms can be taken. Alarms are discussed further in *Chapter 12, Alarms*.

Chapter 3: Upgrading InControl

When new releases of InControl are made available, these can be downloaded by logging in as a customer to <http://www.clavister.com> and selecting the relevant download. InControl updates are packaged as a set of four Windows executable .exe files which run an installation wizard. There is one installation executable file each for the client, server and ILA components plus a fourth file called *clavister-incontrol-n-nn-nn-bundle-setup.exe* which allows all components to be upgraded together (where *n-nn-nn* is the InControl version number).



Important: Upgrade all InControl components together

*Although InControl releases include separate installation executables for the upgrade of the client, server and ILA, they should be viewed as a single upgrade. One component should **not** be upgraded without the others since dependencies may exist. For this reason, it is recommended to run the **bundle-setup.exe** file.*

Uninstallation of existing versions is not required and the order of installation is not important. However, upgrading from version 1.10 has special requirements which are described later in this section.

Before installing, both the client and server management interfaces should be closed. The server installation will automatically stop the relevant services and then restart them.

The InControl server database is not normally affected by upgrading. Even 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.

Creating a Database Backup

The installation wizard for the InControl server will ask if the current InControl database is to be backed up. By default, this option is enabled and it is recommended not to disable it. The original database is a single file called *ics.db3* with a default location of:

```
%appdata%\Clavister\InControl\Server\
```

Where *%appdata%* is the root path Windows variable and this is usually set to be the folder for the current user's application data. The backup file has the time-stamped filename *dbyyyy-mm-ddThhmmss-i.ics* and is stored in the same directory as the original database file.

A backup file created by the installer can be restored by using the **Database > Load** menu option in the *InControl Server Settings* management interface. This will automatically stop and restart the InControl services.

The server settings interface and saving or restoring the InControl database is discussed further in *Chapter 4, Server Management*.



Caution: Copying the database file requires a stopped server

*Taking a backup of the InControl database can be done outside of InControl by making a copy the **ics.db3** file in Windows. Restoring that copy only requires changing the name back to **ics.db3**. However, **the InControl server must be stopped before these operations**, otherwise the database file can become corrupted. For this reason, it not recommended to perform a backup and restore in this way.*

Upgrading from InControl 1.10

If upgrading from InControl version 1.10 then some special manual operations are required. The three InControl components of client, server and Log Query Server (LQS) must be uninstalled before installing a later InControl version.



Important: Back up the old LQS files

Uninstallation of 1.10 will preserve most of the old server database (including the audit logs) as well as the LQS log database files. These can then be manually transferred into the new InControl version's file structure as described below.

*However, the LQS configuration file **lqs.xml** is deleted during LQS uninstallation and a copy will be needed if the new ILA configuration is to replicate the old LQS configuration. This file is found in the **Clavister\InControl\LQS** folder.*

For the filepaths used in the description below, the Windows variable `%programfiles%` is assumed to be the root path for the old InControl version installation. The variable `%appdata%` is assumed to be the root path for the new installation and this usually defaults to be the current user's application data folder. Both roots may have been changed when LQS was installed.

A. Moving the old server files

- i. Before moving the server files, stop the InControl server service (this is called `ICS.exe` in the Windows process list). This is best done by using the InControl server control interface.
- ii. Take the old server database file `ics.db3` found in:

```
%programfiles%\Clavister\InControl\Server\db
```

And move this file to the new database folder of the new version found in:

```
%appdata%\Clavister\InControl\Server\
```

This will overwrite the existing `ics.db3` file and so the existing database will be lost.

- iii. Now take all files from the old audit file folder:

```
%programfiles%\Clavister\InControl\Server\db\audit
```

And copy them to the new audit folder:

```
%appdata%\Clavister\InControl\Server\audit
```

These will merge the old files with any existing audit files. An old file will overwrite an existing file with the same name.

B. An alternative to moving the server files

Instead of moving the old server files into the new installation directory, the InControl server installer provides the option to specify the location of the new InControl server database. The location chosen can be the same as the old installation directory which still contains the old *ics.db3* database file.

The installer will not overwrite this old database file and it will therefore become the database for the new version. No old server files then need to be moved.

C. Moving the old LQS log files

- i. Take all the subfolders (each has a gateway identifier), but **not** the *lqs.xml* file, from the LQS database folder:

```
%programfiles%\Clavister\InControl\LQS
```

And copy these subfolders with their contents to the ILA database folder:

```
%appdata%\Clavister\InControl\LoggingAgent\LogDatabase
```

The old LQS log folders and files will merge with any existing ILA log files. Files with the same name will be overwritten.

Some typical examples of the names of the copied subfolders is shown in the file explorer screenshot below.

Name	Size	Type	Date Mod
61b3efb0-8987-40a6-90b8-3dff871d88e7		File Folder	2010-09-
869ad421-0ac4-47df-9418-4e06eed426bc		File Folder	2010-06-

- ii. It is important **NOT** to copy the *lqs.xml* file from the old LQS installation **unless** the old LQS configuration is to become the configuration for the new ILA installation. This file is deleted when LQS is uninstalled so a copy should be made before beginning the uninstall process.

When it is transferred into the new ILA directory structure, the file *lqs.xml* will be automatically converted to become the current ILA configuration file *ila.xml* but **only** when the ILA Windows service (called *ILA.exe* in the process list) is restarted. To do this, go into the Windows control panel and restart the service.



Note

The file *lqs.xml* is deleted during the conversion process *ila.xml*. Retain a copy of *lqs.xml* in case the conversion process does not complete successfully.

Chapter 4: Server Management

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

Displaying the Server Management Interface

Selecting *Clavister InControl Server Settings* from the Windows start menu causes the management user interface for the server to be displayed. Displaying this interface will not affect the running of the server if it is already started. If the server is not running then displaying the management interface will have the effect of also starting the server.

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 **File > Service > Stop** menu option in the server management interface (or alternatively, stopping it through the Windows process manager).

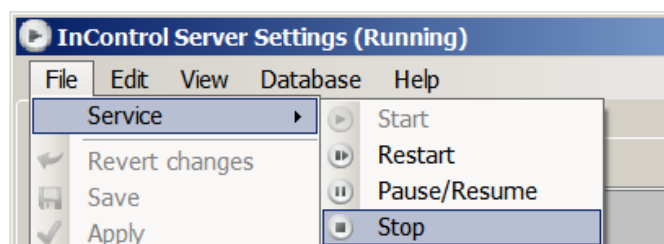


Note: Login to the account under which the server runs

To access the server interface, it is necessary to login as the user under which the server runs. If, as recommended, a local account has been created for this purpose then it is this account that must be logged into.

Stopping and Pausing the Server

Closing the server management 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 management interface. The same menu option can then be selected to resume the server after a pause.

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



Warning: Logout all clients before stopping the server

No clients should be performing any configuration changes or related activities during an operation that stops the InControl server such as:

- *Manually stopping the server.*
- *A server database backup or restore operation.*
- *A server software upgrade.*

One of the effects of a client working on a checked-out configuration when the server is stopped is that all changes will be lost.

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 is important to remember that the server log messages being discussed here are totally separate from the log messages generated by cOS Core 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

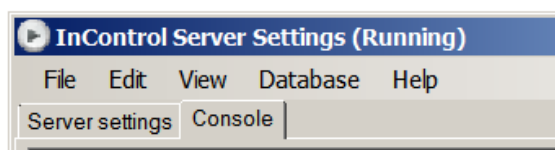
By default, the **Transfer Limit** parameter has a value of 2. This means that after deployment of a new configuration is initiated, the number of concurrent uploads to Clavister Security Gateways will be limited to two.

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

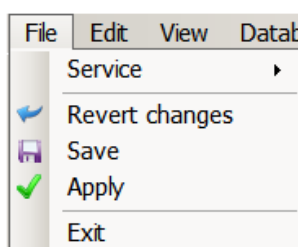
The server interface contains a **Console** tab which gives easy access to log messages generated

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 management 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**

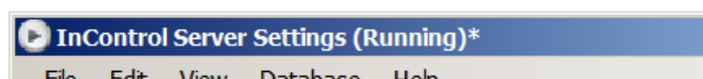
This option saves the changes but doesn't apply them to the running server. They will be applied if the server restarts.

- **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.

Once any unsaved change is made to the server configuration, this is indicated by an asterisk ("*") appearing to the right of the management interface window title as shown below.



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 entire server database is stored in a single file called *ics.db3* and its default location is:

```
%appdata%\Clavister\InControl\Server\
```

Where *%appdata%* is the root path Windows variable and this is usually set to be the folder for the current user's application data.

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.

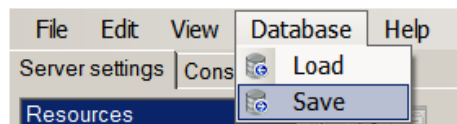
There are two ways of performing a backup:

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

These are discussed below:

1. Backup initiated through the server management interface.

In the server management interface, select 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, *db2015-02-26_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.

When a backup or restore is performed via the server settings management interface, the InControl server will be automatically stopped and restarted

2. Backup initiated through the command line.

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

```
> 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. The backup filename used has the default naming format described above and cannot be changed before performing the backup.

When using the *Server Settings* command to perform a backup or restore, the InControl server will be automatically stopped and restarted.

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 with the following Windows console command:

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

A restore will overwrite the existing database so that should be backed up if it may be required later.

When a database restore is complete, the InControl server will restart automatically 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.



Note: Backup files are automatically compressed

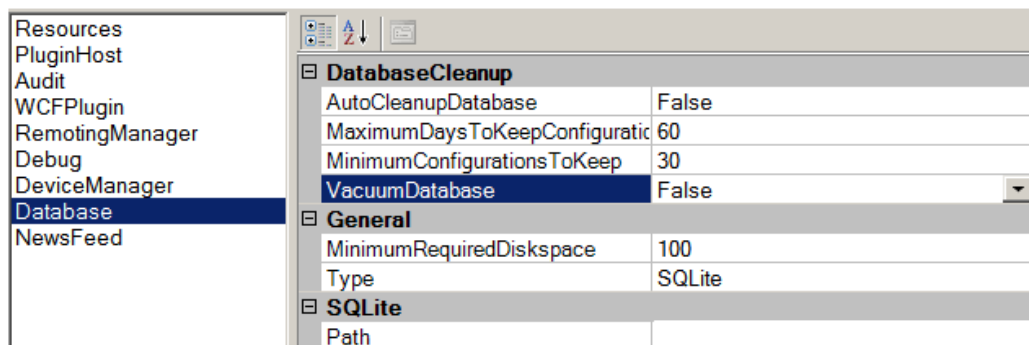
When using the InControl server settings interface or command to create a database backup file, the file is automatically compressed using GZIP to conserve disk space. Decompression is automatic when a backup is restored in the same way.

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.

Disk Space Management

The management interface provides settings for managing the disk space taken up by the server and its database.



These settings are used as follows:

- **DatabaseCleanup**

These settings are used as follows:

- Enabling **AutoCleanupDatabase** means that the automatic cleanup process is initiated on server startup and then repeatedly after each hour has elapsed. Enabling this option will help keep the size of the database from growing continuously and this can both help database efficiency and reduce the time needed to back up the database.

If this option is not enabled, the database file will retain the space occupied by deleted configuration data leading to an ever bigger and less efficient database file.

- ii. When the automatic cleanup runs, any configuration in the revision history older than the number of days specified by **MaximumDaysToKeepConfigurations** is deleted but only if the **MinimumConfigurationsToKeep** is exceeded for that gateway.
- iii. The **MinimumConfigurationsToKeep** specifies the minimum number of configurations in the revision history for each individual gateway that are kept. Only if this number is exceeded can any revisions be deleted by the automatic cleanup process.
- iv. The **VacuumDatabase** option is only used when the *AutoCleanupDatabase* option is enabled. If it is enabled, the cleanup process will also compact the database file down to the smallest size possible, removing any unused space in the process. This will make subsequent database access as efficient as possible. This compaction will **only** take place on InControl server startup and not at other times when automatic cleanup runs.



Warning: The VacuumDatabase option is time intensive

*The **VacuumDatabase** option can require significant amounts of processing time to complete depending on database size. It should therefore only be enabled when circumstances allow adequate time for it to complete following server startup.*

- **MinimumRequiredDisk**

This is the amount of free disk space that is required for the InControl server. If the free disk space falls under this value, the only action that occurs is that an alert is created which warns of the condition. This setting is not dependent on the value of *AutoCleanupDatabase* and the cleanup process is **not** initiated when the alert is generated.

- **Type**

This parameter is designed for future versions of InControl which will support different database products. At this time only one type is supported and its location is specified by the *Path* parameter. Neither of these parameters should be changed in the current InControl version.

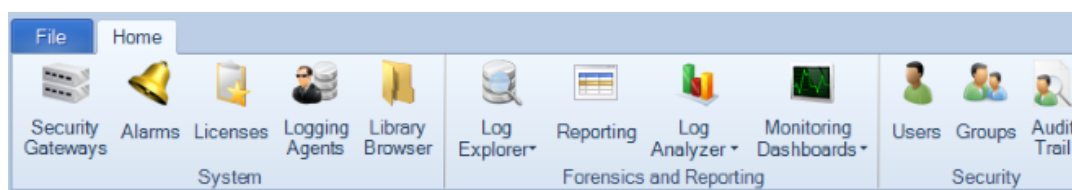
The *SQLite* setting will be used for a future feature and should not be changed. This setting is totally separate from the database settings for the ILA server.

Chapter 5: The Client Interface

The Client Interface Layout

The InControl client interface is built around a series of *Ribbon Toolbars* and associated *Tabs*

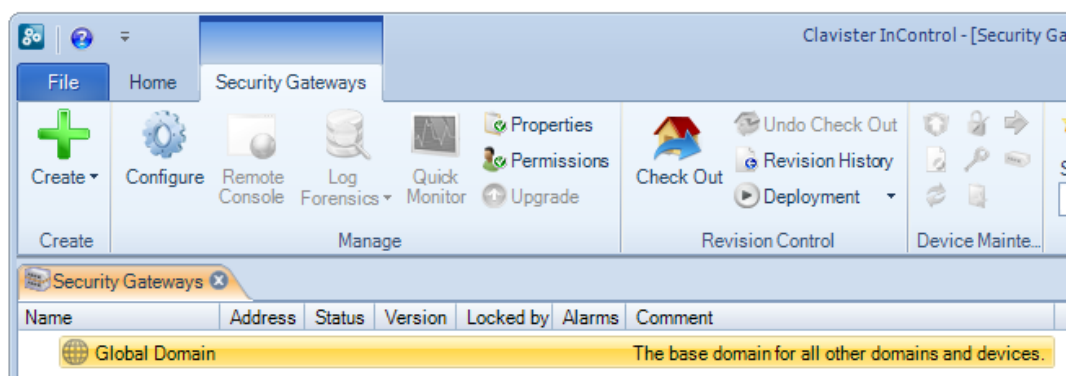
The *Home* tab provides the most important of InControl's functions.



The Security Gateways Tab

The most frequently used of the buttons in the *Home* ribbon toolbar will be the *Security Gateways* button. This will display the *Security Gateways* tab which is the primary means of navigating into the configurations of individual gateways, HA clusters and domains.

When a client starts for the first time, the only entry in this tab's navigation tree is the *Global Domain*. This is the default parent domain for all other security gateways and other domains and provides the ability to create universal objects that can be shared by all the domain's children.



Opening Tabs

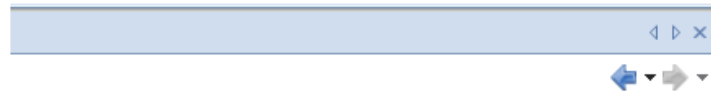
When selected, other functions such as the *Alarms* and *Licenses* cause their own tab to be

opened.



Going Forwards and Backwards in the History

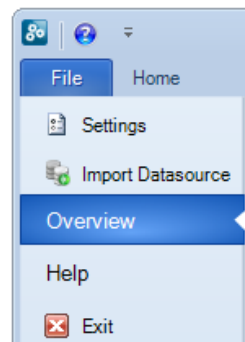
The central pane of the client interface displays the key information related to the currently active tab. The history of what is displayed in this pane is kept in the same way as a web browser. It is possible to go forwards and backwards in this history using the large arrow buttons at the top right (the smaller arrow buttons move through the tabs).



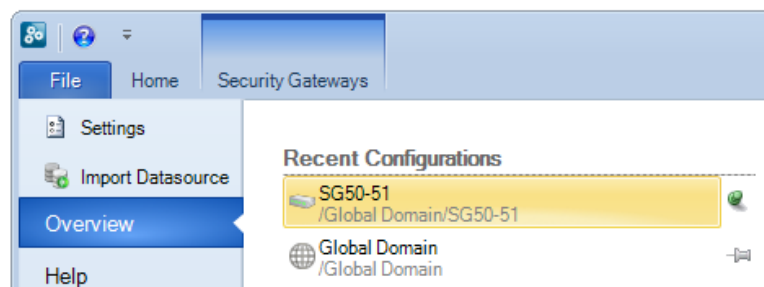
The key shortcut **Alt + Left Arrow** can be also be used to move backwards through the history and **Alt + Right Arrow** moves forward.

The File Tab

The *File* tab provides some general functions relevant to client operation.



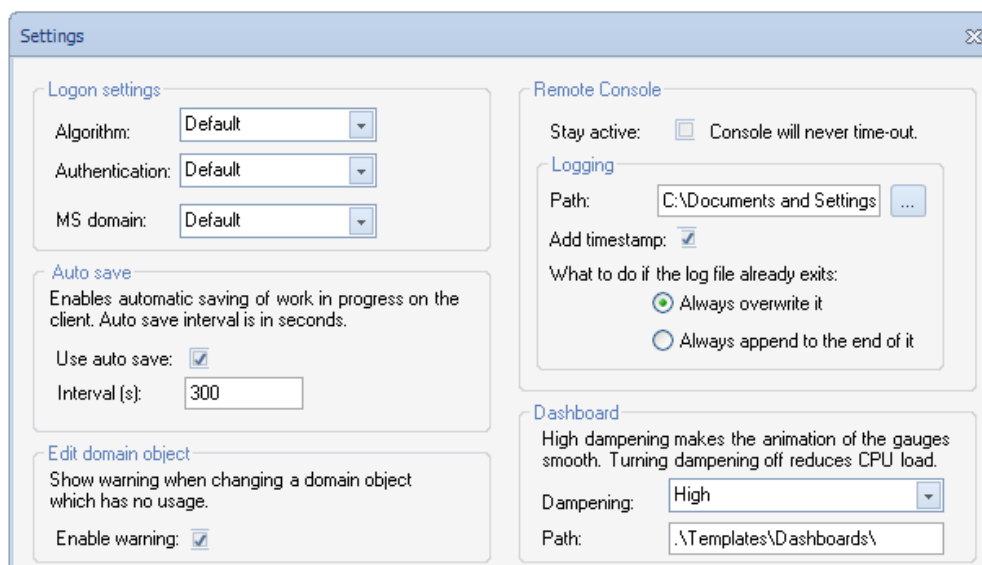
To the right of the menu options, there is a list of the last ten configurations that have recently been opened for editing. Double clicking any of the list will open that configuration for editing.



Once the recently edited list reaches ten entries, the configuration that was edited furthest back in time is lost as a newly edited configuration is added. To change this behavior, the pin icons to the right of the configuration name can be clicked so that the configuration is "pinned" to the list. The *SG50-51* in the example list above has been pinned in this way and now cannot disappear from the list.

Client Settings

By choosing the **Settings** option, the client preferences dialog will appear. This allows a number of general preferences for the client to be changed.



The different parts of this dialog are discussed next:

A. Client Logon settings

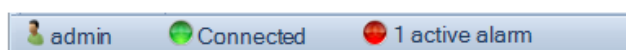
The settings in the first section of the client settings dialog relate to the initial client logon:

- **MSDomain**

This decides the authentication source:

- Internal* - The username/password is authenticated against the InControl server's internal database. No external server is used.
- MSDomain* - The username/password is authenticated against a connected Windows *Active Directory* server. No InControl login dialog is displayed and credentials do not need to be entered.
- Auto* - The *MSDomain* option is tried first. If no active directory server is found then the *Internal* option is used and the login dialog is displayed for credentials to be entered.

The default value for this setting is *Auto*. After successful logon, the authentication source is always indicated at the bottom-left of the InControl client interface. For example, if the source was internal with the user name of *admin*, the interface would appear as below:



Important: The MSDomain option requires further configuration

The **MSDomain** option for client logon requires the following additional steps:

- A new user group is added in the InControl client which associates the active directory group which the client belongs to with the relevant privileges.
- In the InControl server settings interface, the **AuthenticationMethod** option must

be set to **MSDomain**.

- The InControl client **ICC.exe** command line must be appended with the additional **-AuthenticationMethod** option set to **MSDomain** and the **-Host** option set to the IPv4 address of the InControl server.

These steps are described in detail in **Chapter 15, User Accounts and Groups**.

- **Authentication**

If login authentication is performed with the *MSDomain* option, this is the protocol used to communicate with the Windows Active Directory server. The default value is *Negotiate*.

- **Algorithm**

This is the encryption algorithm used to communicate with the InControl server. Different algorithms have different advantages/disadvantages. The default value is *Rjindael*.

B. The AutoSave Function

The *Autosave* function in the client settings dialog provides a way to routinely save any changes made to data in the client to the local disk. This means that any work done, for example 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 the *AutoSaveInterval* value specifies the time between saves.

C. Edit Domain Object Warning

This setting in the client settings dialog controls a warning message that appears when editing any domain object that is not used by any of the security gateways within that domain.

Flagging unused objects is explained further in *Chapter 14, Domains*.

D. Remote Console Settings

These options in the client settings dialog affect how the remote console functions. They are:

- **Never time-out** - By default, a InControl remote console session will automatically disconnect after a certain period of inactivity. Enabling this option disables the time-out.
- A InControl remote console session can be copied to a logging file. The following options can be set:
 - **Path** - This is the location of the file that is created for the log. The log file name is of the form: *<gateway-name>_log.txt*.
 - **Add timestamp** - A timestamp is added to the beginning of each line in the log file.
 - **Always overwrite/append** - Determines if old log data for the gateway is overwritten every time logging is enabled.

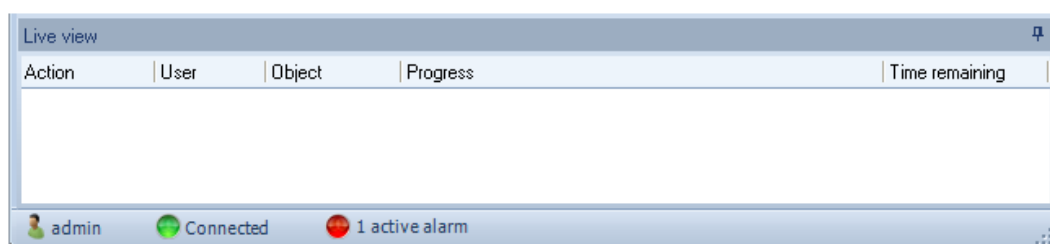
See *Chapter 16, Remote Console* for more details about the InControl console.

E. Dashboard Dampening

The client settings dialog allows the graphical refresh rate ("dampening") of the dashboard controls to be altered. The smooth change of dashboard controls during monitoring can consume significant processor resources and this may have to be reduced if the processor is heavily loaded.

The Progress View Panel

During an operation that requires a waiting period, such as the deployment of a new configuration, the *Progress View Panel* will appear, sliding up into the lower portion of the client window.



This panel displays the progress of the following server related operations:

- Adding a gateway or logging agent.
- Checking in a gateway.
- Deploying a gateway or logging agent configuration.
- Uploading or downloading a cOS Core version.

Each operation is displayed in a list in the *Live View* panel with a progress bar initially displayed under the *Progress* column along with a *Time remaining* estimate. For example, checking in and deploying the gateway called *My_GW* would result in the following.

Action	User	Object	Progress	Time remaining
Check in	admin	My_GW	Completed at 12:57:53	Done
Deploy	admin	My_GW	<div style="width: 100%; background-color: green;"></div> 100%	Done

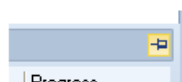
After all operations are completed, they remain in the *Live View* list for approximately 20 seconds before being removed.

Action	User	Object	Progress	Time remaining
Check in	admin	My_GW	Completed at 12:59:49	Done
Deploy	admin	My_GW	Completed at 12:59:54	Done

The *Live View* panel can be displayed at any time using the *Live View* button.



By default, the panel slides out of view when no operations are in progress. However, it can be locked in place by using the pin button in the corner.



The *Live View* panel displays operations not only for the local client but for all clients connected to the server.

Client Runtime Options

It is possible to specify a number of options when running the InControl client. The client executable file has the name *ICC.exe* and any option parameters follow the *ICC.exe* console command, separated by a space from their assigned value. For example:

```
ICC.exe -host 192.168.1.22 -username myname -password mypswd -silent true
```

Adding any options is best done by locating the InControl client option in the Windows **Start** menu, right clicking it and then selecting **Properties** to edit the initiating Windows console command. Alternatively, a console could be opened and the command could then be entered with the desired options.

The available options are as follows:

- **-Help**

For use in a console, this displays all the available command options. The option **-?** can also be used instead to list available options.

- **-AuthenticationMethod**

This can be set to one of the following:

- Internal** - No active directory server is used)
- MSDomain** - Only use an active directory server)
- Auto** - The default setting, if no active directory server then use internal)

These values are further explained above in the section on client logon settings. For logon using an active directory for authentication, this setting must be specified and doing this is described in *Chapter 15, User Accounts and Groups*.

- **-Host**

This is the URL or IP address of the InControl server.

- **-Port**

This is the port number to be used when connecting to the InControl server.

- **-Username**

The username to be used at client startup.

- **-Password**

The password to be used at client startup.

- **-MSDomainType**

Possible values:

ntlm

kerberos

negotiate (the default)

These values are explained above in the section on client logon settings.

- **-Algorithm**

Possible values:

DES

TripleDES

RC2

Rjindael (the default)

These values are explained above in the section on client logon settings.

- **-Silent**

Possible values:

Yes/True/1

No/False/2 (the default)

When enabled this suppresses the appearance of the client logon screen. Both the *-Username* and *-Password* options must also be specified to use this option.

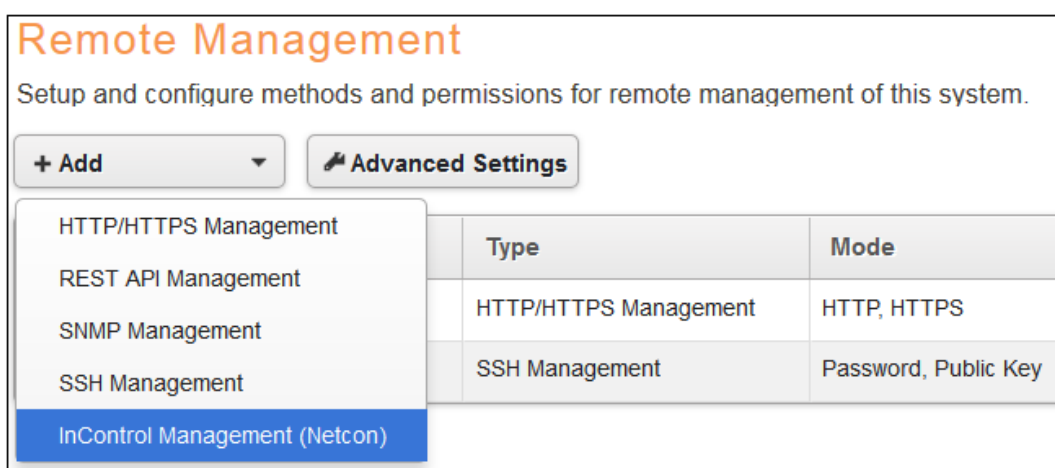
Chapter 6: Preparing cOS Core

Before a Clavister Security Gateway can be brought under InControl control, a *Remote Management* object that allows that control must be created in the cOS Core configuration of the security gateway. This chapter describes how that object is created and configured.

Creating a Remote Management Object

To create the *Remote Management* object, use the following steps:

1. Open the cOS Core management Web Interface in a browser.
2. Log in directly to cOS Core.
3. Go to **System > Device > Remote Management**.
4. Select the **Add** option.
5. Choose *InControl Management (Netcon)* from the list of *Remote Management* object types, as shown below.



Type	Mode
HTTP/HTTPS Management	HTTP, HTTPS
SSH Management	Password, Public Key

This will open up the properties display for the new *InControl Management* object. This is shown below with some example values already entered.

InControl Management (Netcon)

Configure Netcon management to enable remote management to the system.

Mode:

Idle timeout:

PSK:

Access Filter

Interface:

Network:

The configured properties are the following:

- **Mode**

The following options are available: This is normally set to *Configure* which allows complete control.

- Configure** - This is the normal setting and allows InControl complete control over the configuration.
- Console** - This allows full control but the configuration can only be administered through InControl's console function.
- Uptimepoll** - This allows cOS Core to only respond to ICMP ping messages from InControl so that the online status of the security gateway is correctly displayed.

This chapter will assume throughout that the *Mode* property is set to the value *Configure*.

- **Idle Timeout**

After this many seconds of inactivity, the connection is closed.

- **PSK**

This is a *Pre-Shared Key* object that specifies the hexadecimal key that secures communication between InControl and cOS Core. This key must agree with the value of the *Secret Key* property of the corresponding gateway object in InControl. Creating this object is described in *Appendix B, Netcon Key Generation*.

- **Interface**

The Ethernet interface on which InControl connections will be accepted.

- **Network**

The single IP or range of source IPs from which InControl connections will be accepted.

The Gateway Initiated Netcon Option

The Clavister Security Gateway itself can initiate addition to InControl by enabling the *Gateway Initiated* option. This allows another set of related properties to be set for the object, as shown below.

Gateway Initiated

Gateway Initiated: ☒

InControl Server IP:

InControl Server Port:

Remote Management ID:

The additional properties for gateway initiated Netcon are the following:

- **InControl Server IP**

This is the IP address of the InControl server which cOS Core will automatically try to contact.

- **InControl Server Port**

The port number is used for connection on the InControl server. This default port number is 998.

- **Remote Management ID**

Since the Clavister Security Gateway may be behind a NATing network device, InControl cannot use the security gateway's IP address in order to add it to the list of managed devices. Instead of the IP address, this *Remote Management ID* value will be used as the ID for the gateway and this must be specified when the gateway is defined in InControl. The value entered must match the value of *Remote Management ID* specified for the corresponding *Remote Management* object in cOS Core.

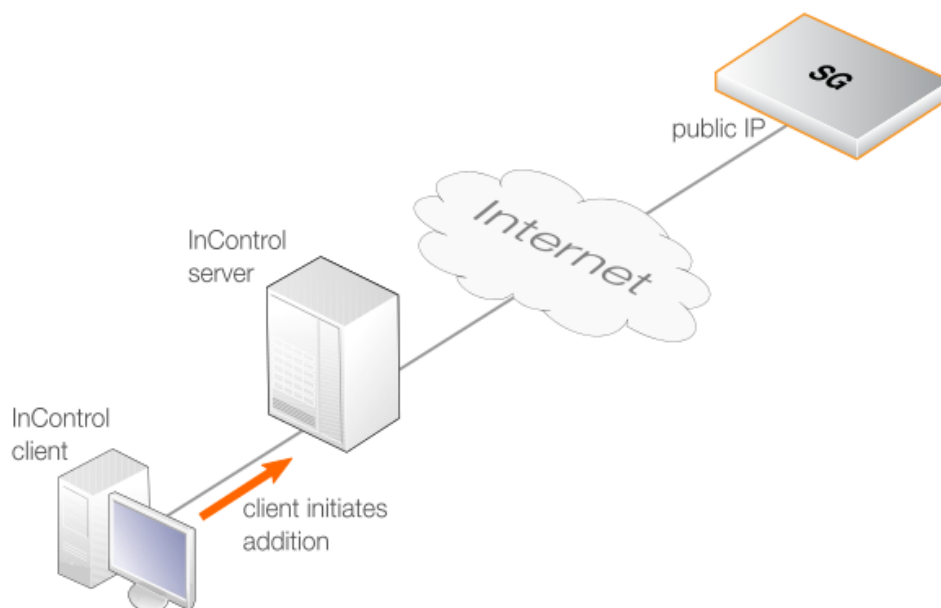
When to Use Gateway Initiated Netcon

There are two methods for how a Clavister Security Gateway can be added to InControl and brought under its control:

- **InControl Initiates Addition**

This is done by first adding a *Remote Management* object to cOS Core then adding the gateway through the InControl client (described in *Chapter 7, Adding Security Gateways*). This method is also known as *Server Initiated Netcon*.

The communications between the InControl server and the security gateway might be across the Internet and this is illustrated in the diagram below. In this case, the security gateway must have a static public IP address since InControl is initiating the communication.



Note: The InControl server IP type does not matter

With above method of adding a gateway through the InControl client, it does not matter if the InControl server has a public IP address or is behind a NATing device with a private IP. However, the IP address of the gateway should be static. Any changes to the gateway's IP address must also be made to the gateway's properties in InControl.

• **The Clavister Security Gateway Initiates Addition**

If the Clavister Security Gateway has a private IP address and is behind a NATing device, the InControl server will not be able to connect to it across the Internet because it does not have a public IP. In this case, the approach described above will not work. Instead, cOS Core must be configured so that it initiates the addition to InControl control. This cOS Core feature is called *Gateway Initiated Netcon* (where *Netcon* is the proprietary Clavister protocol used between the InControl server and cOS Core).

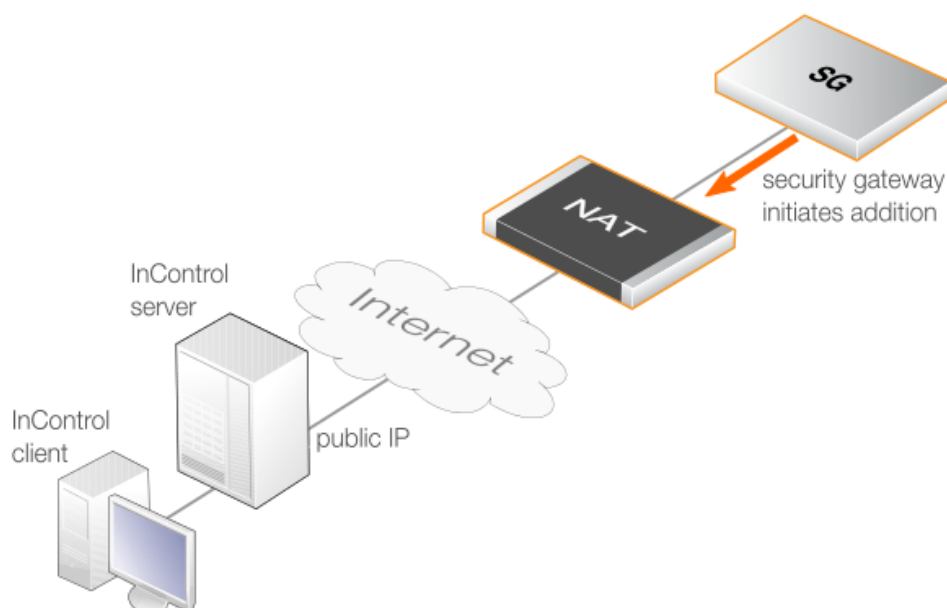
An alternative situation where this approach should be used is when the gateway is not behind a NATing device but its IP address can change and is not known at a given point in time. In either case, *Gateway Initiated Netcon* means that the gateway does not need a static IP address and it can find the InControl server instead of the other way around.

Gateway initiated Netcon requires the following:

- i. As usual, a *Remote Management* object must be created in the cOS Core configuration but with the *Use Gateway Initiated Netcon* option enabled. Doing this is described later in this chapter.
- ii. A corresponding *Gateway* object must then be created in InControl that has the *Reverse Management* option enabled and has the same *Secret Key* and *ID* values as those specified in the cOS Core *Remote Management* object.
- iii. It also requires that the InControl server has a static public IP address if management traffic traverses the Internet. This IP is specified in the *Remote Management* object so that cOS Core can contact it and register that it is ready to be added.

The gateway initiated Netcon option is intended for use only if the security gateway is behind a NATing device. Otherwise, the standard method of security gateway addition should be used. The appropriate scenario for gateway initiated Netcon usage is illustrated in the

diagram below.



Steps for Setting Up Gateway Initiated Netcon

When setting up gateway initiated Netcon, the following ordering of steps must be followed:

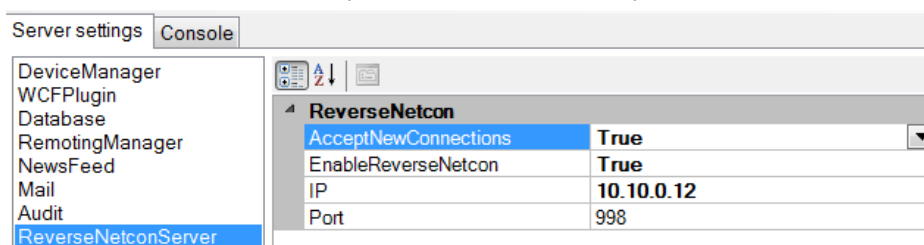
1. Create a Remote Management object in cOS Core

Once the *InControl Management* object is configured and activated, if the *Use Gateway Initiated Netcon* option is enabled the cOS Core will immediately try to contact the specified InControl server. This will be done repeatedly at 5 second intervals until successful.

2. Enable Netcon in the InControl Server Interface

Gateway Initiated Netcon must be explicitly enabled for the InControl server. This is done with the following steps:

- i. From the Windows *Start* menu, select *Clavister > Clavister InControl Server Settings* to open the server interface. Administrator rights will be required for changes.
- ii. Select the *ReverseNetconServer* options from the left-hand pane, as shown below.



- iii. In the right-hand pane, set *AcceptNewConnections* and *EnableReverseNetcon* to a value of *True*. If a specific server interface is to be used for accepting incoming gateway connections then the IP address of that interface should be specified in the *IP* field. If any interface can be used, the *IP* field should be set to *0.0.0.0*. The port for connections defaults to 998.

- iv. Select *File > Service > Restart* to restart the server. The server interface will prompt to save the changes before restarting the service.

Note that if the *AcceptNewConnections* option is disabled and *EnableReverseNetcon* is enabled, reverse Netcon will function but no new gateways can be added to InControl.

3. **Create a Gateway object in InControl**

A corresponding *Gateway* object must now be created using the InControl client and this **must** be done after the *Remote Management* object is created. When specifying the InControl properties for the gateway, the following is entered:

- i. The *Online* option should be enabled for the status.
- ii. The option *Gateway Initiated* option must be enabled.
- iii. The *Remote Management ID* property must match the *Remote Management ID* property specified in the cOS Core *Remote Management* object.
- iv. The *Secret Key* property must match the hexadecimal key of the *PSK* specified in the cOS Core *Remote Management* object.

Creating gateways for both methods of addition in InControl is further described in *Chapter 7, Adding Security Gateways*.

4. **cOS Core finds and adds the polling gateway**

Once the InControl *Gateway* object is created, InControl will look for a matching Clavister Security Gateway that is polling the InControl server. When it finds the match, it will add the device as a managed gateway. This InControl client interface will then display the gateway's ID instead of its IP address. The IP address will remain unknown and is not needed for communication between InControl and the managed gateway.

Once the Clavister Security Gateway is added using gateway initiated Netcon, it can be managed just like a gateway that is added to InControl in the normal way.

Chapter 7: Adding Security Gateways

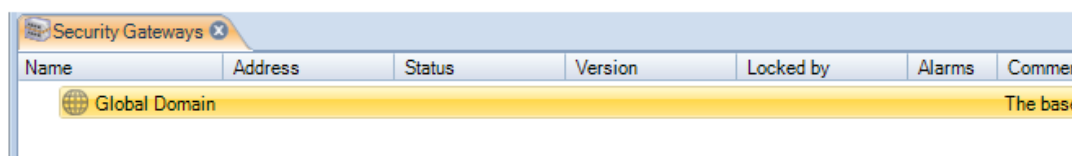
Usually, first task after installation of InControl is adding a Clavister Security Gateway so that it comes under InControl control. The major steps when adding a security gateway are the following:

- Log in as an administrator to cOS Core and create a *Pre-Shared Key* (PSK) object that defines the hexadecimal key InControl will use and then define a *Remote Management* object that allows InControl access and that uses the *Pre-Shared Key* object. This step is described fully in the previous *Chapter 6, Preparing cOS Core*.
- Open the InControl client and add the Clavister Security Gateway, including the key from the *Pre-Shared Key* object created in the previous step. This chapter describes this second step in detail.

To add a security gateway through the InControl client, press the *Security Gateways* button in the main ribbon toolbar.



This opens the *Security Gateway* tab in the client's central panel.



Before any gateways are added, the tab contains only the *Global Domain* which is the parent for all sub-domains or security gateways. The *Global Domain* has its own set of configuration values which can be applied to all of its children.

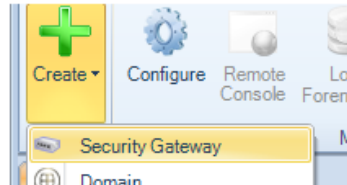


Tip: Only add to the Global Domain when necessary

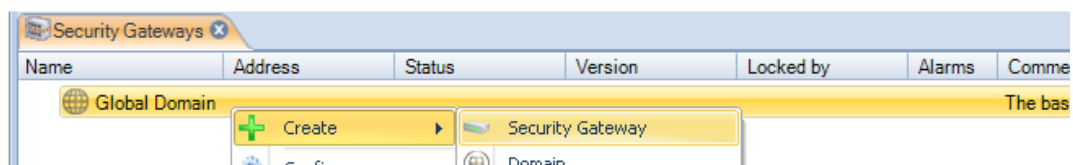
For the fastest InControl response times, only keep objects in the Global Domain when necessary. If an object is only used in one gateway, keep the object just in that gateway's

configuration.

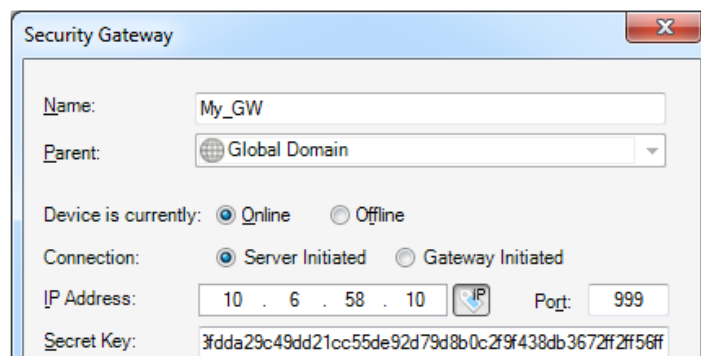
Above the tab, is a new toolbar for security gateway specific operations. Press the plus button followed by selecting the *Security Gateway* option in the menu to add the new gateway.



Alternatively, this step could be done by right clicking the *Global* domain node in the *Security Gateways* tab and choosing *Security Gateway* from the *Create* menu.



The *New Security Gateway* dialog will now appear and the properties of the gateway can be entered. In this example, the new security gateway will be called *My_GW*.



The name, IP address and secret key of the security gateway is 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.

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



Tip

To move between sections 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.



If the gateway is being added using *Gateway Initiated Netcon* (the gateway initiates the addition) then the *Gateway Initiated* option (shown below) should be selected and the *Remote Management ID* that is specified in the corresponding *Remote Management* object in cOS Core should be used instead of the IP address. This is discussed further in the previous *Chapter 6, Preparing cOS Core*.

State: ☒ Online ☐ Offline

Management: ☐ Server Initiated ☒ Gateway Initiated

Remote Management ID:

The *Secret Key* is the hexadecimal *Netcon* key required by cOS Core for communication with InControl (*Netcon* is a secured Clavister proprietary protocol). This key must be the same value as the *Passphrase* property of the *Pre-Shared Key* object in cOS Core which is used with the *Remote Management* object that allows InControl control. Obtaining this key is explained further in *Appendix B, Netcon Key Generation*.

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

Security Gateways					
Name	Address	Status	License	Version	Comment
Global Domain					
The base domain for all other domains and device					
My_GW	10.5.5.233	OK		11.04.00.48	

If we open the *Alarms* tab, there is one alarm line that indicates there is no valid license that allows the gateway to be managed by InControl.

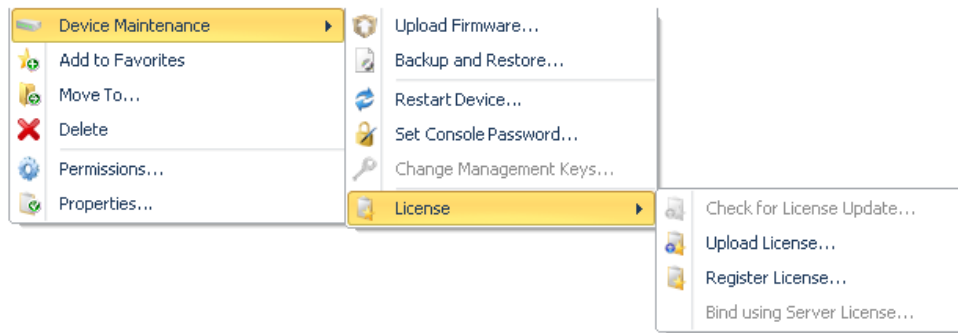
Security Gateways					
Alarms					
Status	Date	Severity	Source	Entity	Description
Warning	2010-11-15 14:44:39	Warning	Management Server	My_GW	Need license to manage Security Gateway from managem...

Binding a License

As explained in Chapter 11, *Licensing* there are a number of licensing options for InControl usage.

- If cOS Core is running in the 2 hour demonstration mode, no licensing is needed.
- If cOS Core has a license then the *CENTRALIZED_MANAGEMENT* option in the license has to be enabled. If this is not the case then an alarm is generated to indicate this as shown above.
- If neither of the above two options is the case then cOS Core has to have a valid *InControl Server 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 and selecting the *Bind to InControl using Server License* option.

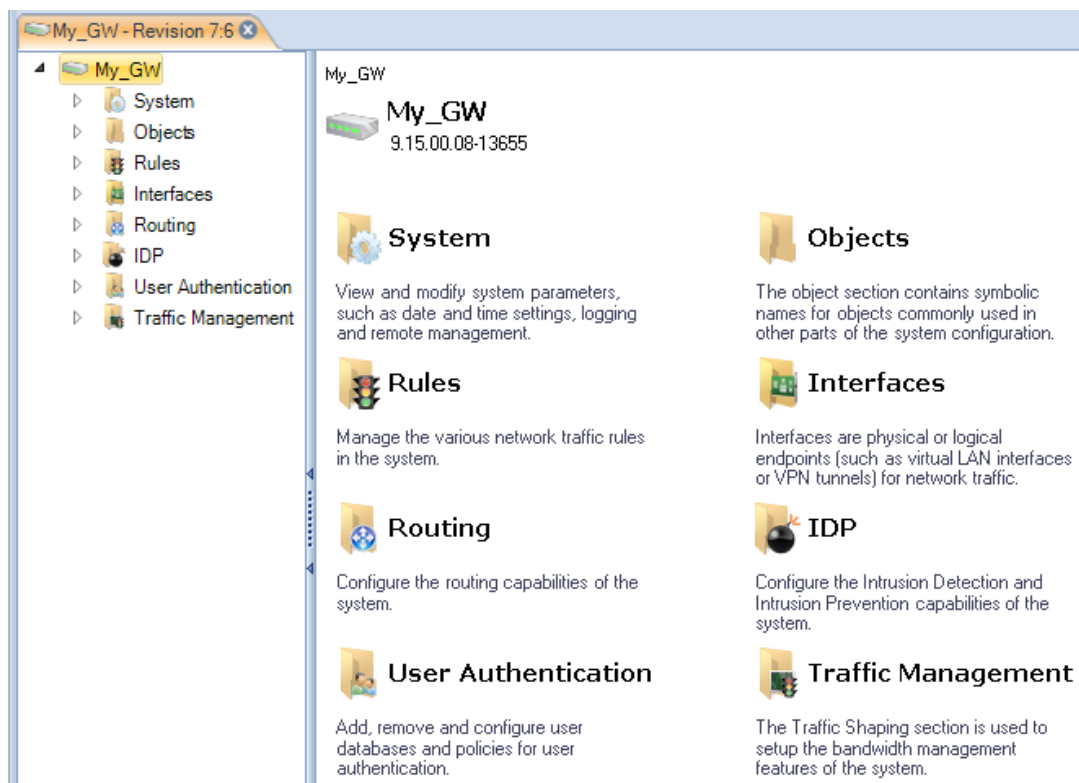


When the gateway is added, an alarm appears in the *Alarms* tab list panel to warn that it is unbound. Binding can also be done by right clicking this alarm in the alarm list and selecting the bind option from the displayed context menu.

Binding gateways to the server license is also discussed in Chapter 11, *Licensing* but is repeated here for emphasis as this step can be forgotten.

Editing the Configuration

By double clicking the new gateway, the object navigation tree opens as a new tab in the central part of the InControl interface.



The tab title text in the example above is *My_GW - Revision 7:6*. The numbers "7:6" represent the number of times this security gateway's configuration has been edited via InControl and non-InControl means. The number to the left of the colon is the number of times the configuration has been edited by non-InControl means. The number on the right is the number of times it has been edited using InControl.

The navigation tree to the left of the tab shows the object hierarchy of the configuration. This will

be structured differently between a cOS Core version and an earlier CorePlus version.



Note: InControl must parse a configuration on initial opens

The very first time an added security gateway's configuration is opened and read by InControl, there will be a brief delay while the configuration is parsed and loaded into the server database. The delay will depend on the processor speed of the InControl server. Subsequent opens will not have this delay.

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.

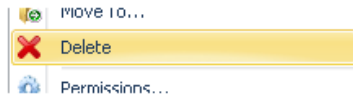
- **Routes**

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.

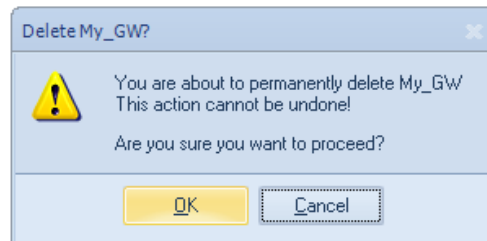
All of the above features are fully described further in the *cOS Core Administrators Guide*. An example of editing a configuration is described later in Chapter 9, *A First Security Policy*.

Deleting Security Gateways

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



A confirming dialog is displayed before the delete is finalized.



It is important to be certain about wanting to delete the gateway there is no undelete following confirmation.

Switching from Online to Offline

In the properties dialog for a security gateway, the administrator has the option to have the device either *Online* or *Offline*. These states can be set either when a security gateway is added to InControl or they can be changed after a security gateway is added. These states are defined as follows:

- **Online**

This is the default state for a security gateway and means that it is under the control of InControl and InControl is communicating with it.

- **Offline**

The *Offline* state means that the security gateway is not under the control of InControl and behaves as an autonomous device. In this state, no changes made in InControl will affect the gateway. The security gateway itself will be unaffected by changing to the *Offline* state and will continue running as though nothing has happened.

Switching to the *Offline* state can only be achieved by the administrator manually changing the state in the InControl interface. It is never done automatically, even if the security gateway is no longer functioning.

A newly added security gateway can be marked as being *Offline*, in which case the IP address and PSK are not needed for addition but will need to be entered later if the state is changed to *Online*.

Switching Back to Online from Offline

If the administrator changes the security gateway status from *Offline* back to *Online*, the following will happen:

- If they have not been previously entered, the security gateway's IP address and PSK must be entered in order to connect to it.
- On connection, InControl will read the current configuration of the security gateway and this will overwrite the current configuration stored in the InControl database and the device will perform a reconfigure operation.

InControl will present the user with a warning that the InControl database will be overwritten and ask if it should continue. It should be noted that will still be possible to later revert the configuration in InControl to the earlier version.

- The security gateway will now be under the control of InControl with no change to its local configuration.
- To revert the, now online, security gateway to a previous configuration, the administrator can select another configuration from the revision history.

Chapter 8: Revision Management

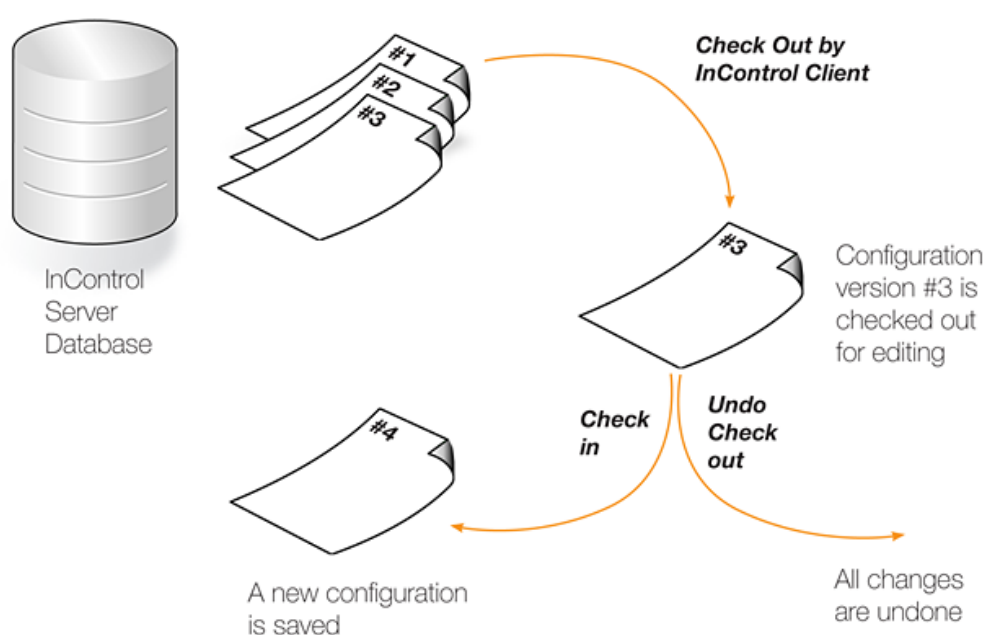
Revision Management is the ability to save and track changes made to cOS Core configurations and is an important tool for managing Clavister Security Gateways. Revision management allows the administrator to keep track of what was changed in configurations, when it was changed, who made the changes and 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.

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.



Note: InControl and Web Interface version control are separate

If version control is performed through InControl, the Web Interface should not be used to upload previously backed up configuration versions. Web Interface backups are independent of InControl.

Once InControl version control is adopted, version control through the Web Interface should not be used.

Checking Out a Configuration

Whenever an administrator wants to start modifying a configuration, the configuration should be first checked out. This can be done as a separate operation but will occur automatically when the first change is made to a configuration.

Checking out can be done separately by pressing the check out button in either the *Security Gateways* tab toolbar or the toolbar for the individual gateway's tab.



Tip: A keyboard shortcut exists for check in/out

*A range of InControl operations can be executed with a keyboard shortcut. For both check out and check in, the short cut is **Ctrl+Shift+C** after selecting the target in the Security Gateways tab.*

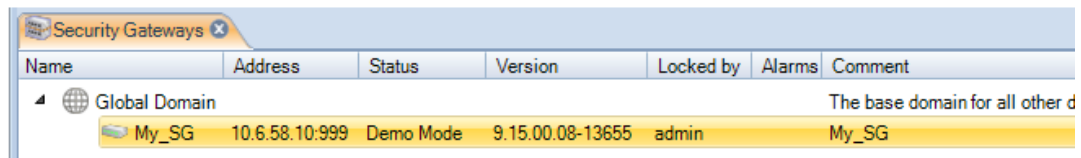
*All available shortcuts are listed in **Appendix D, Keyboard Shortcuts**.*

The administrator who performs the checking out, now gets 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 InControl clients editing the same configuration simultaneously.

In a multi-administrator environment, with multiple InControl clients, the best practice is to try and ensure a configuration is not be checked out for any longer than is absolutely necessary.

Already Checked Out Security Gateways

If a security gateway is already checked out by another InControl client, this is indicated in the *Locked by* column with the name of the user who has performed the check out. In the example below, the user *admin* has already checked out the gateway *My_SG*.

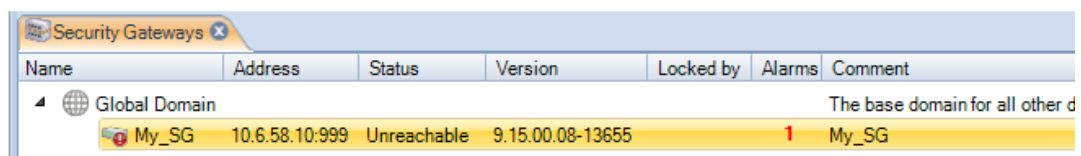


Name	Address	Status	Version	Locked by	Alarms	Comment
Global Domain						The base domain for all other d
My_SG	10.6.58.10:999	Demo Mode	9.15.00.08-13655	admin		My_SG

Since the checking 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 Alarms

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



Name	Address	Status	Version	Locked by	Alarms	Comment
Global Domain						The base domain for all other d
My_SG	10.6.58.10:999	Unreachable	9.15.00.08-13655		1	My_SG

Open the *Alarms* tab to investigate this further. In the above example, the status of the gateway is *Unreachable* which may be the cause for the alarm. This topic is discussed further in *Chapter 12, Alarms*.

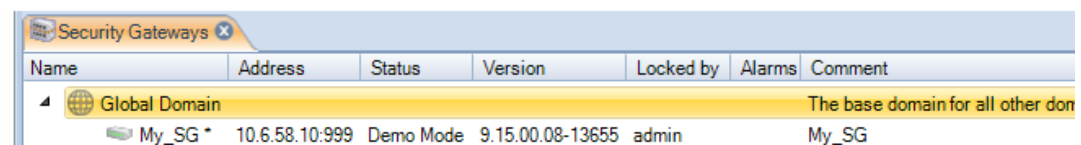
Automatic Check Out

If a security gateway has its configuration changed in some way without first checking out the unit, the gateway is automatically checked out by InControl. If the unit is already checked out by someone else, it is only possible to read configuration information.

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.

If a gateway's configuration has been changed, this is shown by an asterisk appearing next to the gateway's name in the *Security Gateways* tab.



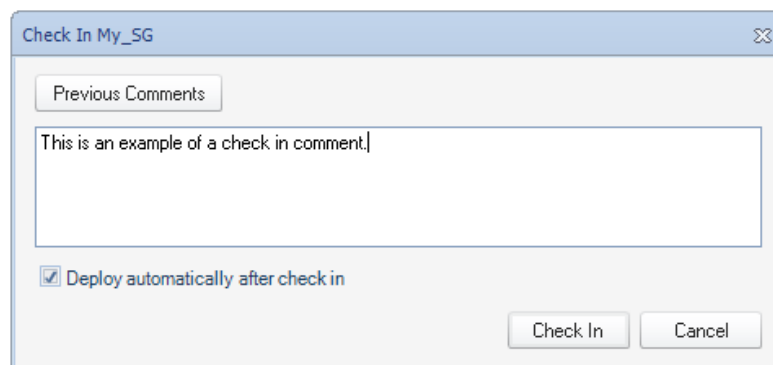
Name	Address	Status	Version	Locked by	Alarms	Comment
Global Domain						The base domain for all other don
My_SG *	10.6.58.10:999	Demo Mode	9.15.00.08-13655	admin		My_SG

Check in can be done by pressing the *Check In* button for the gateway.



To complete check in, a dialog appears to confirm the check in and ass a comment. It is recommended that the administrator add a comment for each check in. This provides an easy

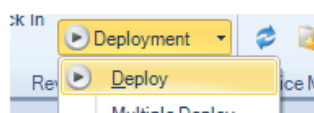
way to identify changes in the revision history.



This dialog also provides the option to automatically deploy the configuration at the same time that the check in occurs. This option is disabled by default but enabled in the example above.

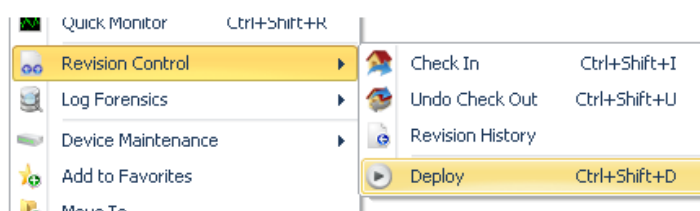
Deploying Changes

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 selecting the deploy option.



Using deploy will cause all configuration changes since check out 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 that appear in a bottom panel in the client interface.

Like many other option, a deploy can also be initiated by right clicking the gateway in the *Security Gateways* tab and selecting the option in the context menu.



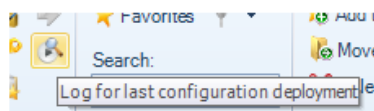
If the InControl client is closed before configuration changes are deployed, those changes are still saved between client sessions. When that same InControl client is started up, undeployed changes will still be visible in the client's view of the configuration.

Checking for Deployment Problems

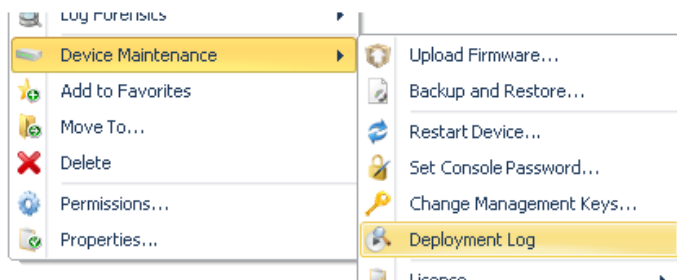
If there is an problems in the configuration that prevents deployment, the InControl client will indicate this by automatically displaying the *Deployment Log Dialog*.

However, some configuration problems are not so serious that they prevent deployment but still result in a warning message. These warnings are also shown in the *Deployment Log Dialog* but this time it is not shown automatically. Instead, the log can be viewed at any time after

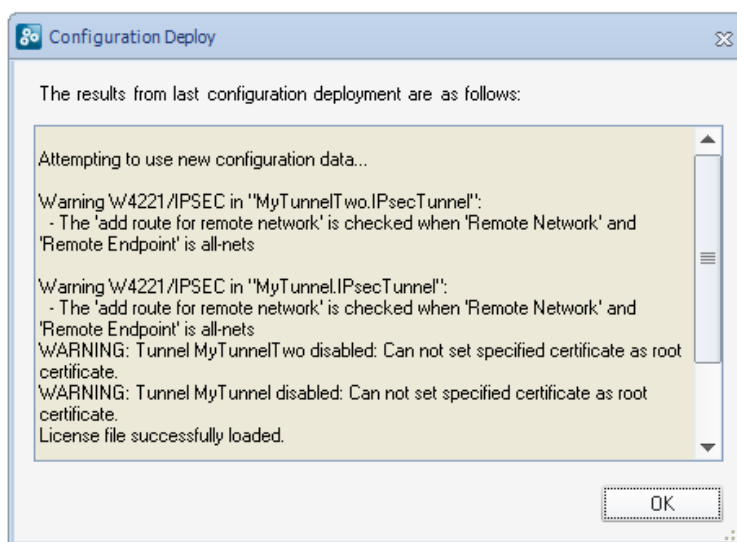
deployment by pressing the *Deploy Log* button in the toolbar.



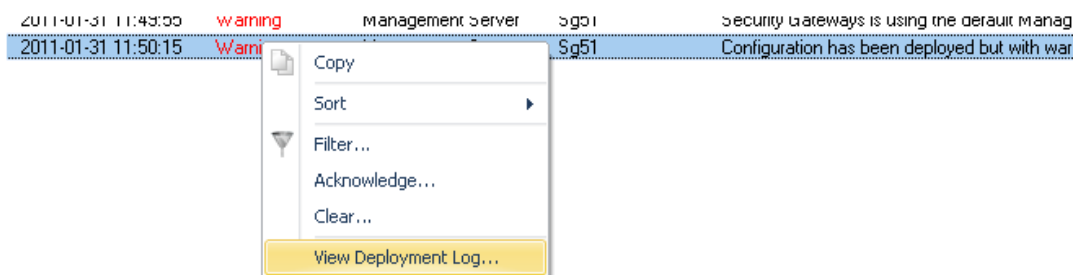
This option can also be selected through the context menu for a gateway in the *Security Gateways* tab.



An example of the *Deployment Log Dialog* is shown below. This shows warning messages relating to issues with the IPsec tunnels *MyTunnel* and *MyTunnelTwo*.



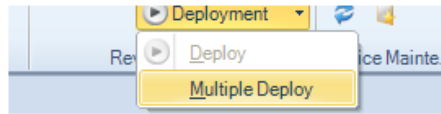
If a deployment has any errors or warnings, a single alarm will be generated and this will appear in the *Alarms* tab. The deployment log can also be viewed by right clicking this alarm and selecting the *View Deployment Log* option.



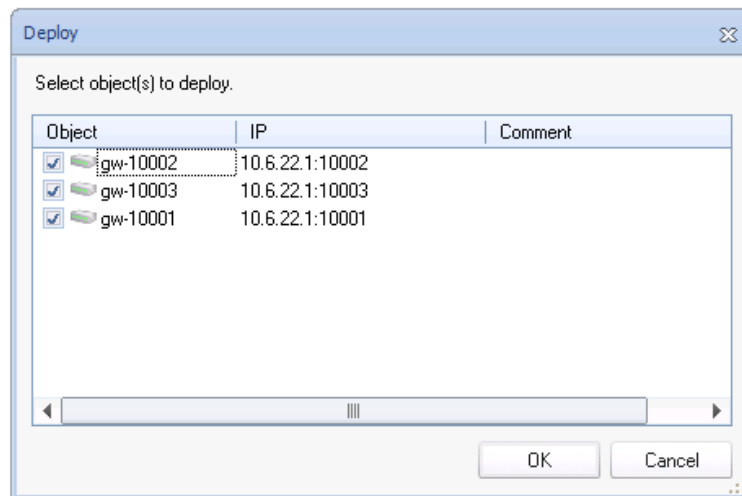
Deployment logs are always fetched directly from a security gateway so the deployment may have been initiated from the Web Interface or CLI. Also, the log only relates to the last deployment made for a gateway.

Deploying Multiple Configurations

An alternative to using the deploy button is to choose the *Multiple Deploy* option.

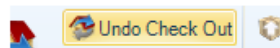


This will display a dialog that lists the changed configurations that are yet to be deployed so that individual entries in the list can be selected for deployment. By default, all the changed gateways are selected in the displayed list.

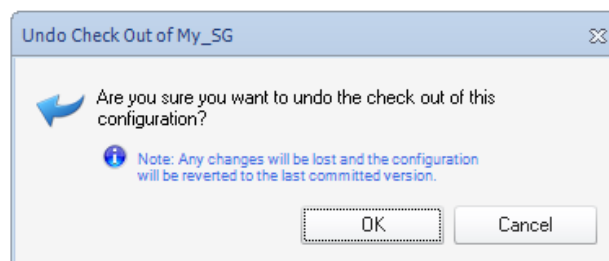


Undoing Check Out

In the event that a configuration is checked out and changes are made but the changes are to be discarded while the check out is reversed, pressing the *Undo Check Out* button can achieve this.

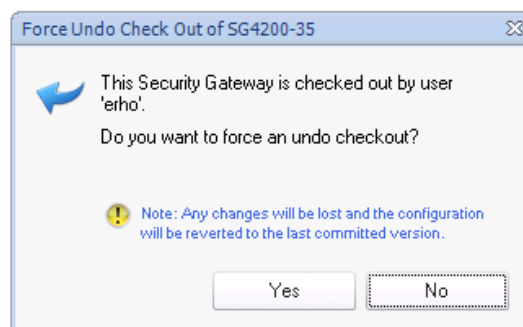


The following dialog is displayed if this option is chosen:



Forcing Undo Check Out

A user in the *administration* group can force the undoing of a checkout by any other user. This is done by choosing the *Undo Check Out* option which will result in this dialog.



Checking In Domains Changes

Domains such as the Global Domain, can be checked out, modified and deployed just like a security gateway. However, when a domain is checked out, any child domains or security gateways are **not** automatically also checked out.

When a domain is checked in and one or more gateway configurations inherit changed objects from the domain, an alarm is raised for the affected gateways. These gateways then need to have their configurations manually deployed to have the domain changes take effect (deployment does not need a gateway to be also checked out).

If a gateway that inherits changes is checked out then such a deployment cannot take place. In this case, any inherited changes will be queued on the InControl server. The next time the gateway has its configuration deployed following check-in, the queued changes are applied.

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 warning message to tell the user that something has changed. The message gives the user the option to update their view of the configuration and this is the recommended action.

However, it is strongly recommended when using InControl that all configuration changes are made through the InControl client and using the Web Interface or CLI is avoided. This will also mean that the InControl audit log correctly reflect all configuration changes made.

Revision History

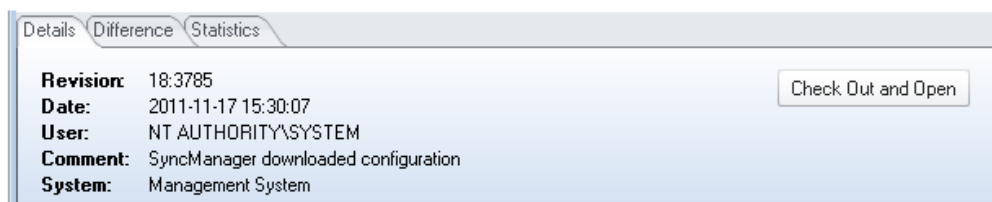
In the *Revision Control* option of the context menu for a security gateway is the *Revision History* option.



Selecting this brings up the *Revision History* tab which lists all the configuration changes made.

Revision	Date	User	Comment	System
18:3785	2011-11-17 15:30:07	NT AU...	SyncManager downloaded configuration	Management System
18:3784	2011-11-17 15:28:38	NT AU...	SyncManager downloaded configuration	Management System

By selecting a particular revision, a summary of that revision can be displayed at the bottom of the *Revision History* tab.



The button **Check Out and Open** allows any revision in the history to be opened. It can then be viewed, even changed and then it can be deployed to the gateway. If it is deployed, it becomes the current configuration and moves to the top of the list in the *Revision History* tab.

By selecting the *Difference* tab, the difference between the selected configuration and its predecessor can be seen.

Results	Revision 18:3777	Revision 18:3783
br_lan.IP4Address		
Device		
main.RoutingTable		
apa1_copy.IP4Address		<added>
apa1.IP4Address		<added>

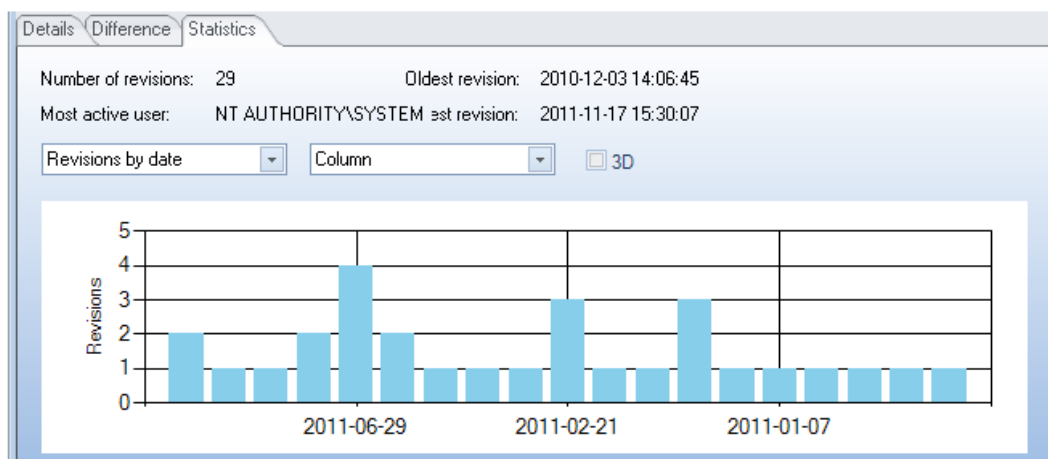
Additions and deletions are marked as such. A change appears in blue and the old and revised values are shown in their respective columns. Expanding the node at the left can reveal more detail about the change.

Device	RemoteCnfVersion	ConfigUser	ConfigDate
br_lan.IP4Address	3777	3783	
Device			
RemoteCnfVersion	3777	3783	
ConfigUser	NetconManagement10.6.40...	NetconManagement10.6.40...	
ConfigDate	2011-09-01 23:06:29	2011-11-08 19:39:36	
main.RoutingTable			
ana1_conv.IP4Address			

By holding the **Ctrl** key down, multiple, possibly non-sequential revisions can be selected in the *Revision History* tab and the differences between them is displayed in multiple columns in the *Difference* tab. In the example below, three revisions have been selected for comparison.

Details Difference Statistics			
Results	Revision 18:3774	Revision 18:3773	Revision 18:3772
[-] DeleteThisObject.IP4_			<deleted>
[-] Device			
RemoteCfgVersion	3774	3773	3772
ConfigUser	NetconManagement10.6.15...	NetconManagement10.6.15...	NetconManagement10.6.15...
ConfigDate	2011-06-29 16:49:05	2011-06-29 14:17:04	2011-06-29 14:00:59
[-] RemoteMgmtSettings			

The *Statistics* tab provides the ability to see graphical representations of revision changes by date or by user. An example of a typical bar chart presentation is shown below.



Revision History Node ID Changes for HA Clusters

When examining the revision history of an HA cluster, the **Node ID** can either be zero or one. If this ID changes between revisions on the history, it is not a cause for concern.

The value of the *Node ID* reflects which unit in the cluster was changed first. Zero indicates the master and one indicates the slave. If all changes are performed under the control of InControl, the *Node ID* will remain constant.

However, if changes are made outside of InControl then the *Node ID* can change in the revision history. Such changes might be made with the Web Interface or the CLI but may also come from cOS Core version changes performed outside of InControl.

Chapter 9: A First Security Policy

The *IP rule sets* are one of the most important cOS Core components and are used to define the basic *security policies* of a cOS Core 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 cOS Core 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 cOS Core 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 a specific installation.

When InControl is started, the security gateway *My_SG* will appear in the *Security Gateways* tab.

Security Gateways						
Name	Address	Status	Version	Locked by	Alarms	Comment
Global Domain						The base domain for all other d
My_SG	10.6.58.10:999	Demo Mode	9.15.00.08-13655			My_SG

All ICMP Traffic is Initially Dropped

Let us show that the initial cOS Core 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.

```

C:\WINNT\system32\cmd.exe

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 cOS Core is ignoring the ICMP protocol packets, and the *Ping* command returns the *Request timed out* message.

Adding an IP Rule

The steps to add an IP rule that allows cOS Core to respond to *Ping* requests are as follows:

1. First, check out the *My_SG* gateway by pressing the *Check out* button.



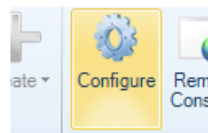
2. Providing no other InControl client has *My_SG* checked out, the check out will succeed and the current user, in this case *admin*, will appear as the locking user.

Security Gateways						
Name	Address	Status	Version	Locked by	Alarms	Comment
Global Domain						
My_SG	10.6.58.10:999	Demo Mode	9.15.00.08-13655	admin	1	My_SG

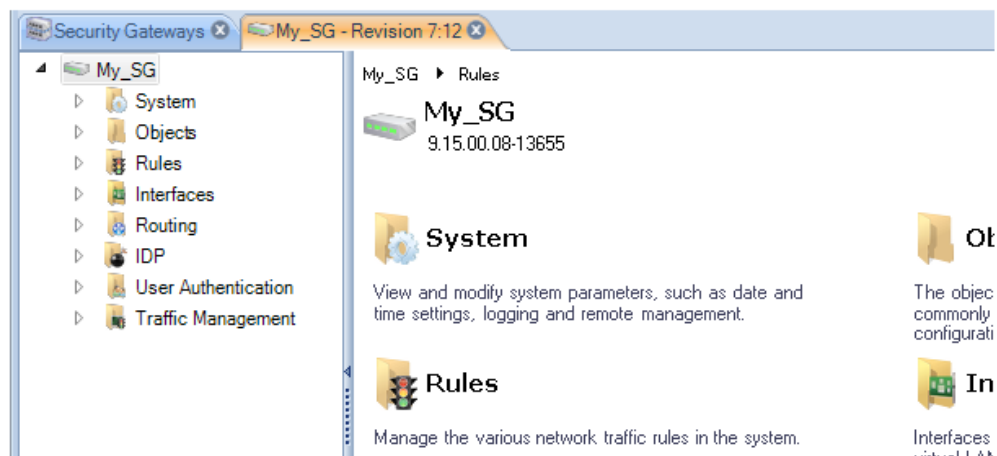
3. The check out event will also be automatically logged in the *Audit Trail*.

Security Gateways Audit Trail							
Time	Severity	User	Category	Acti...	State	Entity	Comments
2010-11-17 10:40:47	Informational	admin	VersionControl	CheckOut	Success	My_SG	Object My_SG was checked
2010-11-17 10:39:51	Informational	admin	Authentication	Login	Success		Access granted for admin

4. Now, display the configuration tab for *My_SG*. This can be done in one of two ways:
- Double click the *My_GW* line in the *Security Gateways* tab.
 - Press the *Configure* button in the *Security Gateways* toolbar.



5. Select *Rules* from the configuration.



6. The gateway configuration tab is now displayed and *IP Rule Sets* can be selected.

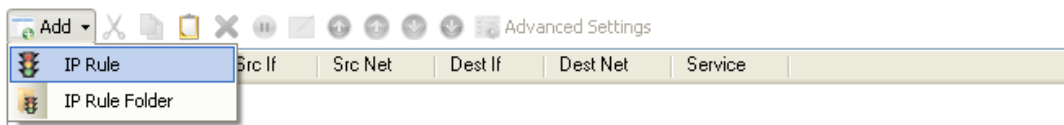


7. A list of IP rule sets is now displayed with the default *main* rule set as the only member.

Name	Comments
main	The main IP ruleset of the system.

8. By selecting the *main* IP rule set we get a list the IP rules in it. Initially it is empty which is equivalent to dropping all traffic without any logging.

By pressing the *Add* button for this rule set, a new rule can be defined to allow *Ping* requests.



9. Now, define the IP rule that will allow traffic. First, define the *General* rule properties. Any suitable name can be specified, in this case *MgmtPing*.

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

Name:	<input type="text" value="MgmtPing"/>
Action:	<input type="text" value="Allow"/>
Service:	<input type="text" value="all_icmp"/>
Schedule:	<input type="text" value="(None)"/>

10. Next, 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 many of the security policy rule sets in cOS Core.

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 cOS Core that will respond.

	Source	Destination
Interface:	<input type="text" value="lan"/>	<input type="text" value="core"/>
Network:	<input type="text" value="lanet"/>	<input type="text" value="all-nets"/>

11. If required, enable the sending of log messages when this IP rule is triggered. This is done by selecting the *Log Settings* tab and enabling the option.

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



Note: A log receiver needs to be defined

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

12. 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

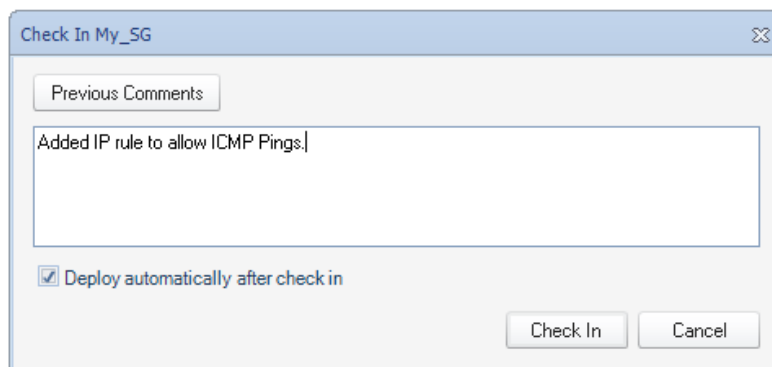
next step.

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

13. Finally, check the new configuration in and deploy it. This can be done in a single step, by pressing the *Check In* button.



14. The check in dialog allows a comment and also the option to deploy in the same operation.

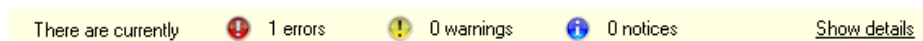


The audit log shows that the two operations of check in and deploy have taken place.

Time	Seve...	User	Category	Action	State	Entity	Comments
2010-11-17 12:49:43	Informational	admin	Configuration	Write	Success	My_SG	Configuration Wri
2010-11-17 12:49:43	Informational	admin	VersionControl	CheckIn	Success	My_SG	Configuration My

Configuration Errors/Warnings/Notices

As a configuration is being modified, any configuration issues can be dynamically detected by InControl before deployment. A summary of these are displayed in a panel at the top of the configuration objects pane. An example of a single detected configuration error is shown below.



The issues that might be detected can be of three types:

- **Errors** - These are serious issues that will prevent deployment and must be fixed.
- **Warnings** - These are issues which could cause problems but will not prevent deployment.
- **Notices** - These are issues which are unlikely to cause problems.

Clicking the **Show details** link will expand the pane to explain why the issues have been flagged.

Verifying that *Ping* Works

Now verify that cOS Core 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 22, *Troubleshooting Connections* for possible reasons.

Editing an Existing Object

In most cases, once a configuration object is created, there is a choice of two ways to change it using InControl:

- Double click the object's line in the object list to open a new edit window in order to change any of the properties.
- Alternatively, directly click once on the cell of the property value to be changed in the object list. The cell will open and allow the value to be changed directly in the cell without opening an edit window. Unless the cell is for a textual value such as a name or comment, a drop-down list will appear from which a new value can be chosen.

Below, an example of the in-cell editing of an IP rule's *Action* property is shown. After the action cell is clicked once, a drop-down list of possible values is displayed. After changing the cell's value, pressing the *Return* key will close the cell and complete the edit.

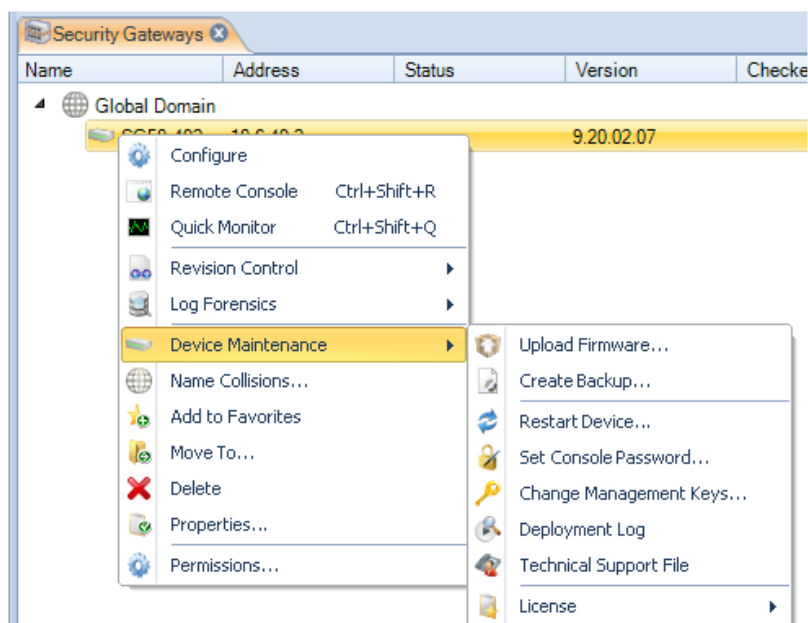
#	Name	Action	Src If
1	MgmtPing	Allow	lan

Name	Comments
Drop	Drop the packet silently
Reject	Drop the packet and respond with an ICMP error or TCP reset
Allow	Stateful connection creation
NAT	Dynamic Address Translation (hide)

The drawback to in-cell editing is that not all object properties are displayed and only the displayed ones can be changed with this method.

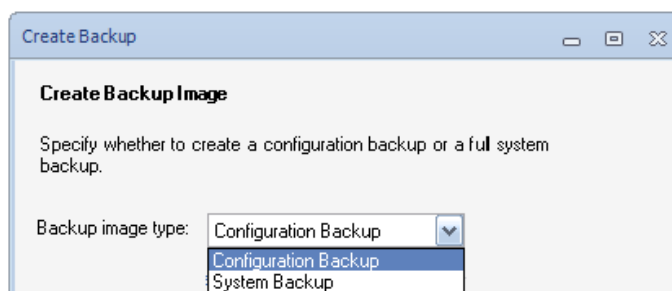
Chapter 10: Device Maintenance

This section deals with the options found in the *Device Maintenance* submenu that is accessed by right clicking a security gateway in the *Security Gateways* tab.



The *Create Backup* Option

Selecting *Create Backup* will display the following dialog.



This creates a backup of either the configuration or the entire system including the current cOS

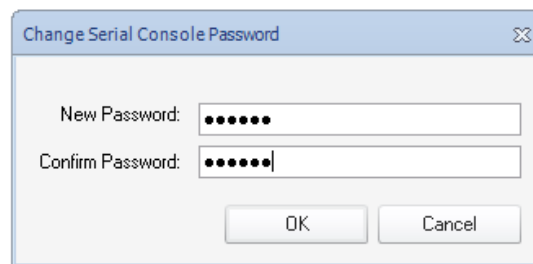
Core version plus the configuration. The backup is saved to a new, separate file on local disk.

The InControl database is not used for the creation of the backup. Instead, the backup file data comes directly from the security gateway itself. This means that the process is exactly equivalent to creating a backup through the Web Interface.

Backups of the configuration only can also be created by selecting the menu option **Revision Control > Revision History** to open the *Revision History* tab, right clicking a revision to get the context menu and then selecting the *Backup* option. In this case the configuration backup file is created from the InControl database but it can only be then restored through the Web Interface.

The Set Console Password Option

The *Set Console Password* option is used to change the password of the serial console.



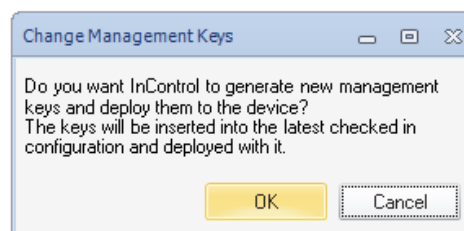
A dialog box titled "Change Serial Console Password" with a close button (X) in the top right corner. It contains two text input fields: "New Password:" and "Confirm Password:". Both fields are filled with seven dots, indicating masked text. Below the fields are two buttons: "OK" and "Cancel".

The only other way of changing the serial console password is in the *boot menu* which can be entered from the serial console during startup. The InControl option offers a way to change the password without disruption to traffic.

If the serial console password had never been set previously, this option will set it for the first time.

The Changing Management Keys Option

The *Changing Management Keys* option will automatically generate a new management key and deploy it to the security gateway while at the same time updating the InControl database.

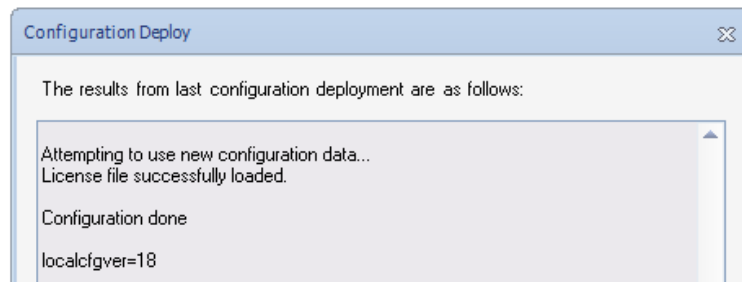


A dialog box titled "Change Management Keys" with standard window controls (minimize, maximize, close) in the top right corner. The main text area contains the following message: "Do you want InControl to generate new management keys and deploy them to the device? The keys will be inserted into the latest checked in configuration and deployed with it." At the bottom are two buttons: "OK" (highlighted in yellow) and "Cancel".

The keys are used to ensure secure communication between InControl and the security gateway. They should be changed if it is felt the existing key could have been compromised.

The Deployment Log Option

The *Deployment Log* presents a brief summary of the results for the last configuration deployment to this security gateway. This deployment might have occurred through InControl, the Web Interface or the CLI.



Depending on the hardware platform, the additional statistic *localcfgver* may be shown. This is the number of times the configuration has been changed outside of InControl.

The Technical Support Option

The *Technical Support* option is used to generate a single text file that can be used by qualified support personnel to troubleshoot system issues.

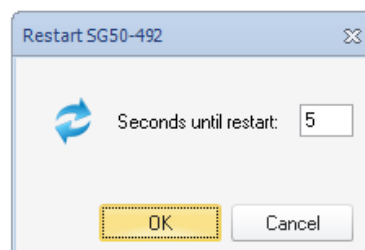
The file is created as a text file on local disk so that it can be easily mailed to support personnel. The file name has a default format, for example *techsupport-20111201.txt* and it is recommended to retain this.

Using this option is equivalent to the CLI command:

```
Device:/> techsupport
```

The Restart Device Option

The *Restart Device* will display a dialog for restarting the security gateway.



With the default value of 5 seconds, this is equivalent to the CLI command:

```
Device:/> shutdown 5
```

This executes the shutdown of cOS Core after a waiting period of 5 seconds. The shutdown will reload cOS Core and then the current configuration but not reload the firmware loader. All connections and VPN tunnels will be closed gracefully.

The License Option

The *License* option deals with the cOS Core licensing in the security gateway. This subject is covered in the following chapter in *Section 11.2, "cOS Core Licensing"*.

Chapter 11: Licensing

- InControl Licensing, page 65
- cOS Core Licensing, page 71

11.1. InControl Licensing

InControl Licensing Options

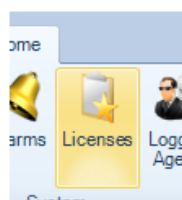
This section will discuss the licensing options for InControl itself. That is , the licensing required for InControl to be able to manage security gateways. The licensing for individual gateways is discussed later in *Section 11.2, "cOS Core Licensing"*.

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 Licenses Tab

The three options listed above are described next but first it should be noted that all licensing is managed through InControl using the *Licenses* tab which is displayed by pressing the *Licenses* button in the *Home* ribbon toolbar.



The *Licenses* tab shows details of licenses already loaded into the InControl server. An example of this tab is shown below. Here, a single license has been uploaded to the server and this is bound to a gateway called *My_GW*. The start and expiry dates for the license are listed.

Registration Key	Object Name	Status	Issue Date	Expiration Date
4196-4239-5947...	/Global Domain/My_GW	OK	2010-08-11	2013-05-09

By selecting any individual license in the *Licenses* tab, the contents of the license are displayed. The example below shows the first few lines of the details for the license selected above.

Parameter	Value
Type	FIREWALL
OEM Id	N/A
Registered To	NIHO Corporation
Registration Key	4196-4239-5947
Subscription valid until	2013-05-09
Issued Date	2010-08-11
Registration Date	2010-05-09
Last Modified	2010-08-11
MAC Address	00-90-08-07-4F

It is important to understand that the *Licenses* tab displays all licenses uploaded to the InControl server. Seeing a license in the list does not mean that the license has been deployed. However, an alarm is created by InControl if an older license has been deployed when a newer one is available on the server.

A. Management with 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 cOS Core demonstration mode. In this scenario, InControl will have full functionality for any number of Clavister Security Gateways. The purpose of this is to allow evaluation of the complete InControl product without any licensing.

It is possible to add security gateways to InControl which have a license but the license does not allow InControl management. In this case, the only management functionality possible within InControl is use of the remote console feature for direct CLI access. For more on console access, see *Chapter 16, Remote Console*.

B. Per Security Gateway Licensing

Each individual Clavister Security Gateway can have a cOS Core license that includes the ability for management by InControl and this is the usual way that InControl is licensed. In this case, no special license for the InControl server is needed and InControl can manage any correctly licensed Clavister Security Gateway.

After purchase, a cOS Core license file is downloaded from the Clavister *License Center* in the normal way and contains the license parameter *CENTRALIZED_MANAGEMENT*. The license can be purchased with or without this parameter enabled. If the license allows InControl management, 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 purchase date.

If a security gateway has a valid license but not one that allows InControl management, it can still be defined and added to InControl. However, it will not be possible to read and edit the gateway's configuration and a line in the *Alarms* tab list will indicate that the required license is missing.

Status	Date	Severity	Source	Entity	Name
●	2010-...	Warning	Managem...	My_GW	Need license to manage Security Gateway from managementserver

C. InControl Server Licensing

With larger populations of Clavister Security Gateways, administering each individual cOS Core 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 organization's specific needs so the purchase options should be discussed with your Clavister product representative.

With a server license, the cOS Core 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 cOS Core license and contains the following two key parameters:

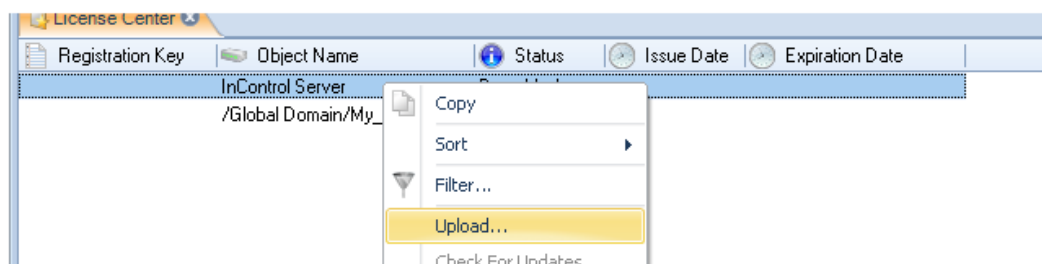
1. *PROP_CLIENTSESSIONS* - How many simultaneous InControl client sessions can be opened at any one time.
2. *PROP_DEVICES* - The maximum number of security gateways that can be managed by an InControl server (and therefore by any InControl client connected to that server).

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).

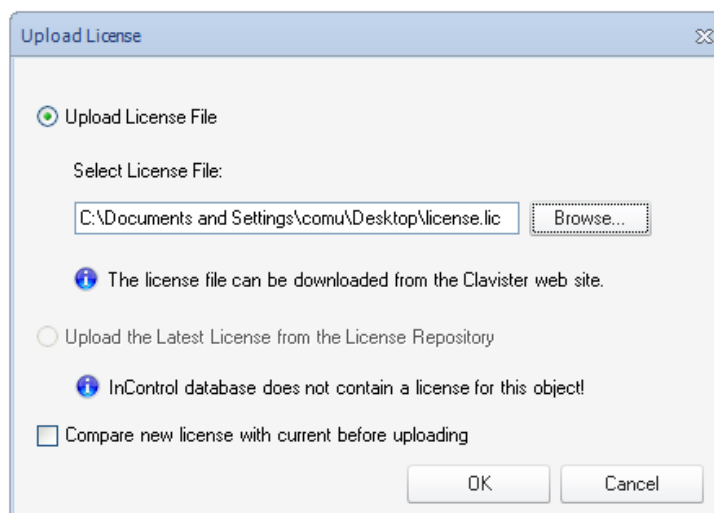
Downloading a Server License

A server license (.lic) file always has to be manually downloaded from the Clavister *License Center* to the local computer disk.

Once downloaded, it can be uploaded to the server by right clicking the license line in the *Licenses* tab list and selecting *Upload*.



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

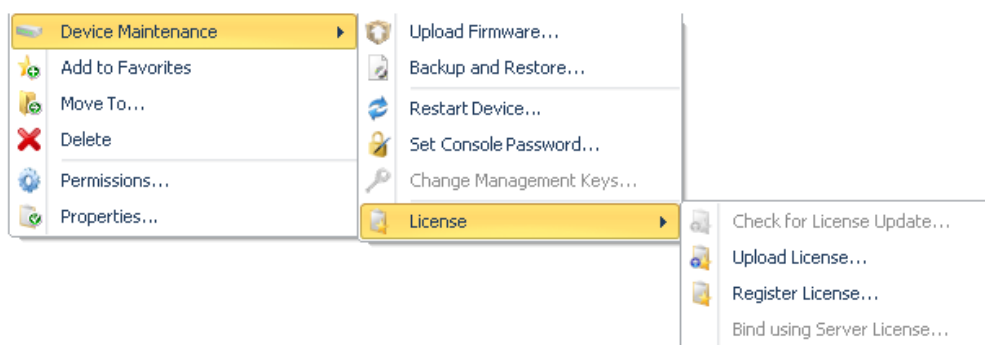


Even if automatic license updating is enabled (this is described later), server licenses will not be updated automatically. New server licenses always have to download manually as described above.

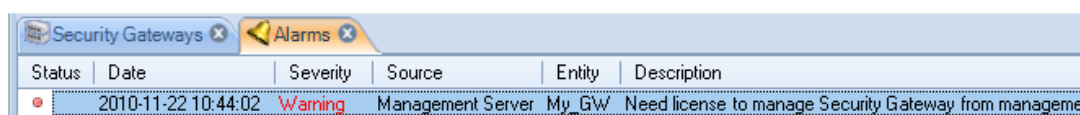
Binding Gateways to an InControl Server License

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, **the final step should be binding the gateway to the license.**

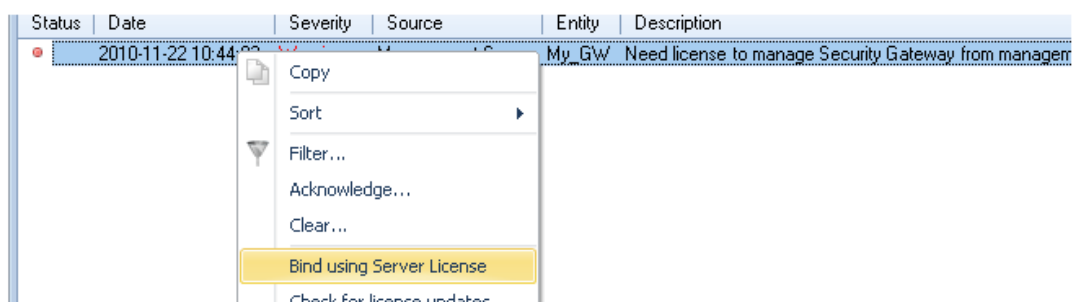
Binding is done by right clicking the gateway in the navigation tree of the *Security Gateways* tab and selecting the *Bind using Server License* option.



When a new gateway is added to InControl, an alarm appears in the *Alarms* tab list 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 using Server License* option from the displayed context menu.



Older cOS Core Licenses and InControl

Any cOS Core licenses that were purchased before the release of cOS Core version 9.10 can automatically have the *CENTRALIZED_MANAGEMENT* license parameter enabled and this is included in the cost of the original license. (This is not applicable to 9.12 telecom users.)

Obviously, the *CENTRALIZED_MANAGEMENT* parameter will not already appear in an older license file downloaded before 9.10 so the licensee should download a new, replacement license file from the Clavister *Customer Web* and upload it to the security gateway. This 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 the period.

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

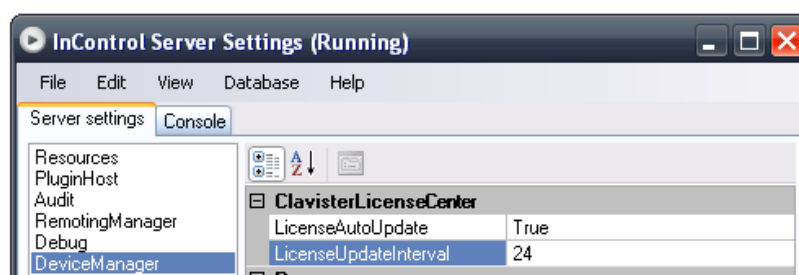
Retrieval of InControl Server Licenses

The *License Center* is a secured section of the Clavister website at:

<http://www.clavister.com>

This can be logged into directly through a normal web browser in order to perform license management manually. However, InControl can manage licenses automatically once the login credentials are specified.

The InControl server can automatically retrieve server licenses from the Clavister *License Center*. This feature is enabled through the *DeviceManager* set of options in the InControl server management interface.

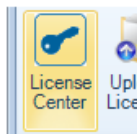


The interval between searches by the server for new updates in the license center is set to a default of 24 hours.

Enabling Automatic License Download

For InControl to be able to communicate directly with the Clavister *License Center* over the public

Internet, the administrator must first enter the relevant customer login information in InControl. This is done by pressing the *License Center* button in the toolbar of the *Licenses* tab.



InControl immediately tries to connect to the Clavister *License Center*. After successful connection, a dialog requesting login credentials is displayed. The credentials entered are the same as those used for accessing the *License Center* on the Clavister website using a web browser.

A dialog box titled 'Enter License Center credentials' with a close button in the top right corner. It contains two input fields: 'Username:' with the text 'My_Organization_Name' and 'Password:' with a masked password represented by ten dots. Below the fields is the text 'Enter the same credentials used for license center website access'. At the bottom are 'OK' and 'Cancel' buttons.

After the credentials are successfully registered, licenses can be automatically retrieved and deployed to the installed security gateway or to the InControl server.

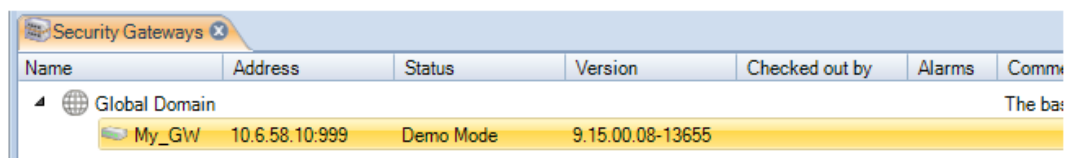
11.2. cOS Core Licensing

With or without InControl, a Clavister Security Gateway requires a *cOS Core License* in order to function correctly. The license determines the operational capabilities of the security gateway as well as protecting against the unauthorized use of Clavister products.

As explained in the previous, this license can also specify that InControl usage is allowed through the *CENTRALIZED_MANAGEMENT* parameter. If it is not, a separate InControl license must be used and associated with the InControl server.

New Gateways Without an Existing License

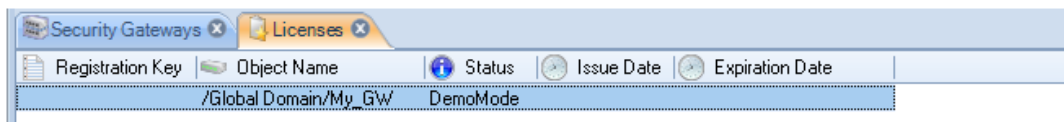
When a new security gateway is added to InControl and it does not have a valid cOS Core license associated with it, the gateway functions in *demonstration mode*. This is indicated in the *Status* column of the *Security Gateways* tab with the word *Demo Mode*.



Name	Address	Status	Version	Checked out by	Alarms	Comments
Global Domain						The base
My_GW	10.6.58.10:999	Demo Mode	9.15.00.08-13655			

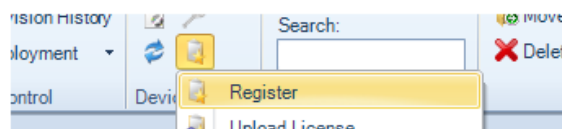
This mode means that cOS Core will cease to function after two hours of operation except for allowing management access. A restart is then required to continue running the product for another two hours. InControl always has full functionality when managing a gateway operating in demonstration mode.

In the *Licenses* tab a gateway in demo mode has an entry like the one shown below but this is not really a license and acts as a reminder that demo mode is in effect.



Registration Key	Object Name	Status	Issue Date	Expiration Date
	/Global Domain/My_GW	DemoMode		

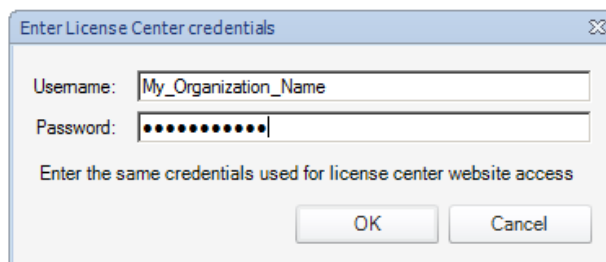
To retrieve a valid license for this gateway over the Internet from the Clavister *License Center*, press the *License* button in the *Security Gateways* tab and choose *Register* from the drop down menu.



This can also be done by right clicking the gateway and selecting *Register* from the context menu.



If this has not been done before, InControl will ask for the login credentials to the *License Center* so it can gain access to the Clavister server across the Internet.



Enter License Center credentials

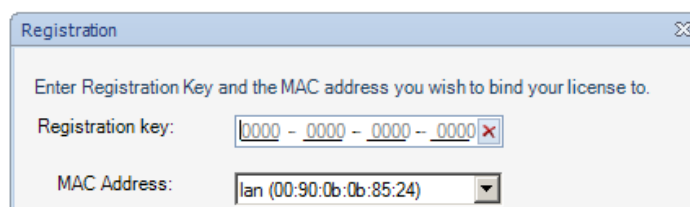
Username:

Password:

Enter the same credentials used for license center website access

OK Cancel

At this point, the *Registration Key* for the new gateway must be entered. This tells the *License Center* which gateway the license is needed for and is usually found on a label attached to Clavister hardware or has been supplied by email for other types of cOS Core installations.



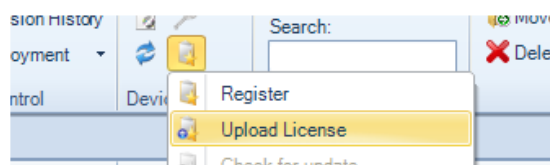
Registration

Enter Registration Key and the MAC address you wish to bind your license to.

Registration key:

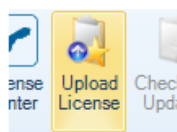
MAC Address:

InControl now downloads the relevant license to the InControl server, uploads it to the gateway and following successful installation, it is stored in the InControl *License Repository*. The repository's contents appears in the client's *Licenses* tab list. Later, the administrator can select a listed license for upload then select the *Upload License* option in order to overwrite the current license.

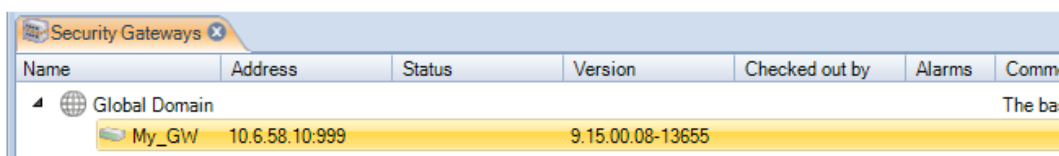


There can only be one license stored in the repository for each gateway under InControl control.

Instead of selecting the gateway first, it is also possible to open the *Licenses* tab, select a specific license to upload from the depository and then press the *Upload License* button.



When the correct license is selected, uploaded and the gateway is correctly licensed, the status becomes blank in the *Security Gateways* tab.



Name	Address	Status	Version	Checked out by	Alarms	Comments
Global Domain						The base
My_GW	10.6.58.10.999		9.15.00.08-13655			

New Gateway with an Existing License

The above steps apply to a new gateway without a license. It may be that a gateway that is

added to InControl already has a license associated with it. If this is the case, InControl automatically downloads a copy of the license from the gateway to the server's license repository and it will appear as a line in the *Licenses* tab list.

When a license update is requested, InControl will ask the Clavister *License Center* over the Internet for any new licenses for the gateway.



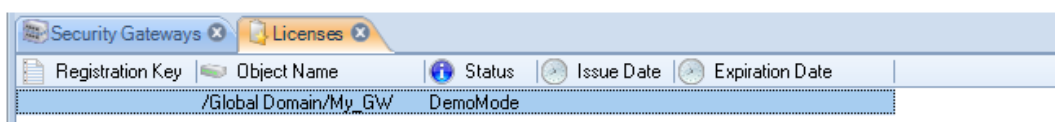
Note: License fetching requires access to the Clavister website

When the InControl server communicates with the Clavister server, it first performs a DNS lookup of **www.clavister.com** and then opens a connection to the returned IPv4 address using port **443**. Any network equipment that is located between the InControl server and the public Internet must permit this connection.

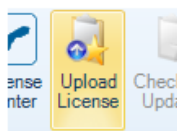
Importing a License File from Disk

License files can be downloaded to local disk from the Clavister *License Center* as a *.lic* file. It may be necessary to import these such license files into InControl and then upload them to a gateway that has no license.

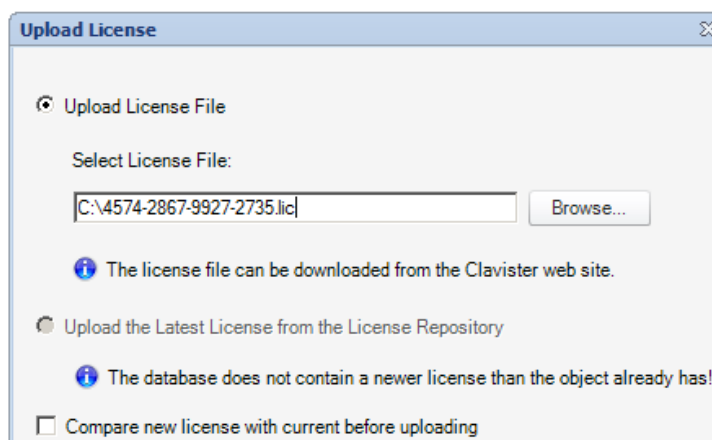
To do this, select the *Demo Mode* line in the *Licenses* tab display.



Now press the *Upload License* button.

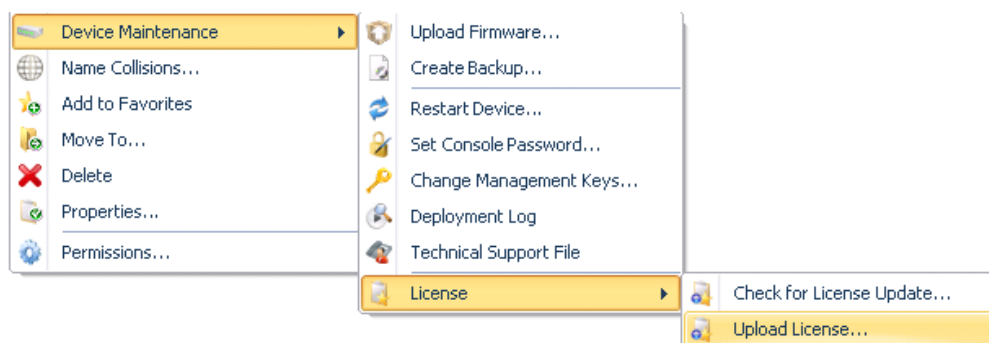


The following dialog is displayed and the license file can be selected from the local disk.



After confirming this dialog, the license is now uploaded to the gateway and then stored in the InControl server license depository.

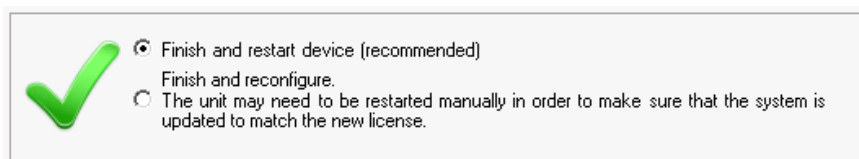
It is also possible to initiate this upload process by right-clicking the gateway and selecting the option in the context menu.



Behavior After Upload

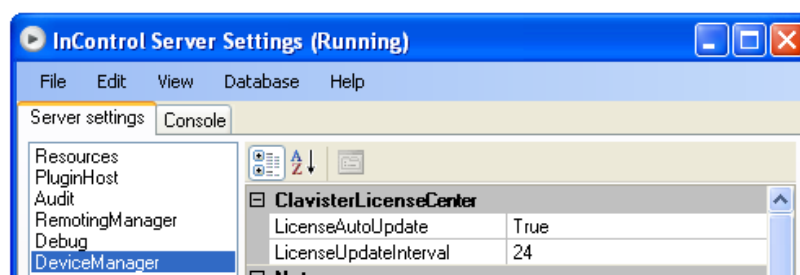
The behavior of the security gateway after license upload depends on the cOS Core version. For versions prior to 10.11, there is an automatic reboot. A reboot will cause all existing connections to be lost. This is because the new license may require a different allocation of memory. For example if the parameter specifying the maximum number of VPN tunnels changes.

For 10.11 and later versions, the InControl client presents the administrator with the following dialog in order to select the action to be taken following license upload.



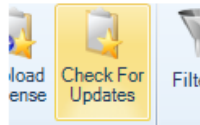
Updating Licenses

By default, an automatic check of the remote Clavister *License Center* server is regularly made by InControl and this is configured through the InControl server interface.

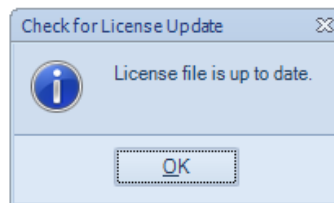


Using these settings the server automatically downloads any new licenses for any added gateways to the license depository, overwriting any existing license for that gateway in the depository. Alarms are created for these downloads so that the administrator is made aware of newer licenses and can upload them when convenient to the relevant gateways.

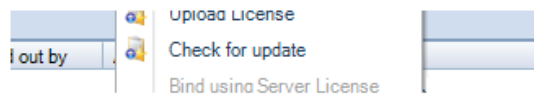
It is possible to force a license update at any time by pressing the *Check for Updates* button in the *Licenses* tab. This checks for updates only for the currently selected license.



If there are no updates to be downloaded for the license, the client will display the following message.



Similarly, it is possible to check for updates for a particular gateway in the *Security Gateways* tab.



Chapter 12: 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.

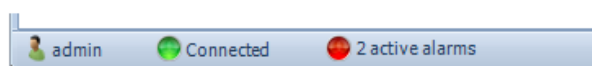
An override feature for the user to clear the alarm manually is provided but this should not normally be needed.

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:

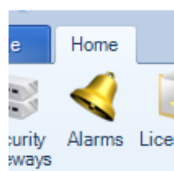


In this example, the display indicates there are two active alarms for this InControl client.

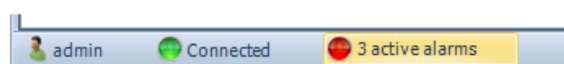
The Alarms Tab

The *Alarms* tab in the InControl client interface displays information about all alarms, including alarms that have been triggered but not yet cleared. The tab can be opened in two ways:

- By pressing the *Alarms* button:



- By pressing the alarms icon itself which acts as a button.



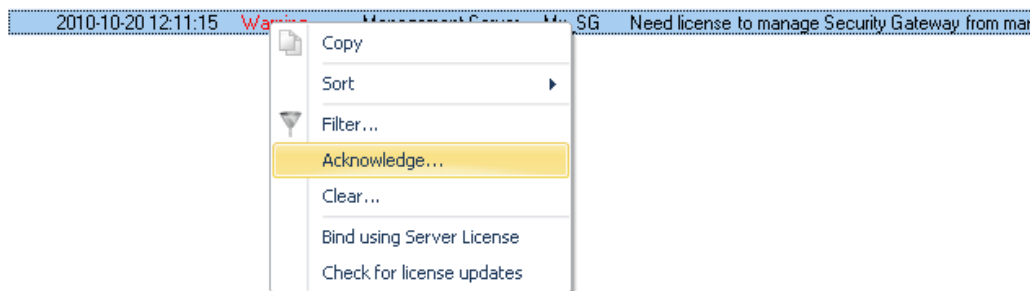
InControl will now display a summary of alarms for this client:

Status	Date	Severity	Source	Entity	Description
•	2010-10-20 14:08:41	Informational	Management Server	My_SG	Object checked out for editing.
•	2010-10-20 14:15:26	Warning	Management Server	My_SG	It was not possible to connect to the security gateway.
•	2010-10-20 12:11:15	Warning	Management Server	My_SG	Need license to manage Security Gateway from man

Further detail for each alarm is provided by selecting a particular alarm. The details displayed for the final alarm above is shown below.

Details	
Parameter	Value
Name	Security Gateway Unreachable
Alarm Type ID	1
Severity	Warning
Status	Not acknowledged
Source	Management Server
Entity	My_SG
Details	Security Gateway My_SG (10.6.58.10) is unreachable.
Description	It was not possible to connect to the security gateway.
First triggered	2010-10-20 14:15:26
Last triggered	2010-10-20 15:40:35

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

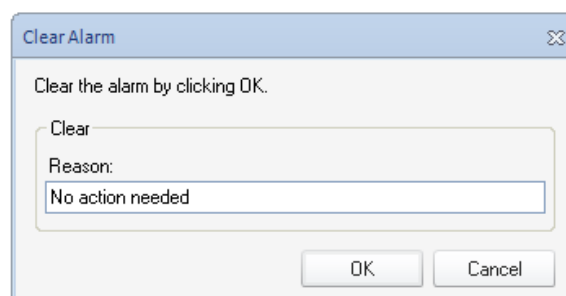


Clearing Alarms

If the *Clear* option is chosen, the meaning is to indicate that the issue that generated the alert has been dealt with.

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 instead of being cleared, then the administrator is stating that the issue generating the alarm has been noted but it has not been dealt with yet. Like the option to clear an alarm, a dialog is displayed 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 *Alarms* tab 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 alarms list.

The Alarm History

cOS Core 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 based on the search criteria listed below:

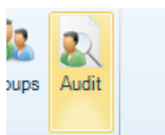
- Time when first triggered.
- Time when first triggered.
- Time when last triggered.
- The source.
- The entity that the alarm refers to. For example, a security gateway.

- 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 13: 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* which consists of a database of *Audit Log Messages*.

The current audit trail is displayed by pressing the *Audit* button.



This opens the *Audit Trail* tab which displays a list of the current trail. An example list is shown below.

A screenshot of a window titled 'Audit Trail'. It contains a table with columns: Time, Severity, User, Category, Action, State, Entity, and Comment. The table lists several log entries, with the second entry highlighted in blue.

Time	Severity	User	Category	Action	State	Entity	Comment
2010-11-15 10:55:31	Informational	NT AUTHORITY\SY...	Database	Write	Success		A relation betw
2010-11-15 10:55:31	Informational	NT AUTHORITY\SY...	Database	Write	Success		User 2 was ac
2010-11-15 10:55:31	Informational	NT AUTHORITY\SY...	Database	Write	Success		Permission ad
2010-11-15 10:59:19	Informational	admin	Authentication	Login	Success		Access grante
2010-11-15 10:55:34	Informational	NT AUTHORITY\SY...	System	None	Success		Management !
2010-11-15 10:55:33	Informational	NT AUTHORITY\SY...	System	None	Success		Database atta
2010-11-15 10:55:31	Informational	NT AUTHORITY\SY...	Database	Write	Success		A relation betw
2010-11-15 10:55:31	Informational	NT AUTHORITY\SY...	Database	Write	Success	root	Added configu

Each entry in the trail shows what action was performed by who, on what and if it succeeded. By default, the audit log shows only the entries for the last hour of client usage. This can be changed by using the filters in the toolbar.

Displaying Audit Details

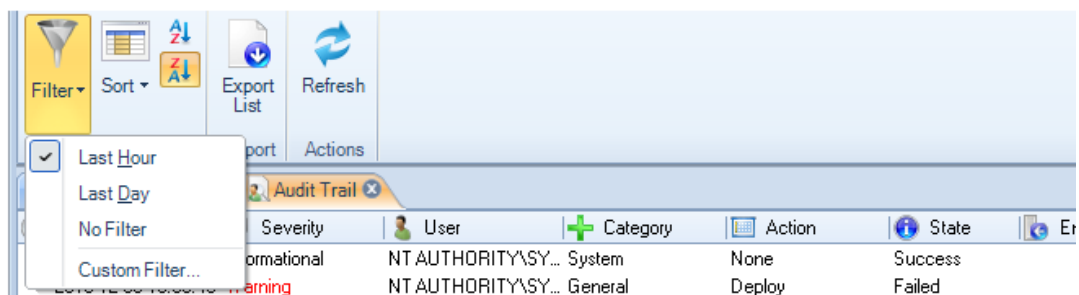
By selecting any single line in the audit trail display, the details of that event are shown in a separate panel underneath. Below is an example of the detail for the entry which indicates that a new user with the name *admin2* was added to the user database.

Details	
Parameter	Value
Entity_Id	N/A
Written	2010-11-15 10:55:31
User	NT AUTHORITY\SYSTEM
Thread_Id	5
Category	Database
Username	auditor
Machine	COMP
Entity_Name	N/A
Severity	Informational
Action_State	Success
User_Id	2
Table	UserTable
Comment	User 2 was added to the database.
Action	Write
Timestamp	2010-11-15T09:55:31.7644275Z

Filtering Audit Log Messages

The audit trail always displays audit log messages for all users connected to the same InControl server.

The filtering features of the *Audit* toolbar allow the display selection to be customized.



By default, the last hour of all audit logs are displayed. As shown above, different time intervals or a custom filter can be created.

A custom filter can involve choosing values for several parameters. A typical filter is shown below.

Audit Trail Filter

Perform custom alarm filtering based on several criteria.

Interval:

Last Hours

Value: 1

Criteria:

Severity: Alert Category: System

User: admin Action: Add

Entity: My_GW State: Success

Chapter 14: Domains

Domains Allow Configuration Object Sharing

The *Global Domain* always exists in a cOS Core configuration by default and this is used to share cOS Core configuration objects amongst all security gateways. It is often the case that a set of configurations objects need to be shared amongst a limited subset of the security gateways defined to InControl. In this situation, a new *Domain* can be defined.



Important: Try to keep the Global Domain small

Although it may seem convenient to keep as much as possible in the global domain, this is not recommended since InControl operations such as opening configurations and deployment can become much slower.

The recommended approach is to only place objects in the Global Domain or sub-domains when they absolutely have to be there. If an object is only needed in one security gateway then keep it as a locally defined object unique to that gateway's configuration.

Domains are Specific to 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 switch to managing configurations using those other interfaces even though they were originally configured using domains.

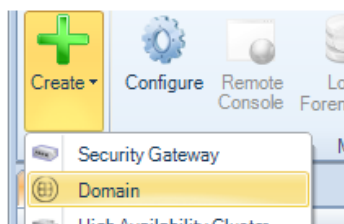
Domains are Initially Empty

Both the *Global Domain* and any new, created domains have the same, default object structure. However, this structure is initially empty and must be filled with any objects that are to be shared.

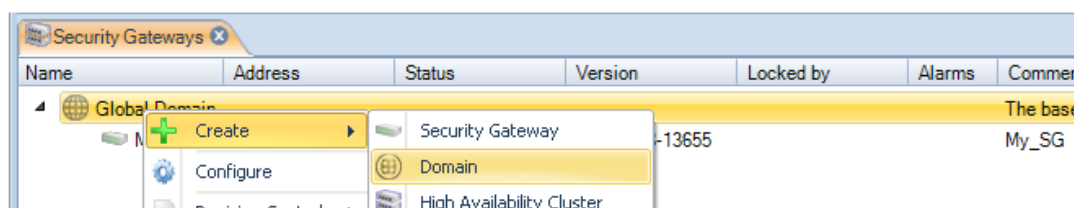
Adding Domains

Adding a domain can be done in one of two ways:

1. Press the *Create* button in the *Security Gateways* tab and choose *Domain*.



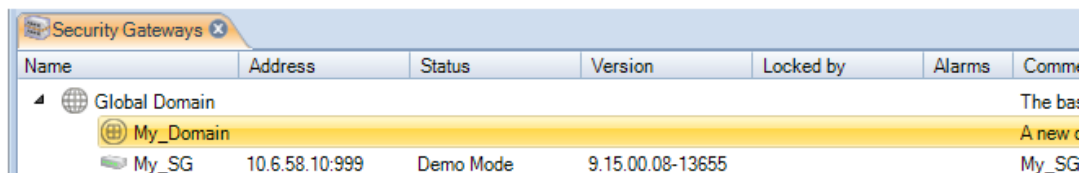
1. Alternatively, right click the global domain in the *Security Gateways* tab navigation tree and choose *Create > Domain*.



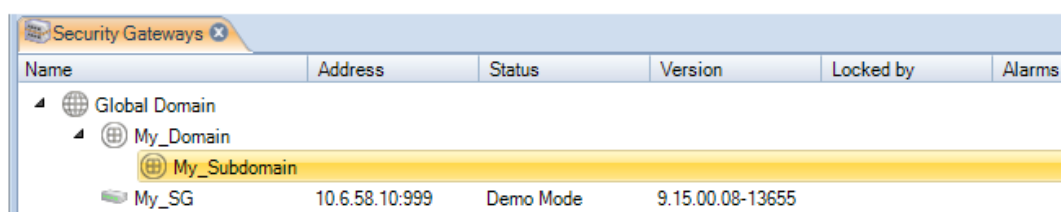
This results in a dialog being displayed so that the name of the new domain can be entered and the parent of the domain selected.



The default parent for a new domain is the *Global Domain* as shown below.

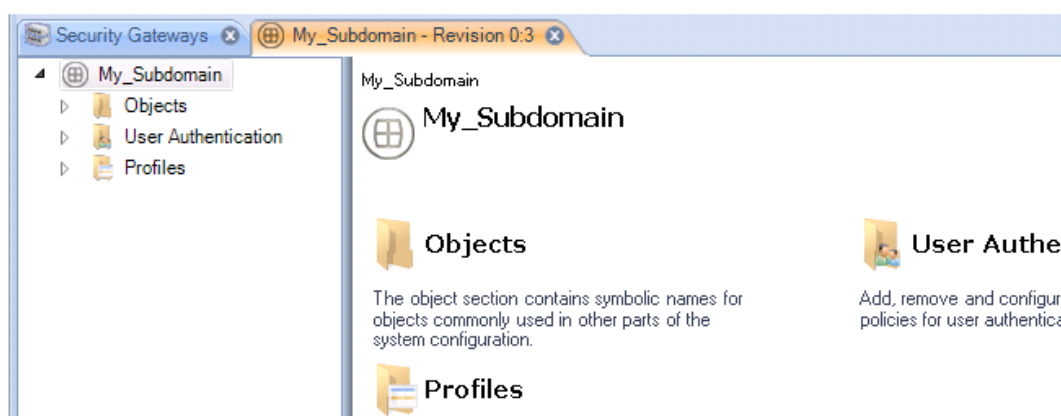


However, it is then possible to create further sub-domain levels. The screenshot below shows a domain called *My_Subdomain* defined under *My_Domain* which is itself defined under the global domain.



Name	Address	Status	Version	Locked by	Alarms
Global Domain					
My_Domain					
My_Subdomain					
My_SG	10.6.58.10:999	Demo Mode	9.15.00.08-13655		

Once defined, any new domain has a set of objects which are similar to the set found in the global domain. This object set then applies only to the security gateways defined within that domain and takes precedence over the same objects found at higher levels. Below is the object navigation tab for *My_Subdomain*.



Tip: Configuration revision numbers

The revision number for the above tab is **0:1**. This means that these configuration objects have been edited once by InControl (the initial creation) and zero times by the Web Interface or by the CLI via SSH.

The domain arrangement means that:

- 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

cOS Core does not allow the same object name to be used twice in a hierarchy of domains and is flagged as an error in InControl.

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 any domain and apply version control to its contents.

When a domain is checked out, only the domain itself is checked out. Any subdomains or

gateways within that domain are not also automatically checked out.

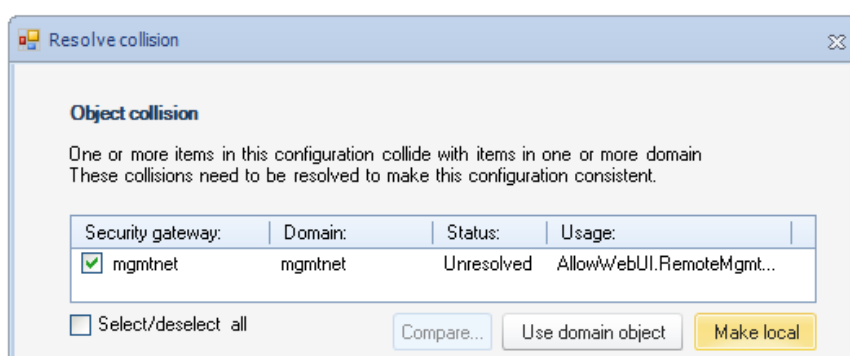
When the domain is checked in, any changes made to objects in the domain that are used by security gateways under the domain are deployed by the InControl server. In other words, the configurations of security gateways affected by changes in their parent domains are automatically updated.

Applying Domain Changes to Checked Out Gateways

Like security 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.

Resolving Object Collisions

If the name of an object in the domain is the same as an object in one of the domain's child security gateways, it will not be possible to check in and deploy the gateway until this duplication is resolved. This is done with the *Resolve Collision* dialog which forces a choice of which duplicate to keep. The example below shows the dialog listing one collision where the object name *mgmtnet* is duplicated.



Such collisions could occur because of a name change or new object creation in a gateway or a domain.



Note: Some upgrades require extra measures for collisions

In some cases of upgrading InControl, the object collision resolution mechanism described above will be unable to deal with certain collision problems where a domain object name is the same as the name on a gateway. This can occur specifically when the two colliding objects are at different hierarchy levels in the domain and gateway. For example, one object is in an address book folder in the domain but is at the top level of the address book on the security gateway. A symptom of this is alert messages continue to appear, one alert for the collision in the domain and a separate alert for the collision in the security gateway.

In this case, the actions to take are as follows:

- *Change the object name manually on the security gateway. This will remove the collision alert for the gateway but not the alert for the domain.*
- *Edit the colliding domain object name but do not change it or enter **OK**. Instead, press the **Cancel** button to leave editing. This will remove the remaining alert for the domain.*

Unlike gateways, imported domains do not also require a cOS Core upgrade procedure to be applied as the second step. Domain objects can therefore be accessed and edited directly after the import. However, any objects from the domain that are used in an imported gateway get automatically duplicated in the child gateway configuration. After the gateway cOS Core version is upgraded but before it can be deployed, the *Resolve Collision* dialog described above will appear in order to choose which duplicate to keep.

Flagging Unused Domain Objects

By default, if a domain object is edited and it is not used in any security gateway configurations, a warning message is displayed.



One reason for this warning is the 8.nn import procedure mentioned above. After an 8.nn datasource is imported but before any security gateways in the datasource are upgraded, imported domain objects can be edited but they will not appear to be used yet in the child gateways. The warning is a reminder of this.

This warning message can be disabled by clicking the checkbox in the message or clicking a checkbox in the *Client Settings* dialog (see *Chapter 5, The Client Interface*).

Domains and the CLI

It is important to understand that domains are logical constructs that only exist within InControl and their purpose is to manage objects common to more than one configuration. However, at the local gateway level, individual configurations themselves are not aware that a configuration object may be in a domain.

The CLI is only used to directly manipulate objects in a single configuration on a single security gateway and therefore cannot be used to manipulate domains. In addition, if a domain object is not used by a particular security gateway within that domain, then the object will not exist in the gateway's configuration and cannot be manipulated using the CLI.

Chapter 15: User Accounts and Groups

The cOS Core User Database

Each Clavister Security Gateway maintains its own user database. The users defined in these databases determine the usernames, passwords and permissions for access using the cOS Core Web Interface or using the CLI via direct SSH access.

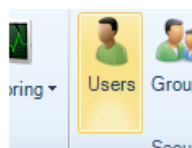
The InControl User Database

The InControl server maintains a single, central database of users which is completely separate from the cOS Core user databases described above. The InControl database is set up independently of the connected security gateways and provides a way of determining which InControl client users have which administrative permissions.

Even when opening a CLI console in the InControl client, access is controlled by this central database.

Listing Users

To open the *Users* tab and list the current users, press the *Users* button in the *Home* toolbar.



The *Users* tab will open to display a current user list.

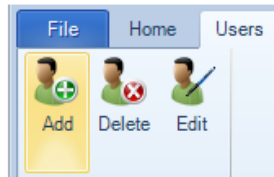
A screenshot of a web application window titled 'Users'. It displays a table with three columns: 'Name', 'Password', and 'Groups'. There are two rows of data. The first row shows 'admin' as the name, a masked password, and 'Administrator' as the group. The second row shows 'auditor' as the name, a masked password, and 'Auditor' as the group. The table has a light blue header and thin borders.

Name	Password	Groups
admin	XXXXXXXXXX	Administrator
auditor	XXXXXXXXXX	Auditor

Two users with the names *admin* (password *admin*) and *auditor* (password *auditor*) are defined by default. They belong to two predefined *User Groups* called respectively *Administrator* and *Auditor*. It is the group which defines the permissions that its members have.

Creating New Users

A new user can be created by pressing the **Add** button in the *Users* tab.



This starts the *New User* wizard which begins by asking for a unique name, for example *admin2*, along with a password.

 A screenshot of the 'New User' wizard window. It contains three input fields: 'Name' with the text 'admin2', 'Password' with six dots, and 'Retype Password' with six dots. The window has a title bar with 'New User' and a close button.

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.

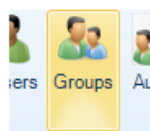
 A screenshot of the 'New User' wizard window showing the group selection step. It features a table with two columns: 'Group' and 'System Permissions'. The 'Administrator' group is selected with a checkmark and has 'All' permissions. The 'Auditor' group is unselected and has 'None' permissions.

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.

Listing Current Groups

To open the *Groups* tab and list the current groups, press the **Groups** button in the *Home* toolbar.



The *Groups* tab will open to display a current group list.

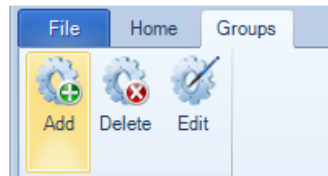
 A screenshot of the 'Groups' tab in a software interface. It displays a table with four columns: 'Name', 'System Permissions', 'R/W Permissions', and 'Local Users'. The table lists two groups: 'Administrator' and 'Auditor'.

Name	System Permissions	R/W Permissions	Local Users
Administrator	All	[Global Domain recursive All]	admin, admin2
Auditor	None	[Global Domain recursive Read]	auditor

Against each group entry is shown a summary of permissions along with member users. The user *admin2* that was added earlier is shown in the above example.

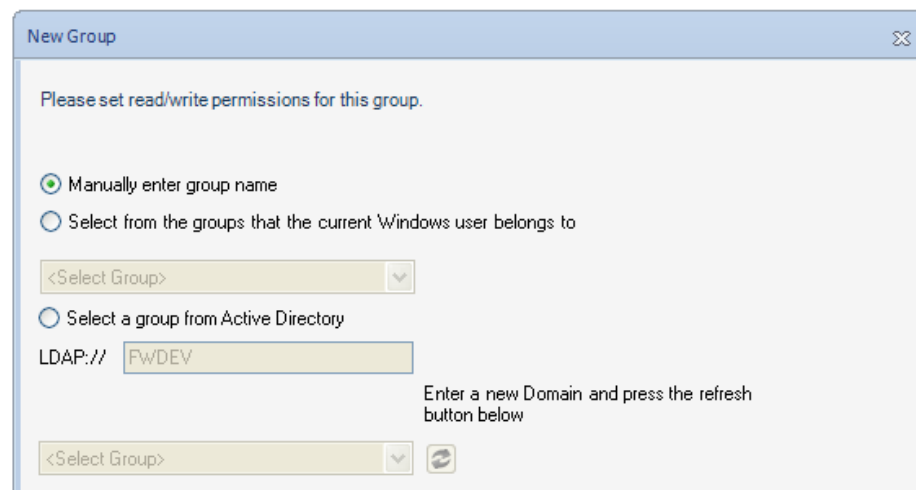
Creating Groups

A new group can be created by pressing the **Add** button in the *Groups* tab.



This starts the *New Group* wizard which begins by asking for a unique name, for example *admin2*, along with a password.

If InControl client login authentication is to be performed using a Windows *Active Directory* server (the *MSDomain* option) then a new group must be created which associates the group name on the active directory server with the required privileges.



The following options are presented for specifying the group name:

- **Manually enter group name**

The administrator can enter the name of the group the user belongs to. This option is for *internal* authentication only.

- **Select from the groups that the current Windows user belongs to**

Specify a Windows domain from the list given. This means that a user who starts the InControl client will automatically be authenticated against a Windows *Active Directory* server and will not need to enter their credentials in the login dialog. The user automatically becomes associated with this group and its permissions.

Selecting this option means that the later wizard step of defining the individual users belonging to the group can be skipped.

Some further steps are required if this option is selected and they are described below, after the description of the wizard.

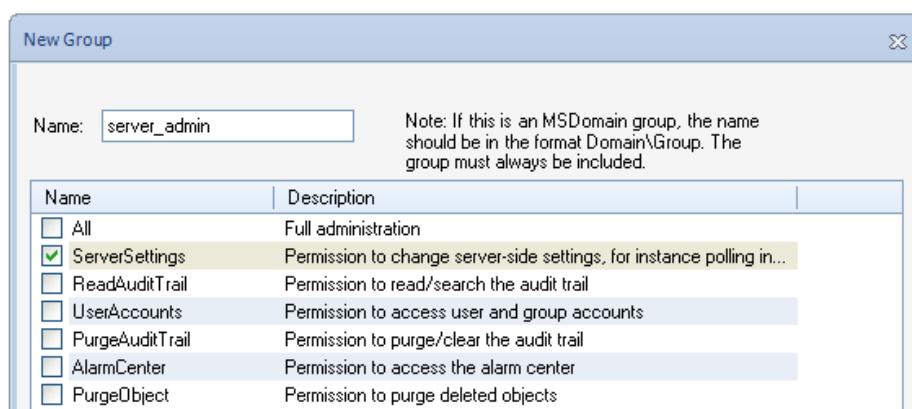
- **Select a group from Active Directory**

This option allows the same type of login as the previous option but the active directory server and associated group can be manually specified. The wizard will automatically select the domain the user is currently logged in with for this option and the administrator can leave this as is or change it.

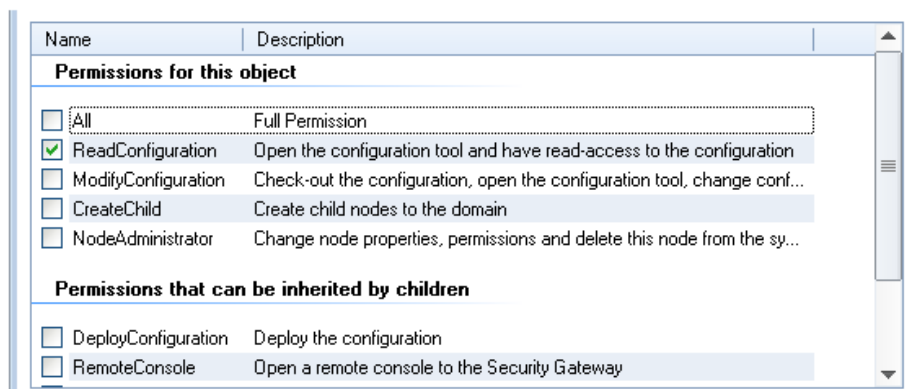
Selecting this option means that the later wizard step of defining the individual users belonging to the group can be skipped.

Some further steps are required if this option is selected and they are described below, after the description of the wizard.

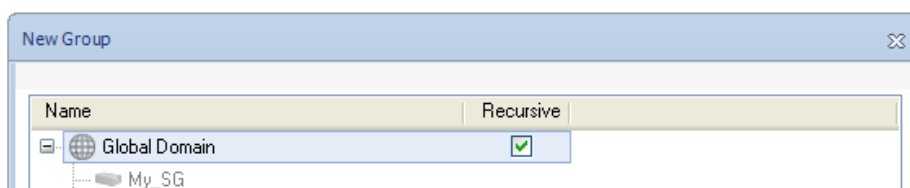
Next we specify a name, in this example *server_admin*, along with what *InControl Server Permissions* the group will have. Here, we select the privilege to change server settings.



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).



The top panel in this wizard step is used to specify to what security gateways or domains the permissions will apply.

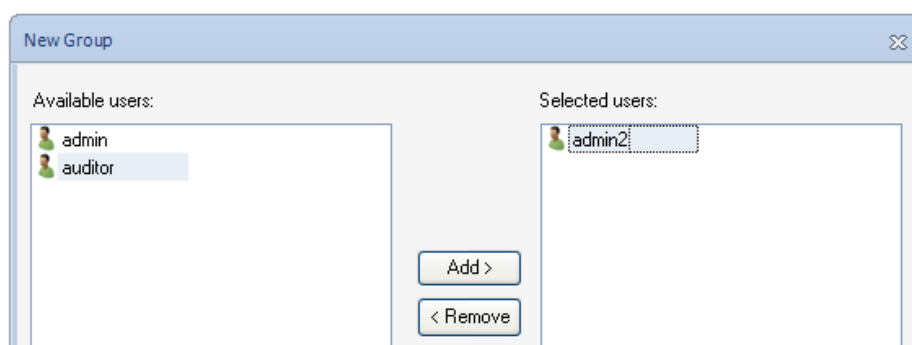


By default, the permissions are specified for the *Global Domain* and is specified as *Recursive*

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. This step should be skipped if this group is only for Active Directory authentication. In this example, the user *admin2* is added into the new group.



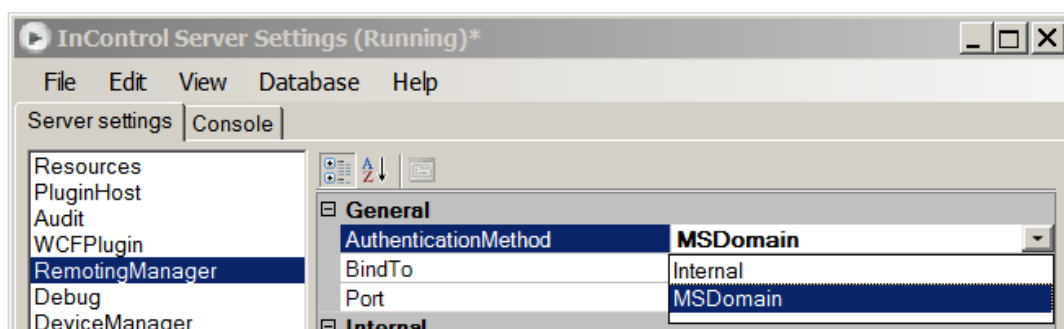
The user *admin2* now belongs to two groups. When this happens, the permissions of all the groups a user belongs to are combined to determine what the user can do. In this case, *admin2* is already a member of the *administrator* group so it is probably better to remove them from that group so they have the limited privileges of the *server_admin* group.

This example also illustrates how group membership can be determined when a user is defined or when a group is defined.

Additional Steps for Active Directory Authentication

If the *Active Directory* option (MSDomain) was selected in the new group wizard, additional steps are required before this type of authentication can function:

1. Close the InControl client and open the InControl server management interface.
2. Under *RemoteManager*, change the *AuthenticationMethod* setting to be *MSDomain*.



3. Select **File > Save** followed by **File > Service > Restart**.
4. Verify that this is working by starting the InControl client. The normal login screen will be presented and the Windows domain user account will be displayed in the bottom-left corner of the client window after logging on.

5. The need to log on is now removed by modifying the command that starts the InControl client. This is done by right-clicking the client shortcut and selecting *Properties*. The *-AuthenticationMethod* and *-Host* options need to be appended to the command line so it appears like the following:

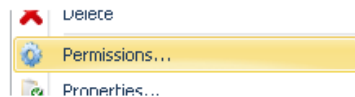
```
ICC.exe -AuthenticationMethod MSDomain -Host <server-ip>
```

Where *<server-ip>* is the IPv4 address of the active directory server that will authenticate the user. This is needed as there may be more than one server available.

6. Now, restart the InControl client. This time the login dialog will not display and the InControl client will be logged automatically by referencing the active directory server. The domain user account will be displayed in the bottom left-hand corner of the client interface.

Setting Permissions on Gateways and Domains

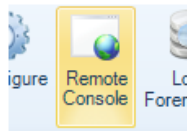
By right clicking a security gateway or domain in the InControl navigation tree, the *Permissions* option can be chosen from the context menu.



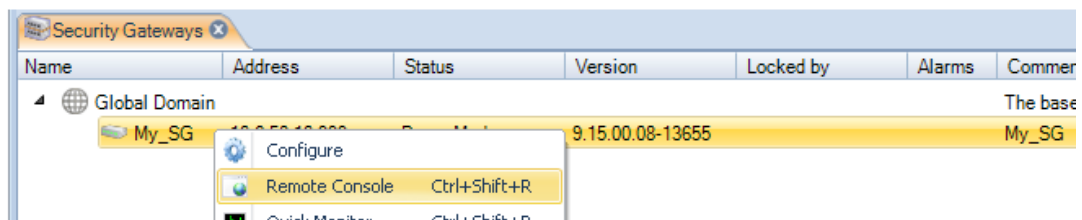
Chapter 16: Remote Console

This chapter describes the *Remote Console* feature of InControl. The console is used to provide CLI access to cOS Core from within the InControl environment.

To open a console, select the target gateway in the *Security Gateways* tab and press the *Remote Console* button in the toolbar.



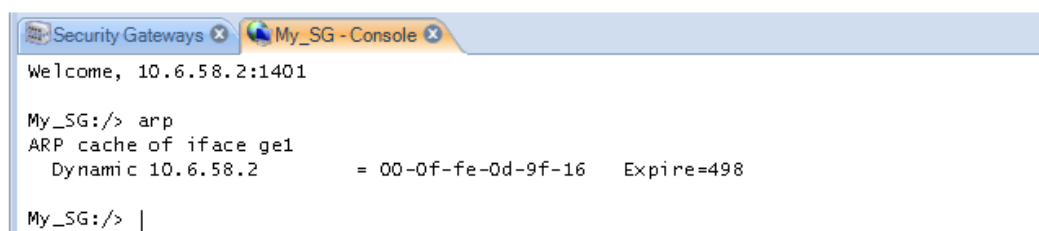
Alternatively, right-click the gateway and select the console option from the context menu.



A new tab then opens that contains the console session. Below, the security gateway *My_GW* has a console tab opened.



This console can now 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. For example, here is the output from an *ifstat* command to list the interfaces.



```

Security Gateways x My_SG - Console x
Welcome, 10.6.58.2:1401

My_SG:/> arp
ARP cache of iface ge1
  Dynamic 10.6.58.2      = 00-0f-fe-0d-9f-16  Expire=498

My_SG:/> |

```

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

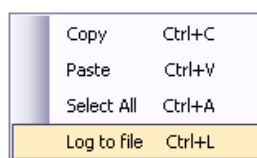
Multiple Console Sessions

It is possible that multiple InControl clients as well as multiple SSH clients could be changing a single cOS Core configuration at the same time using the CLI.

This is allowed by cOS Core but should be avoided. When each CLI console session saves and activates its changes then those changes are immediately applied to the current configuration.

Console Logging

The entire text of console interactions can be logged to a text file. This is done by right clicking the console window and choosing the *Log to file* option from the context menu.

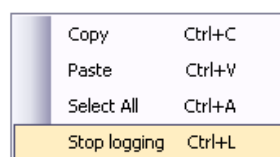


Once enabled, a file is created of the form:

```
<gateway-name>_log.txt
```

And this is saved in the path specified by an option *Client Settings* (see *Chapter 5, The Client Interface*). By default, the path is *Clavister\InControl\Client* in the InControl installation folder.

To stop logging, right click again and select the *Stop logging* option.



An option in *Client Settings* also determines if enabling logging overwrites an existing log file or appends to it. By default, a timestamp is added to the beginning of each line in the log file.

Console Time-out

A console session is subject to the existing cOS Core console timeout restriction. By default, after 1800 seconds (30 minutes) of console inactivity, the session will be closed by cOS Core.

This time-out value can be changed, for example to 3600 seconds (one hour), with the CLI command:

```
Device:/> set RemoteManagement RemoteMgmtSSH AllowSSH SessionIdleTime=3600
```


Alternatively, the time-out can be disabled for all InControl console sessions using an option in *Client Settings* (see *Chapter 5, The Client Interface*).

Chapter 17: Real-time Monitoring

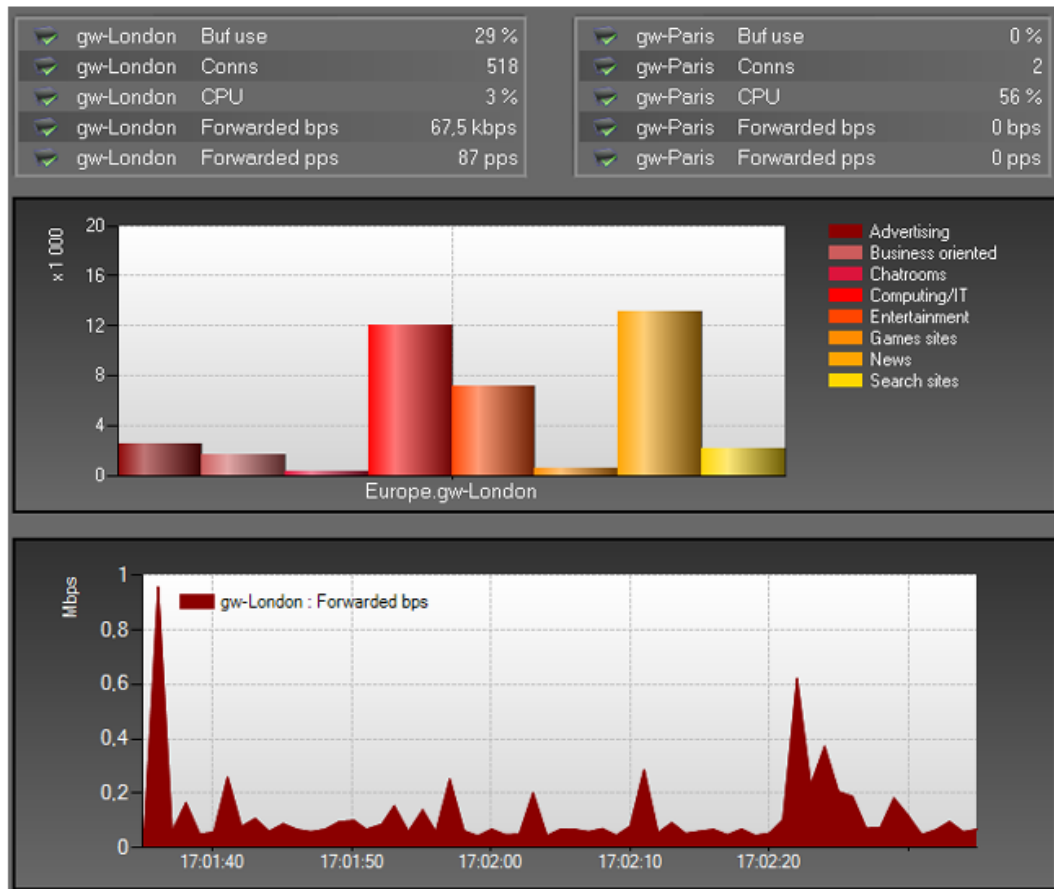
Monitoring Overview

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 cOS Core 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 cOS Core 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 cOS Core 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 cOS Core parameter.

- **Dashboards**

A *Dashboard* is a set of one or more controls that are displayed together for monitoring a group of cOS Core 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.

Monitoring Control Types

The following types of monitoring controls are available:

Generic Monitoring Controls

These fall into two categories:

Gauges

A *Gauge* is a graphical display which can show the current value of a single cOS Core operating parameter on a single Clavister Security Gateway. A range of Gauge styles are available and any style can be associated with any cOS Core parameter.

Chart and List

As an extension of a Gauge, the *Chart* and *List* 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 *Bar Chart* and a *Line Chart*.

Pre-defined Controls

InControl includes special controls that have been created to monitor specific cOS Core parameters. The *Web Content Filtering* control is an example of this.

Layout Controls

These consist of the *Label* control for adding text and/or images to a dashboard, and the *Group* 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.

**Tip**

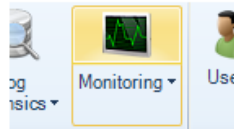
*Toggling between the design and monitor modes can be done with the **F5** function key.*

Designing Dashboards

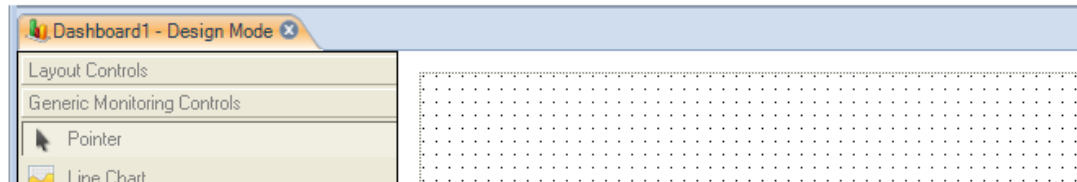
By using the *Design Mode* editor, custom dashboards can be created which contain the monitoring controls that are desired for monitoring particular cOS Core installations.

Starting a New Dashboard

To begin a new dashboard, press the upper part of the *Monitoring* button in the *Home* tab.

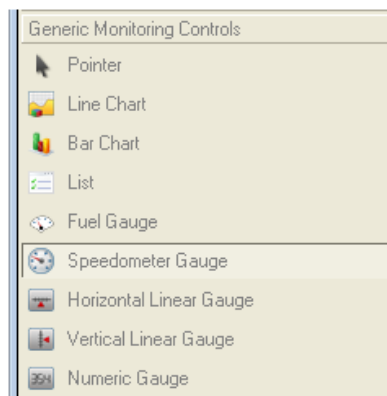


This opens a new *Design Mode* tab with the default name *Dashboard1* and a blank dashboard.



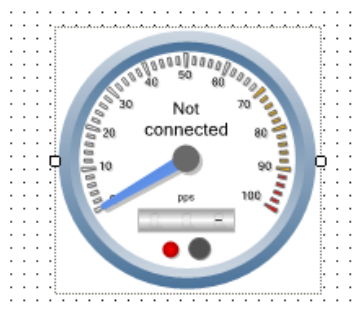
Monitoring Controls

InControl provides a range of *Monitoring Controls* in different styles which are listed in a menu on the left of the design tab.



It is up to the administrator to decide the style that best suits the presentation needs for the value to be monitored. If it is preferable to have a single control monitor more than one parameter, a Bar Chart, Line Chart or List control could be used.

The *Speedometer Gauge* has been selected above. That control will now appear in an area dragged out with the mouse in the cross-hatched design space. Alternatively, it is possible to drag the control from the control menu directly into the design space, in which case a default size is used.



All monitoring control styles can be scaled further, smaller or larger, by dragging their edges at the marked points while their positions can be changed by dragging their borders.

New Controls are Not Connected

The text "**Not Connected**" appears in a new control to indicate that a security gateway and the cOS Core parameter it will monitor on that gateway have not yet been selected for the control.

Monitoring Control Properties

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

Appearance	
CustomTitle	
ShowDeviceName	True
Behaviour	
DynamicMaxValue	True
MaxValue	100
MinValue	0
Data Binding	
MonitoredData	
Design	
(Name)	Speedometer1
Locked	False
Layout	
Location	84; 110
Size	160; 160

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.

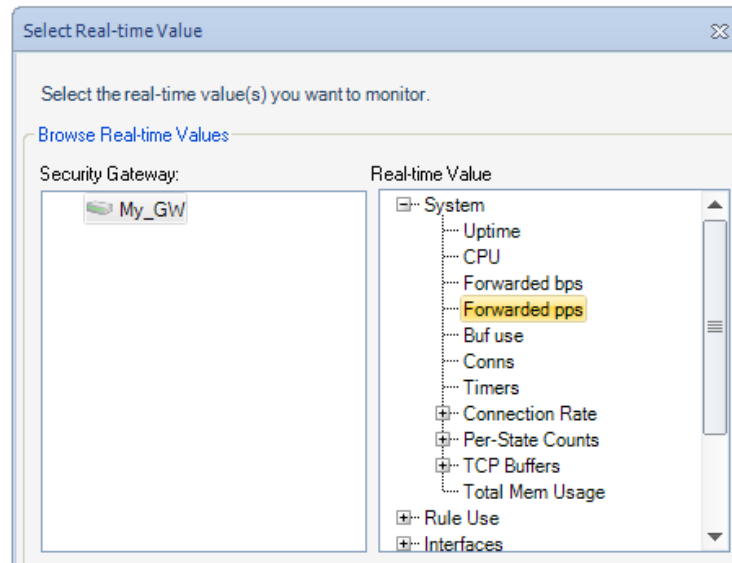
Dynamic Maximums

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 Property

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 cOS Core 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 cOS Core 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: Controls without a binding do nothing

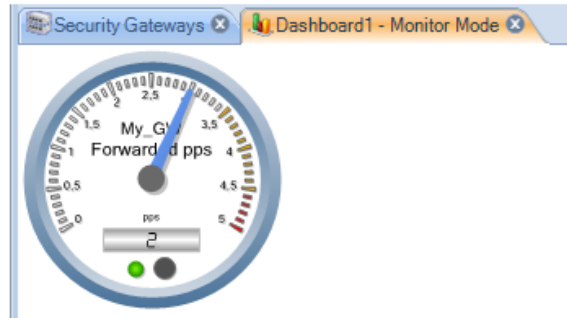
If a control is not associated with one any cOS Core parameter, it will appear in a dashboard but will not do anything in monitor mode.

Changing Design Mode to Monitor Mode

In order to have the new dashboard become "live" and start monitoring a gateway, it is necessary to switch from *Design Mode* to *Monitor Mode*. This is done by pressing the *Run* button.



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



When the *Stop* button is pushed, the dashboard returns to design mode.



Tip

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

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

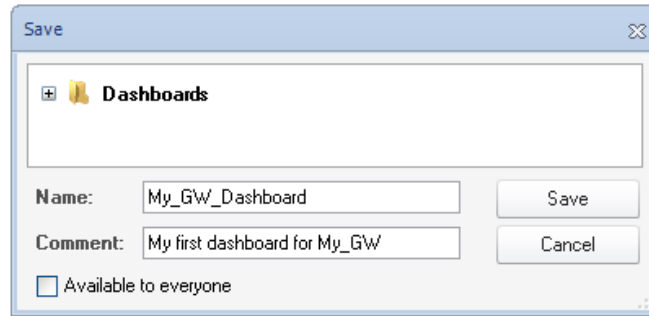
The look and feel of a dashboard or the individual components can often be set by selecting a *Theme*. Themes are purely cosmetic and provide a way to get a color scheme that suits the user.

Saving a Dashboard

Once a dashboard has been created, it can be saved by pressing the *Save* button in the tab's toolbar.

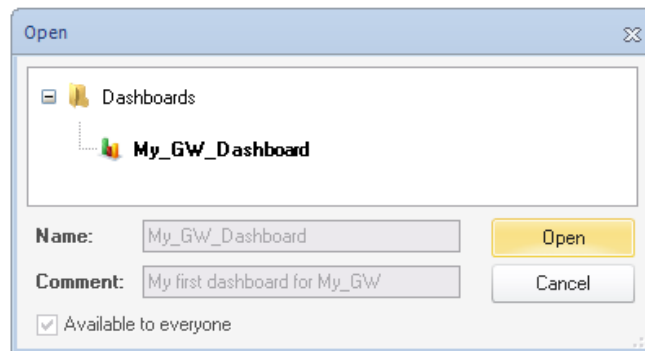


The dashboard is given a user defined name and saved. Dashboards are not saved as normal files in the local file system. Instead, they are saved as an entry in the main InControl server database.



A checkbox at the bottom of the save dialog determines if the dashboard is available to all clients.

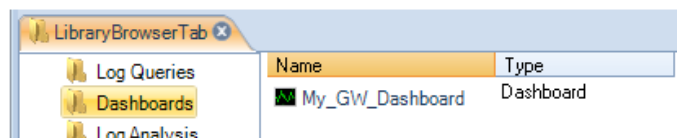
Once saved, the dashboard can be opened at any time by selecting the *Open* function in the toolbar and selecting the dashboard.



Managing Dashboards with the Library Browser

All dashboards are saved in the library of the InControl server database. This library also contains other saved objects such as ILA database queries. The *Library Browser* is a generalized feature for managing any of these saved objects, allowing them to be renamed, deleted, grouped into subfolders and activated.

For example, the dashboard called *My_GW_Dashboard* would appear in the library browser as shown below. Double clicking will activate it and a *Monitor Mode* tab will appear containing the dashboard.

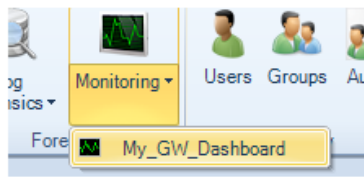


The library browser is fully described in *Chapter 19, The Library Browser*.

Activating from the Dashboard Button

As an alternative to activating a saved dashboard through the library browser, if a gateway is selected in the *Security Gateways* tab, pressing the lower part of the *Dashboard Monitoring* button in the *Home* toolbar brings up a list of available saved dashboards.

In the example below, the dashboard called *My_GW_Dashboard* is available for selection.

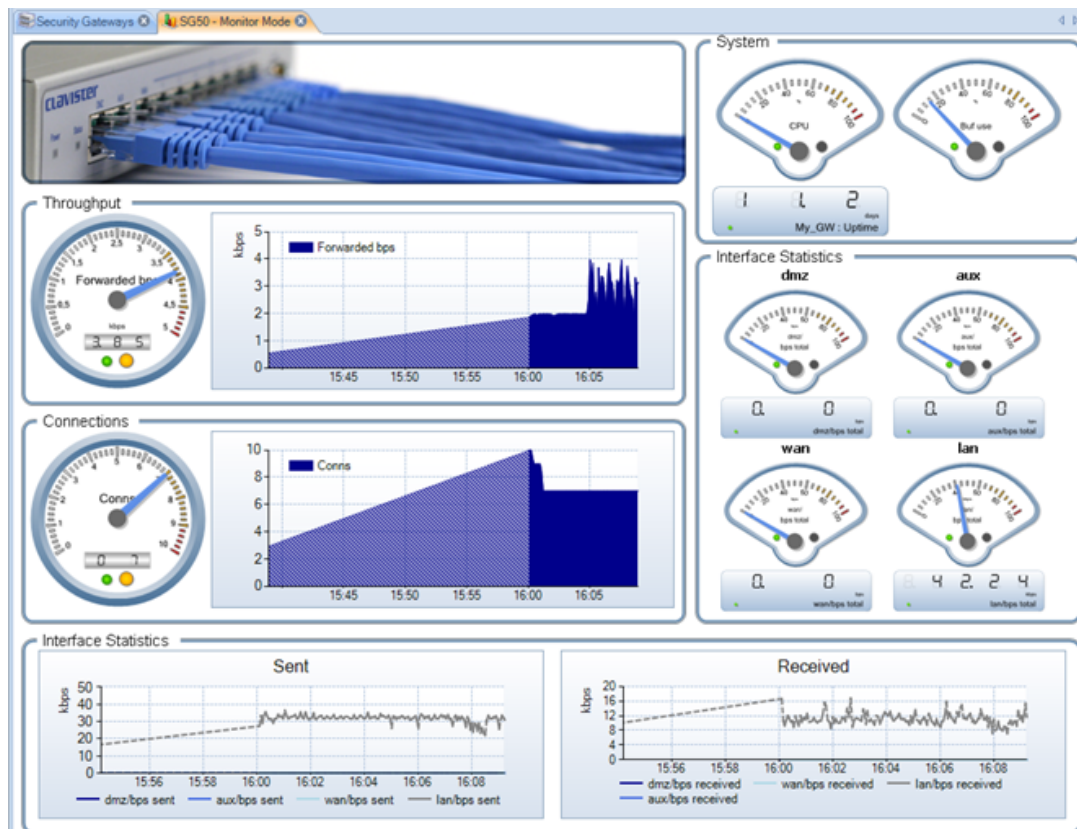


Using Quick Monitor

InControl provides a single pre-defined dashboard that can be displayed using the *Quick Monitor* button in *Security Gateways* toolbar.



Below is an example of how this default dashboard looks.



Tip: Reduce dampening to lower the processor load

To achieve the smooth movement of control indicators, for example the needle in a **Gauge** control, the InControl client can require significant processor resources. This can cause problems if the processor is of a slower type or many other, competing applications.

The InControl processor load can be reduced by going to **Client Settings** and reducing

*dampening from the default value of **High**.*

Chapter 18: Log Event Monitoring

- Memlog Monitoring, page 108
- The ILA, page 110
- The Log Explorer, page 119
- The Query Filter, page 123
- Log Query Language (LQL), page 126
- The Log Analyzer, page 132
- InControl Reporting, page 144

cOS Core generated *Log Event Messages* on a regular basis when certain system events occur, such as the triggering of an IP rule. These events can be captured and then examined using InControl.

There are two ways log events can be viewed in InControl:

- A *Quick Real-time* view can display *Memlog* contents which are log events captured in local cOS Core memory. This is described in *Section 18.1, "Memlog Monitoring"*
- Log messages captured by the proprietary *ILA* log server can be searched and displayed. This is described in *Section 18.2, "The ILA"*.

The proprietary query language that is used to construct ILA queries is described in *Section 18.5, "Log Query Language (LQL)"*.

A full description of cOS Core log generation and all message capture options can be found in the *cOS Core Administrators Guide*.

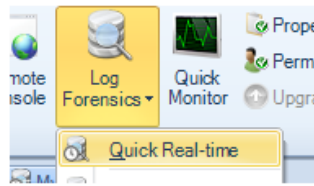
18.1. Memlog Monitoring

All log event messages generated by cOS Core are stored for a limited period in local memory. This type of logging is known as *Memlog* logging.

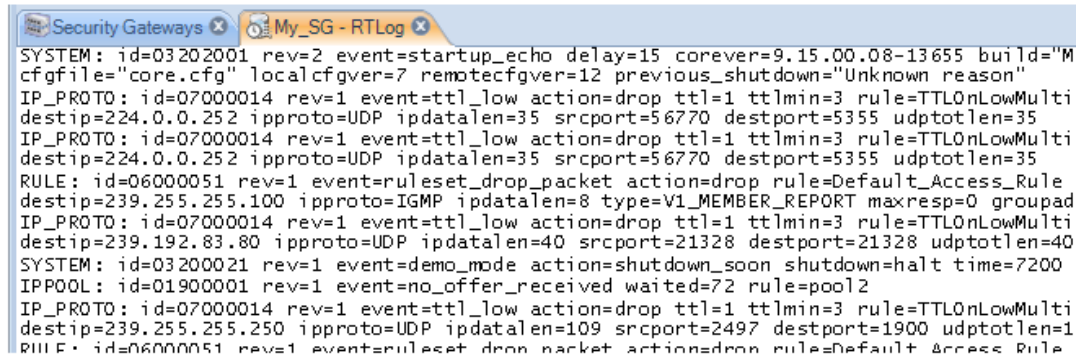
It is possible to use InControl to display the current log messages being written to *Memlog*.

This is done by selecting the gateway in the *Security Gateways* tab, pressing the *Log Forensics*

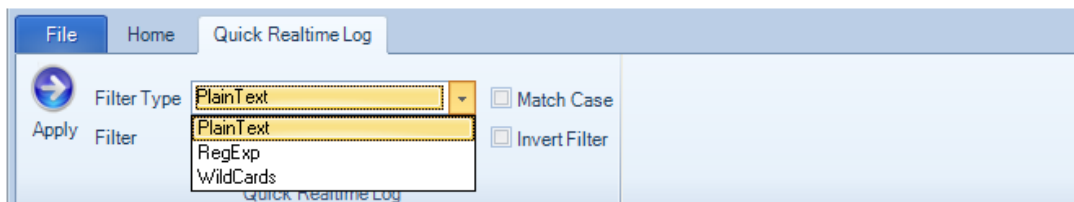
button and selecting *Quick Real-time* from the menu.



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:



The messages are stored in raw form and only limited filtering capability is possible using basic text searching criteria.



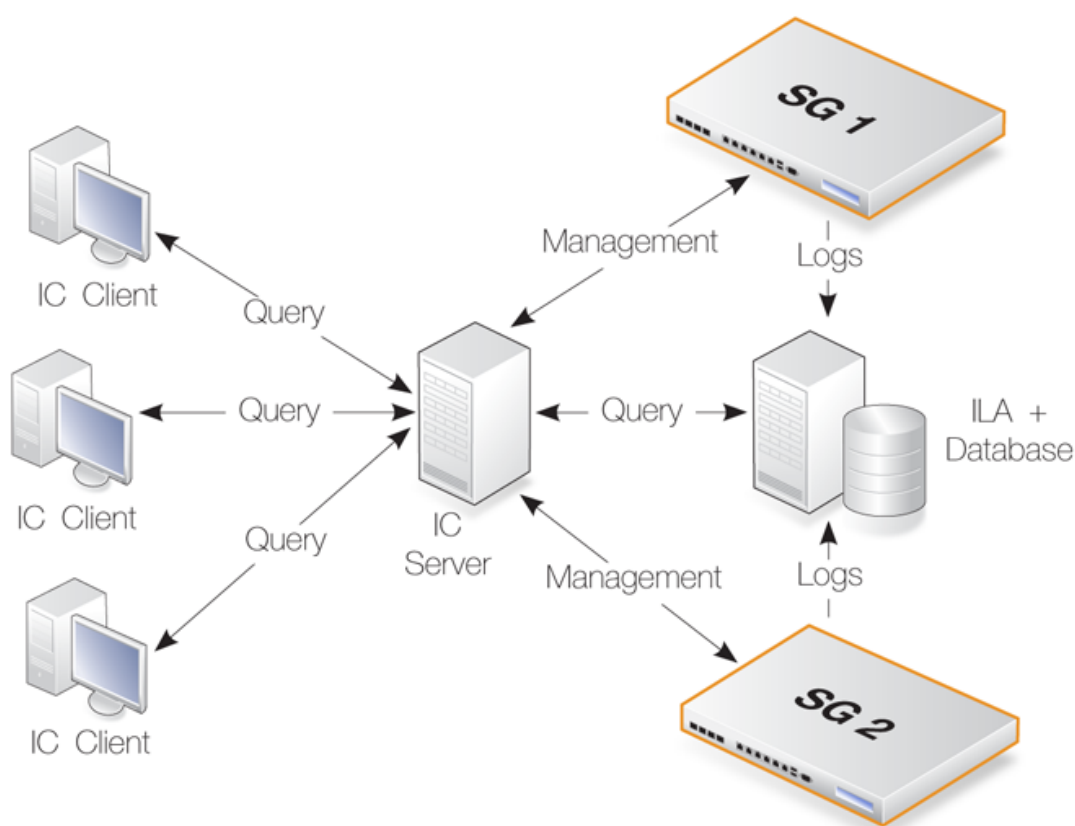
For a more sophisticated logging tool, the *ILA* is recommended and this is described next.

18.2. The ILA

A more sophisticated logging facility than *Memlog* is provided by the proprietary Clavister *InControl Logging Agent* (ILA). This software component comes with the InControl installation package and functions as an optional separate, independent server for receiving and storing cOS Core log event messages.

The ILA can capture log messages generated by any number of Clavister Security Gateways which are also managed through InControl. The ILA event database can then be examined through report generating features integrated into the InControl client.

The diagram below shows how ILA fits into InControl usage. Several security gateways can send messages to the ILA and InControl clients manage it, as well as send log queries to it, via the InControl server. All communication between clients and the ILA are mediated by the InControl server. The ILA and the InControl server could be installed on separate computers or the same computer and could be on the same or separate networks.



Installation

The ILA can be installed separately from the InControl server installation and a separate installer executable file is provided to do this which is called *InControl_ILA_Setup.exe*.

Alternatively, ILA installation can be performed as part of running the single bundled installer executable *InControl_Bundle_Setup.exe* which installs client, server and ILA consecutively. This is the recommended way as the latest versions of all components will be installed together.

Installing a new ILA version does not require uninstallation of the old version. In addition, the old ILA services will be stopped automatically then restarted with the new version.



Note: .NET 3.0 (service pack 2) is required

Both the InControl server and the ILA require at least .NET version 3.0 (service pack 2) to be installed.

The installer provides the option to install .NET as part of the installation process if it detects that it is not already installed.

The ILA can be installed on the same PC as the InControl server or on a different, possibly remote PC. The ILA is always installed on the same computer as the database files which store received log messages. If installed on a separate computer, the ILA must have a network connection to its associated InControl server. This connection can be local or could be made remotely over the public Internet.

More than one ILA installation can be fed by messages from a single Clavister Security Gateway. Similarly, one ILA installation can receive log messages from multiple security gateways. This is determined by what log servers cOS Core is configured to send messages to.

ILA Network Communication Uses Port 5555

If the InControl server and the ILA are running on the same computer, there will be no problem with port usage and communication between them.

However, if the ILA runs on a separate computer then that computer **must allow incoming TCP and UDP connections on port 5555**. TCP port 5555 is used when adding an ILA and/or deploying ILA configurations. UDP port 5555 is used when the InControl server polls the ILA for online status.

ILA Windows Services

The ILA runs as two, separate windows services which are constantly running. These two services are:

- **LogReceiver.exe**

This process performs the logging function of the ILA. It receives log messages and stores them in the ILA database.

The *Status* column of the *Logging Agent* tab in the InControl client does **not** indicate the status of this process.

- **ILA.exe**

If the *Log Analyzer* feature is enabled, this process builds the log analyzer database.

The process also performs all query functions. That is to say, all queries launched from either the *Log Explorer* or *Log Analyzer* features in the InControl client.

If a query is launched and this service is not running, the client will return an error message.

The *Status* column of the *Logging Agent* tab in the InControl client **does** indicate the status of this process.



Important: ILA services must run under same Windows account

*By default, the services **LogReceiver.exe** and **ILA.exe** will run under the same Windows user account. This should not be changed. If they run under two different accounts, the ILA will not function.*

The reason for having two services for the ILA is to allow the *LogReceiver.exe* service to be as efficient and robust as possible. If any execution bottlenecks occur in the *ILA.exe* service, they will not affect log message processing.

The either of the ILA processes stops running for some reason, Windows will wait one minutes before it automatically tries to restart the service.

Restarting ILA Services

Unlike the InControl server, the ILA does not have its own graphical user interface to stop or start its Windows services. If the ILA services might not be running then the status should be checked. One symptom is this if the logging agent has a status of *offline* in the client. Another symptom is if log queries are failing to execute.

To check the ILA services in Windows 7, go to **Control Panel > Administrative Tools > Services**. The Windows services management tool will open with a list of installed services. Look for *Logging Agent* and *Log Receiver* in the list.

 Clavister InControl Log Receiver	Clavister InControl Log Receiver	Started
 Clavister InControl Logging Agent	Clavister InControl Logging Agent	Started
 Clavister InControl Server	Clavister InControl Server	Started

The status for both should be *Started* if the services are running normally. If the status for either is *Stopped* then they can be restarted by selecting **Action > Start**.

Using a Local User Account

Like the installation of the InControl server described in *Chapter 2, Installing InControl*, it is highly recommended to use the same, separate, local user account for the ILA and ILA installation. A local account cannot be logged into remotely, therefore increasing security.



Important: The ILA service needs administrator privileges

*After ILA installation, the Windows service ILA.exe should be run under the local user account **and** this account should have administrator privileges over the ILA database folder.*

Administrator privileges allow the ILA server to create new log message files.

Installing Over Older Versions

When installing over an older version of the ILA, there is no requirement for uninstalling the old version first. In addition, the ILA servers does not require that its Windows service is halted first. This occurs automatically.

ILA Server and InControl Server Communication

Communication between the InControl server and the ILA is achieved using the Clavister

proprietary, secure *Netcon* protocol. Netcon requires that an agreed *Secret Key* is used by both sides of the communication.

By default, the ILA and server use an agreed, predefined secret key. This is displayed in the ILA configuration dialog available through the InControl client and which is discussed later in this section.

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

Configuring cOS Core for ILA Logging

cOS Core for each Clavister Security Gateway should be configured to specify which loggers to send messages to and which messages to send. The term *Logging Agent* is used to refer to an ILA server.

To specify a new ILA server, first press the *Logging Agents* button in the ribbon toolbar of the *Home* tab.



This will open the *Logging Agents* tab. To define a new ILA server, press the *Add* button and a new *Logging Agent* dialog will open.

 A screenshot of the 'Logging Agent' configuration dialog box. It contains the following fields:

- Name:** My_ILA_Server
- Parent:** (empty dropdown menu)
- Device is currently:** Online (selected radio button), Offline (unselected radio button)
- IP address:** 127 . 0 . 0 . 1 (with a small IP icon to the right)
- Port:** 5555
- Secret Key:** DBC2A65220E2D3753149EDED524FC1A140CDA6810FAE
- Comments:** Configure an ILA server.

In the example shown above, a symbolic name of *My_ILA_server* is given for the server. The IP address is given a default value of *127.0.0.1* (the loopback IP address) which will be correct if the ILA server is on the same computer as the InControl server.

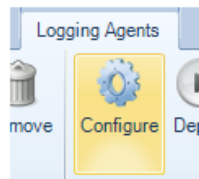
The secret key is automatically given the default value for the ILA server and will be correct provided it has not been changed. After clicking *OK*, this server definition will now appear in the *Logging Agents* tab.

Security Gateways					
Logging Agents					
Name	IPAddress	Port	Locked by	Status	
My_ILA_Server	127.0.0.1	5555		Online	

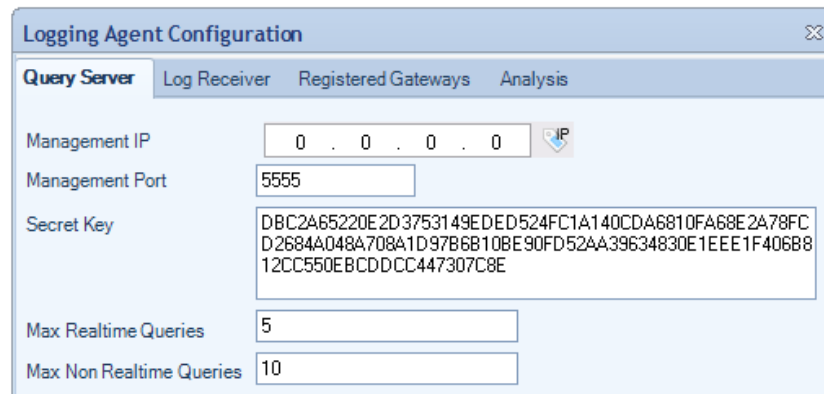
The *Online* field indicates that connection to this ILA server by the InControl server was successful. The *Locked by* field indicates any client that is currently editing the properties of this server.

Editing the ILA Server Configuration

The *Logging Agents* tab also provides the ability to configure the ILA server since, unlike the InControl server, there is no separate graphical interface for doing this.



This brings up the ILA configuration dialog.

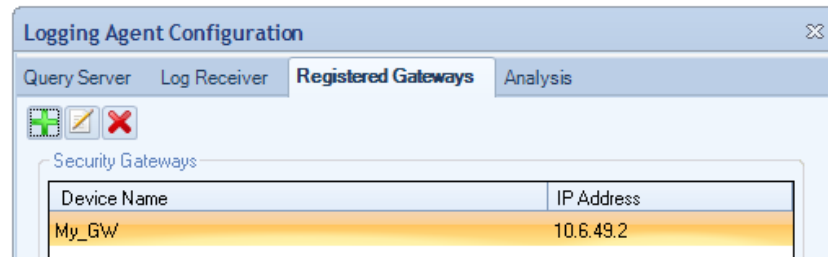


Here, the *Management IP* is the IP address from which management connections to the ILA server come. The management IP address of the ILA server itself is specified in the *ILA Properties* dialog.

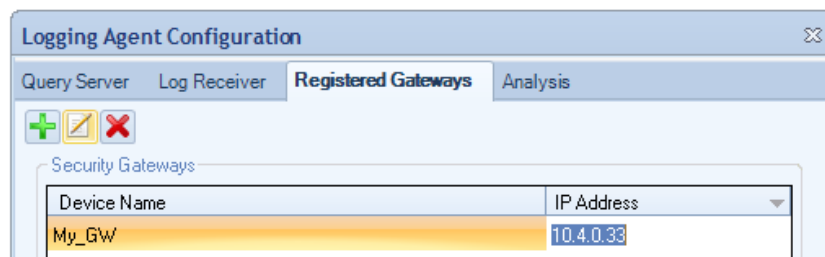
To configure the ILA to accept and store log messages coming from a particular security gateway, select the *Registered Gateways* tab and press the plus "+" button.



After selection, the chosen gateway will appear in the *Registered Gateway* list and the *IP Address* value for the gateway **will default to the management IP address of the gateway** and this is the address from which the ILA will expect log messages.

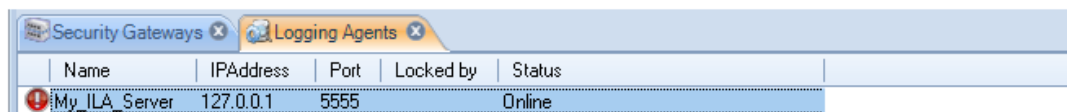


If necessary, this address should be changed by selecting the gateway line, pressing the edit button in the dialog and entering a new value, as shown in example below where the gateway called *My_GW* will send log messages from the IP address *10.4.0.33*.

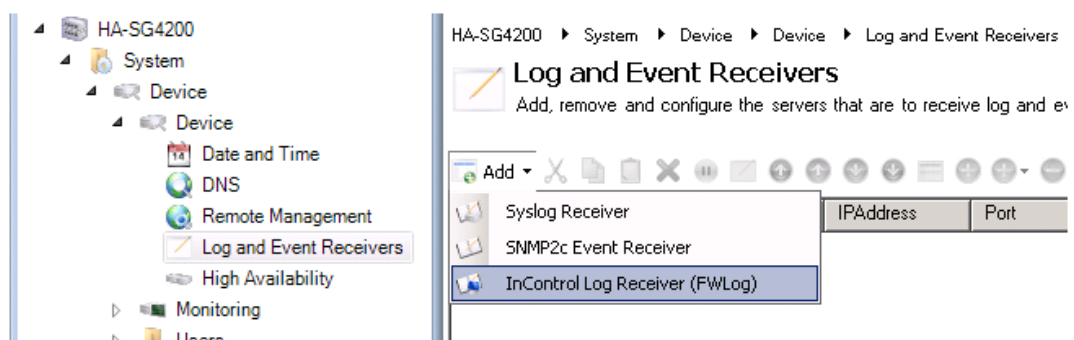


The ILA configuration dialog has the option to deploy immediately after the dialog closes or the deployment can be done using the separate deploy button in this tab's toolbar. Deployment means that the new settings are sent via the InControl server to the ILA server.

If the ILA server configuration has been changed but not deployed, an exclamation icon will appear next to the server in the server list.



Finally, the gateway itself must be configured to send log messages directly to the ILA server. This is done by selecting *System* then *Log and Event Receivers* and adding an *FWLog Receiver*.



The log receiver should be configured with the IP address and port number that is configured for the ILA server. Below, the defaults are specified.

Name:	<input type="text" value="My_ILA_Server"/>	
Routing Table:	<input type="text" value="main"/>	Specifies the routing table the clients host route should be added to.
IP Address:	<input type="text" value="127.0.0.1"/>	Destination IP address.
Port:	<input type="text" value="999"/>	Destination port.

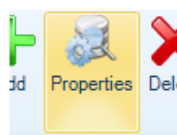
Changing the Secret Key

Changing the secret key of the ILA server is a two-step process where the key has to be changed first on the ILA server and then the local client:

- First, press the *Configure* button, change the secret key in the ILA server configuration and deploy the new configuration to the server.
- Second, right click the ILA server in the server list and select *Properties* to display the properties dialog. Now, set the secret key to same value that was deployed to the server in the previous step and close the dialog.

ILA Database Management

ILA database management options are found in ILA configuration dialog. Access this by selecting the ILA server in the *Logging Agents* tab and pressing the *Properties* button in the tab's toolbar.



Now select the *Log Receiver* tab in the dialog.

 The 'Logging Agent Configuration' dialog box with the 'Log Receiver' tab selected. It contains the following fields:

- UDP Port:
- File Size (Mb):
- Maintenance Hour:
- Days To Keep:
- Log Files Path:

The following parameters are relevant to the ILA database:

- **File Size (Mb)**

This value specifies the maximum file size of the individual files that store log data. The maximum size for this setting is limited to 200 MBytes. It is not related to the total size of the ILA database since the database consists of many of these files. However, the maximum size can affect search speeds.

The ILA database structure consists of a folder for each gateway generating logs. Within each

gateway folder there is a folder for all the log files for each month. At the start of a new day, a new daily log file is created in the relevant month folder. When this daily file reaches the configured maximum size it is closed, compressed using the GZIP algorithm and an additional log file is started for that day.

The advantage of this scheme is in searching logs. Each storage file begins with the start and end time of the logs it contains. This means that logs for a particular time interval can be found quickly provided the individual log files are not too large.

- **Maintenance Hour**

This parameter specifies the time of day when routine maintenance will take place. In the example shown above, 3.00 in the morning has been specified.

- **Days to Keep**

When the routine maintenance process runs, it deletes any files that are older than this numbers of days. This parameter is the principle means of controlling the disk space occupied by the ILA database.

It is up to the administrator to judge an appropriate value for this parameter. It should be based on the amount of free disk space available and the expected rate of increase in the log files. A useful exercise for making this judgment is to observe the size expansion over a few days of typical system usage.

If the ILA server is running on the same computer as the InControl server, it can be seen as also being covered by the alert the InControl server can generate should free disk space fall below a configurable value.

Log Folder and File Naming

As discussed above, ILA keeps messages in files that have a configured maximum size. These files are organized in the following way.

For each month of operation, a folder is created with a folder name made up of the current year and month. For example, the folder name used for the log files created during August 2011 is "201108".

The messages received for each new day within a month are placed in that month's folder and each log file created is given a name of the form:

```
<day>-<suffix>
```

For example, the first log file created on the first of any month has the name "1-0.fwl". The first file created for the second day of any month is "2-0.fwl".

When files reach the configured size limit and a new log file is created for that day, the filename is the same except for the suffix which becomes "-1", "-2" and so on for subsequent files. For example, when the first file for the first of the month reaches the configured limit, the second file created for that day is given the name "1-1.fwl". At the same time, the previous file is compressed using GZIP and its name is changed to "1-0.gz".

All log files for a particular security gateway are stored in a folder dedicated to that gateway and these are stored within the ILA main database folder. Each gateway folder name is created from the unique gateway ID number (since the gateway name can change). The configuration file *ILA.xml* contains a mapping of a gateway's ID number to its IP address.

ILA Logging Without InControl Management

Sometimes there may be a requirement to have a security gateway send log event messages to an ILA server but not give InControl management rights over the gateway.

When InControl can manage a security gateway it means its *NetCon Keys* have been added to the InControl database and any InControl client then has the potential to read and change the configuration. If the aim is just to enable ILA logging, then this can be done without giving the keys to InControl using the following steps:

- Open the InControl client and select the *Security Gateways* tab.
- Add the security gateway and give it a name **but** mark the gateway as being **Offline**. This means that InControl will not try to contact the gateway.
- In the *Logging Agents* tab, bring up the *Configuration* dialog of the target ILA server, select the *Registered Gateways* tab and add the newly defined gateway.

If the *Log Analyzer* function is also to be used, the gateway should be added under the *Analysis* tab (this can be done later).

When the dialog's *OK* button is pressed, this ILA configuration is deployed to the ILA server.

- Stop **both** ILA Windows services. This is done in Windows 7 by pressing the **Start** button, selecting **Run** and starting the utility *services.msc*. Locate the *LogReceiverandILA* service then stop them. Leave the utility open to restart the service later.
- The ILA configuration file *ila.xml* now needs to be manually altered. This file is located in the folder `%appdata%\Clavister\InControl\LoggingAgent`. After opening the file in a text editor, change the gateway's IP from the default of *0.0.0.0* to the actual IP address of the gateway. Save this change.

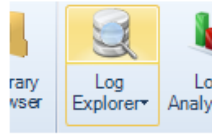
Every time the a new ILA configuration is deployed, this setting will be reinitialized to *0.0.0.0* and this step must therefore be repeated.

- Now restart *LogReceiverandILA* services then close the *services.msc* utility.

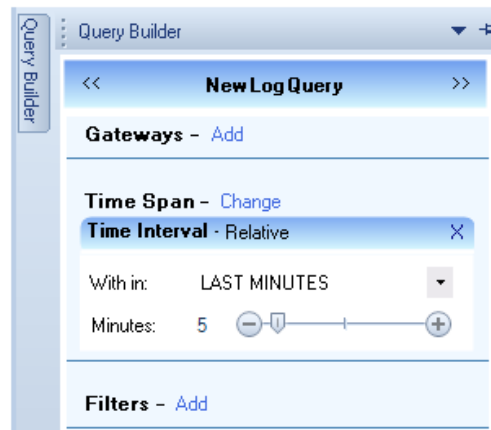
In a later version of InControl these steps will not be required and it will be possible to enable this option through a simple checkbox selection.

18.3. The Log Explorer

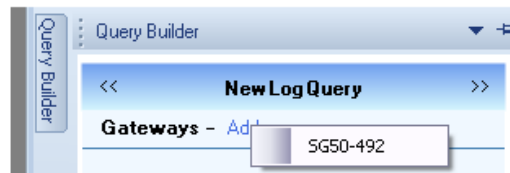
The InControl client provides extensive tools for looking at both real-time ILA logging and examining the log event history kept in the ILA database. To start doing either, press the top part of the *Log Explorer* button.



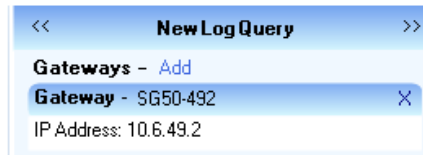
This opens the *Log Explorer* tab. On the left there is a tab which is selected for opening the *Query Builder*.



Select the *Add* option to choose which security gateways will be included in the query. In the example below only one gateway is selectable and it is called *SG50-492*.



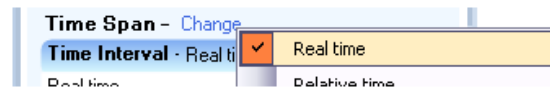
When selected, this gateway now becomes part of the query.



Multiple gateways can be added to the list of gateways for the query.

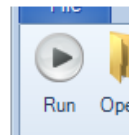
Displaying ILA Log Messages in Real-time

To show the logging that is taking place to an ILA server from the selected gateways in real-time, press the *Change* link for **Time Span** and select *Real Time* from the menu.



Running the Query

The above steps defined a simple query which was showing real-time logging for a particular security gateway. Once a query is defined, it needs to be executed and this is done by pressing the *Run* button in the toolbar.



A real-time display of the received log messages by the ILA server is then displayed. Below is an example of this output, showing administrator login and logout as well as messages related to HA heartbeats.

Time	De...	Name	Message ID	Rule	Severity	Category	Event	Ac
13:25	13:34:31	Unknown	03203000		Notice	SYSTEM	admin_login	
13:25	13:34:31	Unknown	04900001		Notice	SESMGR	sesmgr_session_cre...	none
13:24	13:34:31	Unknown	04000032		Warning	HWM	fanrpm_normal	
13:25	13:34:32	Unknown	01200043	HAMsg_IPCheck	Warning	HA	heartbeat_from_urk...	drop
13:27	13:34:33	Unknown	01200043	HAMsg_IPCheck	Warning	HA	heartbeat_from_urk...	drop
13:26	13:34:33	Unknown	01200043	HAMsg_IPCheck	Warning	HA	heartbeat_from_urk...	drop
13:28	13:34:34	Unknown	01200043	HAMsg_IPCheck	Warning	HA	heartbeat_from_urk...	drop
13:29	13:34:35	Unknown	01200043	HAMsg_IPCheck	Warning	HA	heartbeat_from_urk...	drop
13:28	13:34:35	Unknown	04000031		Warning	HWM	fanrpm_alarm	none
13:31	13:34:37	Unknown	03203001		Notice	SYSTEM	admin_logout	
13:31	13:34:37	Unknown	04900003		Notice	SESMGR	sesmgr_session_re...	none



Tip: Different severities have different colors

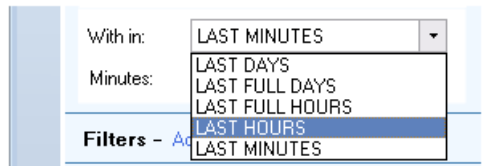
As can be seen the partial screenshot above, different severities are shown in different predefined colors. For example, log messages with severity **Notice** appear in black and messages with severity **Warning** appear in green.

Displaying Logs Using Relative Time

Instead of the real-time option, relative time can be selected.



This view of log messages looks backwards from the current time. A drop-down menu is used to select the desired unit of time and a slider control is used to select the number of the chosen time unit.

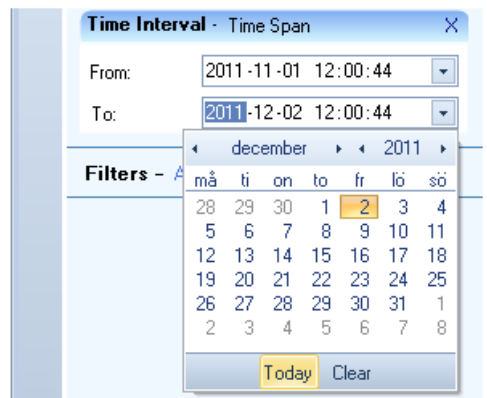


Displaying Logs Using a Time Span

The time span option allows the display of all logs in a specific time range.

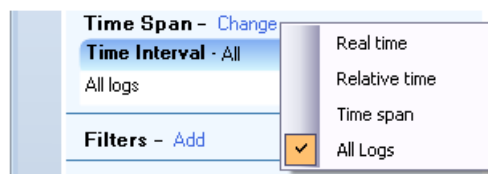


This view of log messages looks backwards to a specific time range which is specified using two date fields.

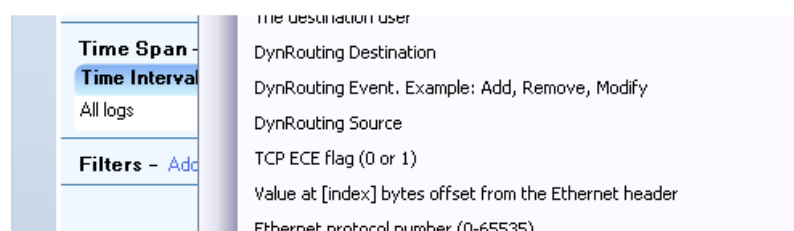


Adding Filters

Except for real-time log display, other options have the potential to display large numbers of log messages. This is usually always the case if the *All Logs* option is chosen.



To refine the displayed logs further, the *Filter* option can be chosen so that one or more filter data types can be matched against specific criteria. When the option is chosen, a data type can be selected from a large menu of choices.



After a filter data type is chosen, a boolean operator and a value can then be specified. In the example below, the action must equal *Allow* for the log message to be displayed.

The screenshot shows a dialog box titled "Filters - Add". Inside, there is a section labeled "Filter - action" with a close button (X). Below this, the "Operator:" is set to "Equal to" and the "Value:" is set to "Allow".

The applied filter can consist of several boolean expressions for different types of data. Below, a second condition to be added to filter out messages that have a severity equal to *Warning*.

The screenshot shows the same "Filters - Add" dialog box, but now it contains two filter conditions. The first condition is "Filter - action" with "Operator: Equal to" and "Value: Allow". The second condition is "Filter - severity" with "Operator: Equal to" and "Value: Warning".

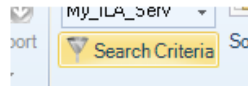
If there is than one filter condition, they can be combined either with a logical *AND* or a logical *OR* depending on the selection made from the combination choices.

18.4. The Query Filter

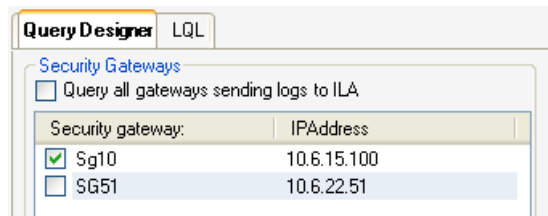
The *Query Filter* is part of the *Log Explorer* and provides an another means of performing simple queries on the ILA database.

The advantage of the *Query Filter* is that the administrator has direct access to the *Log Query Language* (LQL) statements which are the intermediate stage for log database query processing. LQL is described further in *Section 18.5, "Log Query Language (LQL)"*.

The *Query Filter* feature is started by pressing the *Search Criteria* button in the *Log Explorer* tab.



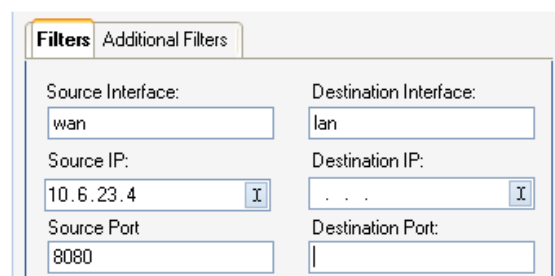
The *Query Filter* dialog then appears for specifying search criteria and a choice can be made about which security gateways are of interest.



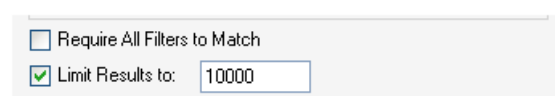
A specific time interval in the past can also be specified.



Most importantly, the individual filtering criteria for the selected security gateways and selected time period are now entered. In the example, below, the source interface, IP and port is specified along with the destination interface.



The *Require All Filters to Match* checkbox at the bottom of the *Query Filter* dialog decides if all the specified values need to match (a logical **AND** between matches) or any need to match (a logical **OR**).



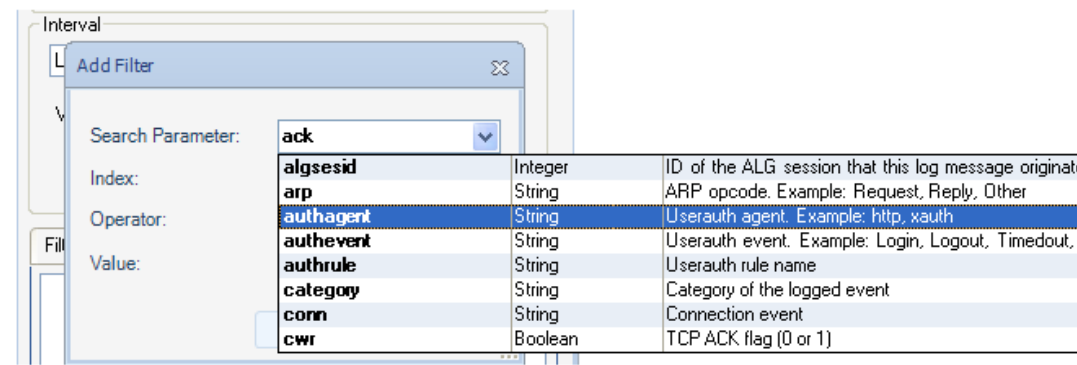
Pressing the **OK** button now sends the query to the ILA server and a list of matching log

messages is returned. It may be advisable to keep the message output limit to the default of 1000 in case the filter needs to be narrowed. Lists of output messages that are too large can make further analysis difficult.

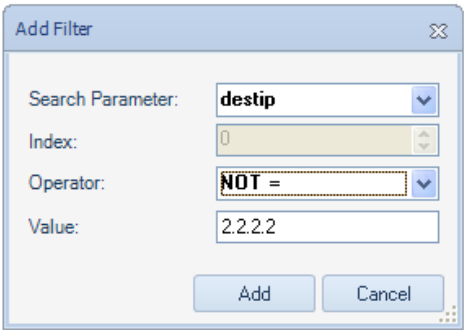
Adding More Filter Parameters

The basic filter parameters shown in the *Filters* tab of this dialog have been chosen as the most typical choices when filtering log messages.

However, the *Additional Filters* tab provides the option of add further criteria to the search. By selecting that tab and then selecting *Add*, a new dialog appears and a particular log message filtering parameter can be selected from the full list.



A set of logical operators can then be used to precisely define what is being searched for. This allows the definition of more complex criteria. For example, the criteria below is the *destip* **not** being equal to the value 2.2.2.2.



This additional filter is combined with any selections made in the previous *Filters* tab to form the final query.

Filtering the Resulting Message List

When the list of log messages matching a query is displayed, a particular column of data can be filtered further by right clicking on it. In the example below, the right click was over the *Message ID* (the context menu below appears to the right of the actual cursor position).

Time	Device Time (UTC)	Name	Message ID	Rule	Severity
14:17:49	15:11:48	Sg51	06000051	Default_Rule	Warning
14:18:22	15:12:21	Sg51	06000051	Default_Rule	Warning
14:18:33	15:12:32	Sg51	07000014	TTL0nLowMulticast	Warning
14:18:36	15:12:35	Sg51	07000014	TTL0nLowMulticast	Warning
14:18:36	15:12:35	Sg51	07000014	TTL0nLowMulticast	Warning
14:19:12	15:13:11	Sg51	07000014	TTL0nLowMulticast	Warning
14:19:49	15:13:48	Sg51	06000051	Default_Rule	Warning
14:20:25	15:14:24	Sg51	06000051	Default_Rule	Warning
14:21:04	15:15:03	Sg51	06000051	Default_Rule	Warning
14:21:05	15:15:04	Sg51	06000051	Default_Rule	Warning
14:21:07	15:15:06	Sg51	06000051	Default_Rule	Warning
14:21:11	15:15:10	Sg51	06000051	Default_Rule	Warning
14:21:49	15:15:48	Sg51	06000051	Default_Rule	Warning
14:21:56	15:15:55	Sg51	06000051	Default_Rule	Warning

With this menu it is now possible to sort or filter in various ways based on the *Message ID*. In addition, the following two options are available:

- **Filter Similar** - This will display all log messages that have the same values as the selected log message, except for the time and name fields. With this option, more than the just the *Message ID* is used for filtering.
- **Filter on Message ID** - will show only those log messages with the same value as the selected message, in this case all messages with the same *Message ID* of 07000014.

18.5. Log Query Language (LQL)

Overview

Clavister *Log Query Language* (LQL) is the language used to perform searches in the ILA log database.

As described previously in *Section 18.3, "The Log Explorer"* and *Section 18.4, "The Query Filter"*, log queries can be constructed without the need to know LQL. However, what happens internally to InControl is that such queries are first converted by the InControl client into LQL statements before being passed to the ILA server for processing.

With the *Query Filter*, the LQL statements created in this way can be examined and changed before the query is processed. For example, the following parameter values might be specified using the following *Query Filter* function.

The screenshot shows the 'Query Filter' dialog box with the 'Filters' tab selected. It contains two columns of input fields for defining search criteria:

Source Interface:	Destination Interface:
wan	lan
Source IP:	Destination IP:
1.2.3.4	4.3.2.1
Source Port:	Destination Port:
8080	9090
Severity:	Category:
EMERGENCY	ANTIVIRUS

If the *LQL* tab in the *Query Filter* is now selected, the LQL statement that this translates to can be immediately viewed and this is shown below for the example.

The screenshot shows the 'Query Filter' dialog box with the 'LQL' tab selected. It displays the generated LQL statement in a text area:

```

1 SELECT TOP 10000 BINARY FROM SG10 LAST MINUTES
2 5 WHERE recviface = 'wan' OR srcip = '1.2.3.4' OR srcport =
3 '8080' OR destiface = 'lan' OR destip = '4.3.2.1' OR destport =
4 '9090' OR severity = 'EMERGENCY' OR category =
5 'ANTIVIRUS'

```

Alternatively, a search can be made by creating the entire LQL statement from scratch. The *LQL* tab is first selected and the an LQL query entered directly into the dialog's text box. To do this, it is necessary to understand how to construct LQL statements.

LQL Syntax

LQL is similar to the traditional SQL used as a query language in many database products. However, LQL has a large number of cOS Core specific keywords and statements. The syntax of an LQL statement 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* (described later), separated by a comma, are specified.

After the mandatory *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 available in the LQL language:

Operator	Usage	Description
NOT	NOT <i>expression</i>	Negates a boolean expression.
AND	<i>expression1</i> AND <i>expression2</i>	Combines two Boolean expressions and evaluates to TRUE when both expressions are TRUE.
OR	<i>expression1</i> OR <i>expression2</i>	Combines two boolean expressions and evaluates TRUE when either of the expressions are TRUE.

The following should be noted about using logical operators:

- The logical operator *OR* and the operator *AND* cannot be used in a single filter expression. For example, the following is valid:

```
srcip='10.0.0.1' AND destip='192.168.123.1' AND destip='192.168.123.2'
```

However, the following is **not** valid:

```
srcip='10.0.0.1' AND (destip='192.168.123.1' OR destip='192.168.123.2')
```

- To achieve the equivalent of mixing *AND* with *OR*, create separate filters and enable or disable the option **Require all filters to match**. Disabling this option is equivalent to a logical *OR* between the individual filters. Enabling the option is equivalent to a logical *AND* between the filters.

For example, to implement the invalid expression above, the expression must be broken into two filters. First, create the following filter for the first part of the expression:

```
srcip='10.0.0.1'
```

Then, create the following filter for the second part of the expression:

```
destip='192.168.123.1' OR destip='192.168.123.2'
```

Now, enable the option **Require all filters to match** to logically *AND* the two filters.

- The *NOT* operator always takes precedence over the other operators.
- Parentheses can be used with the *NOT* operator. For example:

```
NOT(srcip='10.0.0.1' AND destip='192.168.123.1')
```



Note: Capitalizing the logical operators is optional

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 the single quote (') character:

```
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 and these are listed below:

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
hwsrcc	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
icmpsrcip	IPv4 address	Source IP address in ICMP-encapsulated IP packet
icmpdesctip	IPv4 address	Destination IP address in ICMP-encapsulated IP packet
icmpsrcport	Integer	Source port (0-65535) in ICMP-encapsulated IP packet
icmpdestport	Integer	Destination port (0-65535) in ICMP-encapsulated IP packet
icmppipproto	String	IP protocol (0-255) in ICMP-encapsulated IP packet
description	String	Description of the event
fin	Boolean	TCP FIN flag (0 or 1)

Variable	Value Type	Description
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
algmod	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 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
gateway	Name of the gateway that sent the data

Name	Description
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
icmpsrcport	Source port of an ICMP-encapsulated UDP/TCP packet
icmpstd	ttl, icmptype, icmpipproto, icmpdestip, icmpsrcip 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
tcphdrlen	TCP header length
tcpdatalen	TCP data length
tcpptolen	TCP total length (data + header)
standard	date, time, gateway, category, recvif, srcip, srcport, destip, destport, ipproto and description
tcpstd	tcpdatalen, tcphdrlen, 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
usernames	username, srcusername, and destusername

Name	Description
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 (shown above) and may be terminated at any point. For example, the following is a valid time statement:

```
TIMES 2000-01 TO 2000-02
```

18.6. The Log Analyzer

The *Log Analyzer* is a feature that provides further analysis capabilities for looking at ILA log events. However, instead of analyzing the live ILA database logs directly, the analyzer looks at its own special *Log Analyzer Database*.

The log analyzer database is different in that it does not collect individual log events. Instead, it collects statistics for the occurrence of particular event types. For example, the opening of new connections. The log analyzer only starts to be built when the collection of all or specific statistics are enabled for individual security gateways. By default, the database software used is SQLite™ but, as discussed at the end of this section, the administrator can configure InControl so the database is built using alternative software.

The log analyzer database is not built in real-time like the standard ILA database. A low priority background process adds incoming log messages to the database and there can be a brief delay between the two databases becoming synchronized. The reason for this is that the log analyzer database is highly structured to allow much more complicated reporting to be performed quickly.

The *Log Analyzer* does **not** use LQL as an intermediate stage for query processing. LQL is only relevant to the *Log Explorer* feature.



Note: A Summary of the Log Analyzer

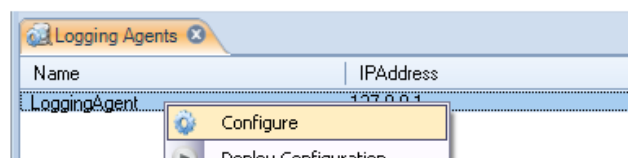
It is important to remember the following about the log analyzer:

- *The analyzer has its own, separate database.*
- *The analyzer database collects statistics about log messages sent to the ILA. It does not collect the log messages themselves.*
- *The analyzer database is only built when enabled through the ILA configuration dialog.*
- *The analyzer database is updated by a low priority background process. It is not updated in real-time and heavy loading can create a delay before the latest statistics are visible in queries.*

Enabling the Log Analyzer Feature

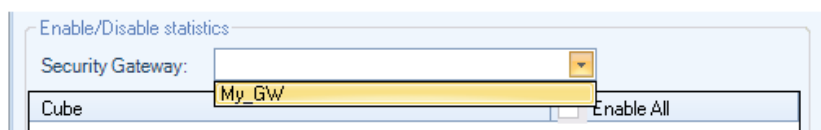
Enabling the log analyzer feature for a security gateway is done with the following steps:

- In the *Logging Agents* tab, open the configuration dialog for the relevant *Logging Agent* by either double clicking the logging agent entry or selecting the agent and pressing the *Configure* button. This can also be done by right clicking the logging agent and selecting the *Configure* option.



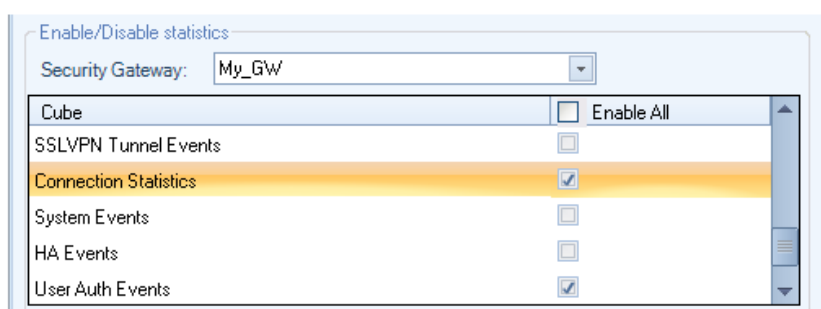
- In the configuration dialog, select the *Analysis* tab and choose a security gateway from the drop-down menu. This is the gateway for which statistics will be saved in the analyzer

database.



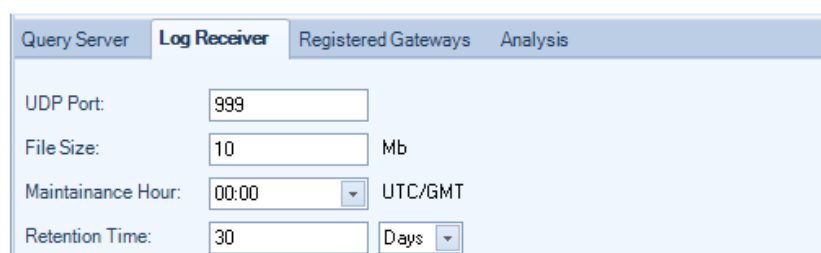
- Now, choose the statistics that are to be collected for this security gateway. These are referred to as the type of *Cube* since the collected data will have more than two dimensions.

For example, in the screenshot below, *Connection Statistics* and *User Auth Events* will be analyzed later.



- This process is then repeated for any other gateways for which statistics are to be saved. Any number of statistics can be saved for any gateway. The database size can become large over an extended period of time and it therefore recommended to limit statistics collection to the least acceptable number of statistics for the least acceptable number of gateways.
- Press *OK* to commit the logging agent configuration changes. The configured statistics will now begin to be saved by the ILA server for analysis by the *Log Analyzer* feature.

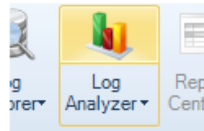
If later, the reverse process is followed so that a selected statistic becomes deselected for a gateway, then that statistic will be removed from the log analyzer database. However, removal does not happen immediately. Instead, this is done during the scheduled maintenance period for the ILA which is specified in the *Log Receiver* tab.



Once the log analyzer database is being constructed for a particular security gateway, the log analyzer query functions can be used to generate reports from that database.

Starting the Log Analyzer

The report generator for the analyzer is started by first pressing the top part of the *Log Analyzer* button in the *Home* toolbar.



This opens the *Log Analyzer* tab. This displays a summary of the current log analyzer database. Initially, this is empty.

As the database expands, the summary might look something like the one below. It summarizes the entire database and summarizes the data for each type of *Cube* currently configured.

Analysis database size: 14 Megabyte(s)
Remaining disk space: 37 Gigabyte(s)

Total log events scanned	Total slices	Earliest log event	Latest log event
2,366,982	33882	Sunday, November 30, 2008	Thursday, April 12, 2012

☐ Cubes Summary

Cube name	Slice count	Earliest event	Latest event	Last update
URL Requests	406	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
Bandwidth Usage	17158	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
ARP And ARP Poison Events	11219	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
L2TP Tunnel Events	26	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
SSLVPN Tunnel Events	4	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
Connection Statistics	3693	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
System Events	1360	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
High Availability Events	2	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012
User Authentication Events	14	Sunday, November 30, 2008	Thursday, April 12, 2012	Wednesday, April 25, 2012

☐ Gateways Summary

Gateway name	Slice Count	Earliest event	Latest event	Last update
--------------	-------------	----------------	--------------	-------------

The term *Slice* is a data warehousing term and does **not** equate with the total number of statistics collected, it can only be used as a guide to the number. However, the number of slices for a cube compared with the total slices in the database indicates the contribution made by that cube.

Also displayed is the status of the background process which updates the database.

Constructing Analyzer Queries

On the left of the *Log Analyzer* tab is the query builder for the log analyzer database. The query is constructed here and then the query is executed by pressing the *Run* button.

A query is built as follows:

- **Select the Cube (required)**

The *Cube* is the type of statistics to be analyzed. The cube selected must be one of the cubes that the ILA is configured to store in the analyzer database. In the screenshot below, the *Bandwidth Usage* cube is selected for this example. The log message IDs included within each cube are listed in *Appendix A, Cube Log Messages*.

By default, the query is assumed to be the selected cube for all security gateways. This can be narrowed using the *Filters* option.

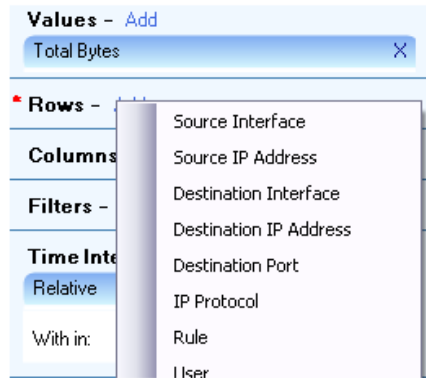
- **Select the Values (required)**

The *Values* setting specifies which statistic from the selected cube is to be displayed in the body of the generated reports. In this example, the *Total Bytes* (sent plus received) will be displayed.

The red asterisk next to *Values* indicates that this is a mandatory parameter that must be specified next.

- **Select the Rows (required)**

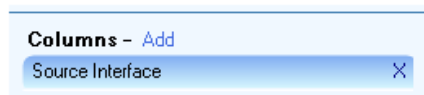
The *Rows* selection specifies what groupings are to be specified in the rows of the data table as well as along the X axis of the generated chart.



- **Select the Columns (optional)**

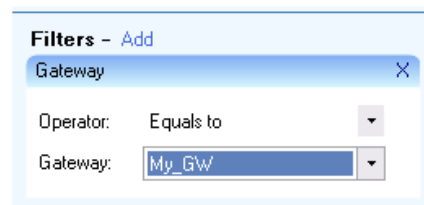
The *Columns* selection specifies what groupings are to be specified in the columns of the data table and along the Y axis of the generated chart. The same groupings can't be specified on for both *Rows* and *Columns*.

If the columns are not specified, the data table columns and chart Y axis default to the *Values* parameter.



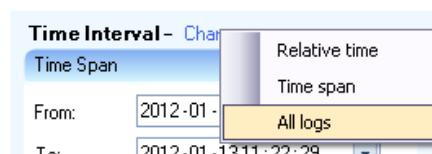
- **Select the Filters (optional)**

Further refinement of the query can be achieved using *Filters*. These allow boolean expressions to be added to the query. For example, the filter shown below specifies that only statistics for the security gateway called *My_GW* are to be included in the query.



- **Select a Time Interval (optional)**

By default, a time window is specified in a query. This is to prevent the administrator from accidentally launching a query which will go through all the statistics since the database can be very large. However, it is possible to query all statistics by selecting the *All logs* option from the *Time Interval* menu as shown below.





Note: Cube, Values and Rows are mandatory

As indicated above, a query requires, at minimum, the **Cube**, **Values** and **Rows** parameters to be set.

Log Message Timestamping Uses UTC/GMT

The log messages sent by cOS Core to the ILA are always timestamped with the time in UTC/GMT. This is done so all security gateway use a common time reference regardless of their location.

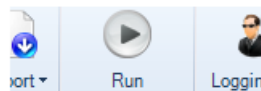
When constructing queries with the log analyzer which involve time, it should always be remembered that the time specified should be UTC/GMT and **not** the local time of the client or security gateway.

However, the ILA also keeps a record of the local time when it receives the log message. In the reports generated from InControl log queries, the *Time* column is the local time when the log message was received by the ILA and the *Device Time* is the UTC/GMT timestamp on the log message added by cOS Core. An example of these two columns in report output from the log analyzer is shown below.

Time	Device Time (UTC)
2012-04-16 02:00:01	2012-04-16 00:00:00
2012-04-16 02:00:01	2012-04-16 00:00:01
2012-04-16 02:00:01	2012-04-16 00:00:01
2012-04-16 02:00:01	2012-04-16 00:00:01
2012-04-16 02:00:01	2012-04-16 00:00:01

Running the Query

When the query is defined, the *Run* button is pressed to begin processing the data in the log query database.



The Last Hour's Data May Not Be Included

The background process which updates the database from the log files runs every 60 minutes. This means that a query will potentially not have access to as much as one hour of the most recently recorded log data. It also means that starting with an empty database, it takes 60 minutes before any data is written into it.

In addition, a query must wait for this hourly background update process to complete if they are both running at the same time. Typically, this will delay the query for no more than a few seconds. However, in some cases where a large update is underway, the wait may become unacceptable and the query will need to be cancelled by the user.

Limiting the Number of Slices Processed

The lower part of the analyzer panel allows the number of database slices in a query to be limited. This is useful when the database becomes large. As mentioned previously, the number of slices do not equate to the number of statistics since there can be more than one statistic in a

slice.

☒ Auto drill down
☒ Require all filters to match
☒ Limit slices to: 10000

A Simple Example Query

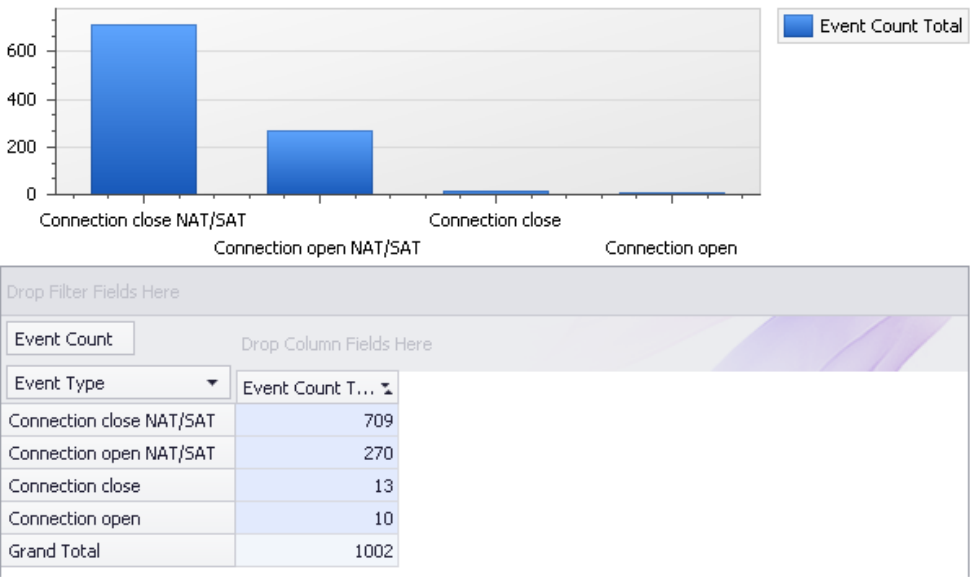
Below is shown an example query which examines connection events broken down by type over a period of time. The period selection is not shown but is limited to a particular time window.

Cube
Connection Statistics

Values - Add
Event Count

Rows - Add
Event Type

After pressing the *Run* button the following bar chart is an example of what might be displayed with the data being summarized both in graphical and numerical form:



Saving Analyzer Queries

A log analyzer query can be saved to the InControl *Object Library* under a specific name by pressing the *Save* button.



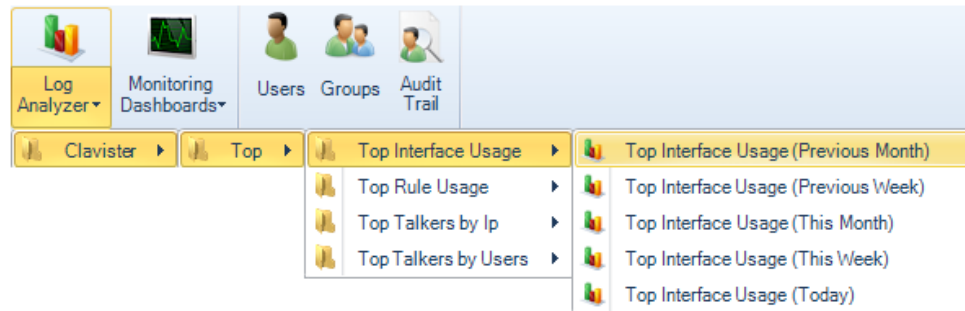
This saves the query not the query's results. The query can then be accessed and executed again through any of the following methods:

- Through the *Library Browser*.

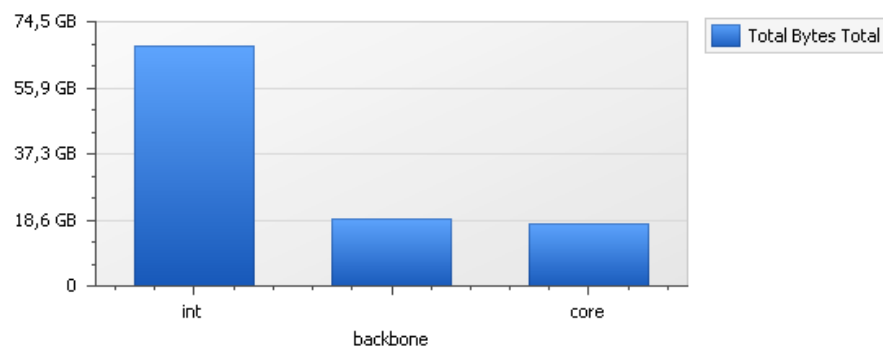
- Through the menu that appears when the *Log Analyzer* tab's *Open* button is pressed.
- Through the menu which appears when the bottom of the *Log Analyzer* button is pressed.

Predefined Queries

A number of predefined analyzer queries come with InControl as standard as these are accessible through the *Library Browser*, through the *Log Analyzer* tab's *Open* button or through the *Log Analyzer* button's bottom half. An example selection in this menu is shown below.



If this predefined query is selected and executed, the resulting results graph is shown below and breaks down traffic in bytes over the previous calendar month by interface. The term *Previous Month* in the menu means the complete calendar month prior to the present month.



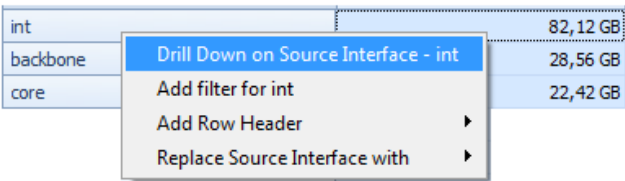
The three interfaces *int*, *backbone* and *core* are displayed in the graph because these are also the interfaces selected in the accompanying numerical results table. By selecting any other interfaces in the table, the barchart's contents can be changed.

Total Bytes	Drop Column Fields Here
Source Interface	Total Bytes Total
int	67,8 GB
backbone	18,79 GB
core	17,56 GB

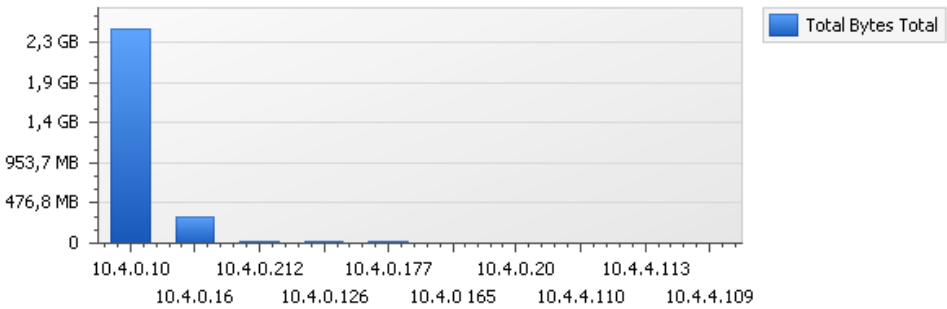
Drill Down

Within the breakdown of statistics by interface, it is possible to break down a particular interface further into individual IP addresses. This feature is known as *Drill Down*.

For example, to drill down into the statistics for the interface called *int*, we can right click on the *int* cell in the table to get a context menu.



By selecting *Drill Down on Source Interface*, the displayed barchart might become something similar to that shown below.



The table below the chart will also change to show the exact traffic breakdown by IP address.

Source IP Address	Total Bytes Total
10.4.0.10	36,21 GB
10.4.0.126	6,45 GB
10.4.0.16	1,45 GB

Auto Drill Down

The drill down behavior is different depending on whether the *Auto drill down* option is enabled. If it is enabled, double clicking a cell will automatically run a new query which assumes that a further data breakdown based on the possible fields. For example, we could have simply doubled clicked the table cell for the *int* interface above to drill down to the IP usage.

When this feature is disabled, double clicking will add to the left hand display of the query criteria but the query will not be run. This allows further modification of the query criteria before execution.

Changing the Database Software

As mentioned previously, by default the ILA uses the SQLite™ software product to build its database from log files and this product is installed as part of the InControl installation process. The SQLite database is always built on the same computer as the ILA server.

The SQLite product is a fast and effective database solution for smaller InControl installations where the database size is not much greater than one gigabyte. For database sizes far in excess of one gigabyte, SQLite can present performance issues which will be seen in the speed of background updating and the response time to complex queries.

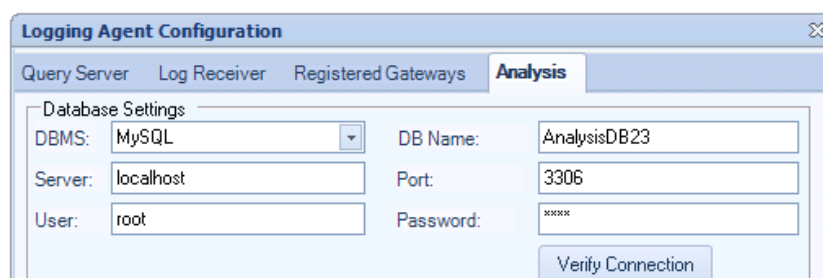
For installations requiring a large database size, one of the following 2 alternative databases should be used:

- **MySQL**
- **InfoBright** (recommended)

Both can provide a better database solution but are not supplied by Clavister. They must be installed as a separate standalone product. Of the two, InfoBright is recommended over MySQL, since it gives vastly superior retrieval speed with the kind of database queries that are typical with this kind of data.

Using MySQL

The *Logging Agent Configuration* dialog below shows how the *DBMS* setting is changed to configure InControl to use MySQL. The MySQL software can be running on the same or a different computer as InControl.



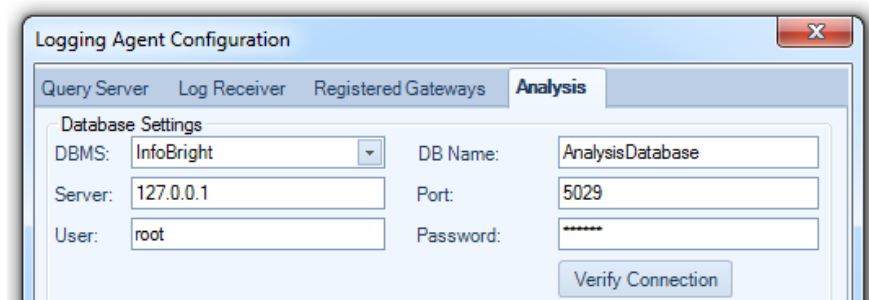
When MySQL is chosen the following data fields are required:

- **DB Name** - This is the name of the database that InControl will create once the dialog is closed.
- **Server** - The IP address of the MySQL server. If MySQL is running on the same computer as the ILA server, this field should be set to *localhost* or *127.0.0.1*.
- **Port** - The port that the MySQL database listens on. The default port is 3306.
- **User** - The MySQL username which InControl will use for access. Within MySQL this user needs the following privileges:
 - i. The ability to create databases.
 - ii. Read and write access.
- **Password** - The password associated with the username.

As soon as the dialog changes are saved, the MySQL database will be created by InControl and the database will begin to be built. Any existing log files will be written into the database. However, migration of data from the old SQLite database is not possible.

Using InfoBright

The *Logging Agent Configuration* dialog below shows how the *DBMS* setting is changed to configure InControl to use InfoBright. The InfoBright software can be running on the same or a different computer as InControl.



When InfoBright is chosen the following data fields are required:

- **DB Name** - This is the name of the database that InControl will create once the dialog is closed.
- **Server** - The IP address of the InfoBright server. If InfoBright is running on the same computer as the ILA server, this field should be set to *localhost* or *127.0.0.1*.
- **Port** - The port that the InfoBright database listens on. The default port is 5029.
- **User** - The InfoBright username which InControl will use for access. Within InfoBright this user needs the following privileges:
 - i. The ability create tables, drop tables, insert, update, delete and create index.
 - ii. Read and write access.
- **Password** - The password associated with the username.

Just as with MySQL, as soon as the dialog changes are saved, the InfoBright database will be created by InControl and the database will be built. Any existing log files will be written into the database. However, migration of data from the old SQLite database is not possible.



Important: InfoBright must have sufficient RAM memory

Ensure that InfoBright runs in an environment that provides the following minimum amounts of RAM memory:

- *On 32 bit systems: 1 Gbytes of RAM.*
- *On 64 bit systems: 2 Gbytes of RAM.*

If the RAM memory is insufficient, reporting will work at first and then, after a certain number of reports are generated, the reports will only contain the message:

No data was returned from the Logging Agent

Restarting the InfoBright database server can temporarily solve this issue.

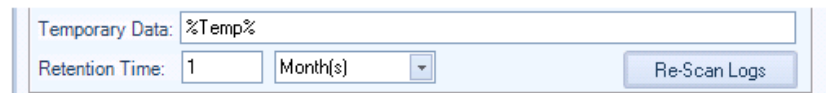
Changing Back to SQLite

The administrator might try using one of the alternative database options and decide that the SQLite version better suits their needs. They can then reselect SQLite. However, the directory on the server used for the ILA database will not be the original directory and instead defaults to a new top level directory the server creates called *C:\Clavister\Analysis*.

The reason for switching to this new directory path for the ILA SQLite database is that the client initiating the change cannot know which version of Windows the server is running on and therefore where the original SQLite database was placed at installation time.

Advanced Database Settings

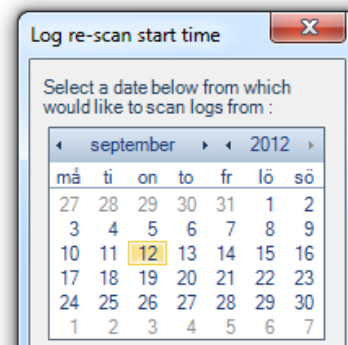
In the dialog that defines the database used, there are fields that allow the setting of the location for temporary data, the retention time and resetting of log indexing.



The *Temporary Data* location is the directory used for storing log data prior to it being added to the database. If the default temporary location is space constrained, it may be advisable to specify an alternative location since the amount of space required can be many gigabytes.

The *Retention Time* is how long old the data in the database can become before it is automatically deleted during routine hourly maintenance. If this time is reduced then the deletion of data will also only occur during hourly maintenance activity.

The button *Re-scan Logs* gives the administrator to ignore all data before a particular date for analysis. When pressed, a further dialog will appear so a particular day can be chosen.



All historical data in the database prior to the date selected is discarded and only data from that date onwards will be retained and be available for analysis.

18.7. InControl Reporting

The *InControl Reporting* subsystem allows the generation of cOS Core log event analysis reports as a file in either HTML or PDF format.

When creating a report file definition, one or more *sections* are added to the definition. Each section contains one of the *Log Analyzer* predefined queries or a custom query (see *Section 18.6, "The Log Analyzer"*). A query can appear in graphical and/or table format and further refinements can also be made to the query.

The following are some key points about the generation of these reports:

- The reports are initiated by the client but it is the InControl server that performs the generation of these reports.
- After initiating report generation, the client does not have to wait for the report to be finished. A progress bar at the bottom of the client interface indicates the report generation progress and the client can continue to be used for other tasks.
- Multiple reports can be in the process of generation at the same time on the server and each will have its own progress bar at the bottom of the client interface.
- The user can close the InControl client and this will have no effect on any ongoing report generation.
- When a report finishes generation, it becomes part of the *Report Archive* on the server. This archive can be managed by the InControl client and completed reports can be opened and saved to the local disk.

Prerequisites for Creating Report Files

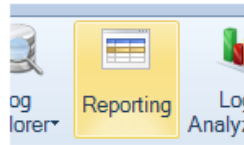
Before a report can be created, the following prerequisites need to be met:

- At least one Clavister Security Gateway needs to be configured to send its log messages to an InControl *Logging Agent*.
- The *Data Cubes* option needs to be enabled for the receiving logging agent. This is done with the following steps:
 - Select *Logging Agents* to see all configured agents.
 - Select the target logging agent from the list.
 - Select *Configure*.
 - Select *Analysis*.
 - Select the *Enable All* option in the *Cube* list, as shown below.

Cube	<input checked="" type="checkbox"/> Enable All
URL Requests	<input checked="" type="checkbox"/>
Bandwidth Usage	<input checked="" type="checkbox"/>
IDP Events	<input checked="" type="checkbox"/>
AntiVirus Alerts	<input checked="" type="checkbox"/>

Listing Existing Reports

To list all the existing reports, select the *Home* toolbar ribbon and then select the *Reporting* icon to open the *Reporting* tab.

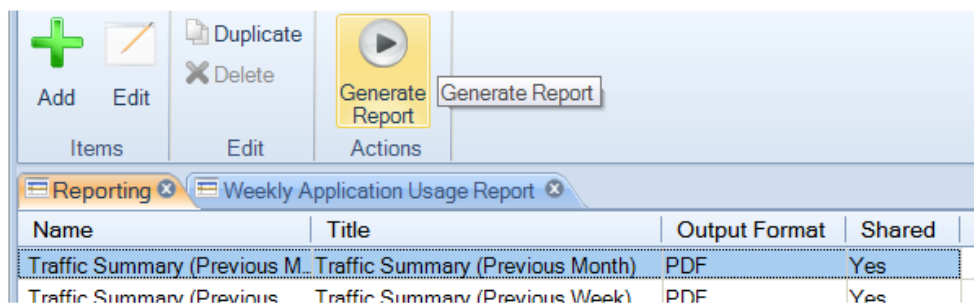


The first time the reporting tab is presented, it displays a list of predefined reports as shown below.

Reporting			
Name	Title	Output Format	Shared
Traffic Summary (Previous M...	Traffic Summary (Previous Month)	PDF	Yes
Traffic Summary (Previous...	Traffic Summary (Previous Week)	PDF	Yes
Traffic Summary (This Month)	Traffic Summary (This Month)	PDF	Yes
Traffic Summary (This Week)	Traffic Summary (This Week)	PDF	Yes
Traffic Summary (Today)	Traffic Summary (Today)	PDF	Yes

Generating a Report

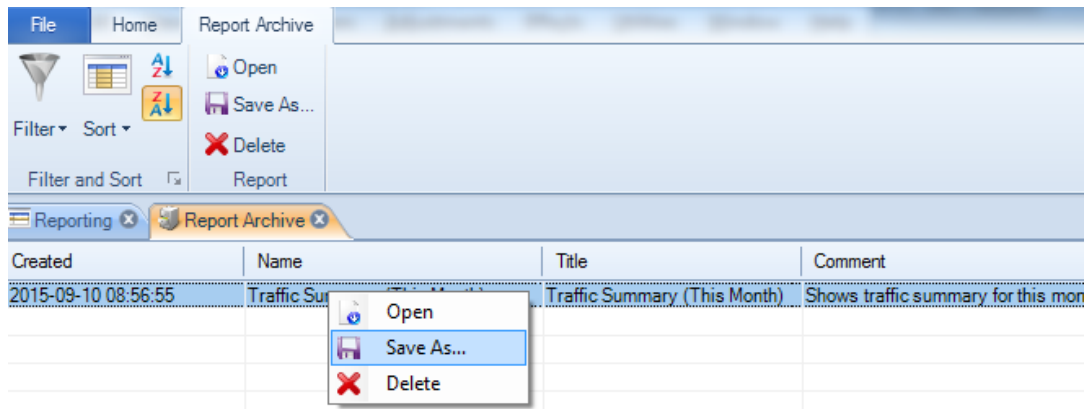
Any of the reports in this list can be generated by selecting the individual report and then selecting the *Generate Report* option in the toolbar ribbon.



The InControl server will now start to generate the report in the background and a progress bar, like the one below, will appear at the bottom of the client interface to indicate the report's progress. The client can be used for other tasks while the report is generated by the server in the background.

Progress View			
Action	User	Object	Progress
Generate report	admin	Traffic Summary (This...	50%

Multiple reports can be requested and can be generated on the InControl server at the same time. A separate progress bar will appear at the bottom of the client interface for each report. Even if the client is closed, report generation will continue. When a report is complete, it is saved on the server in the *Report Archive* and this archive can be managed by pressing the *Archive* button in the toolbar so that the *Report Archive* tab opens in the client as shown below.



Using the *Report Archive* tab, the finished reports on the server can be managed and also saved to the local disk using the *Save as..* option.

Creating a New Report

To create a new report, select *Add* and the following new report dialog will appear.

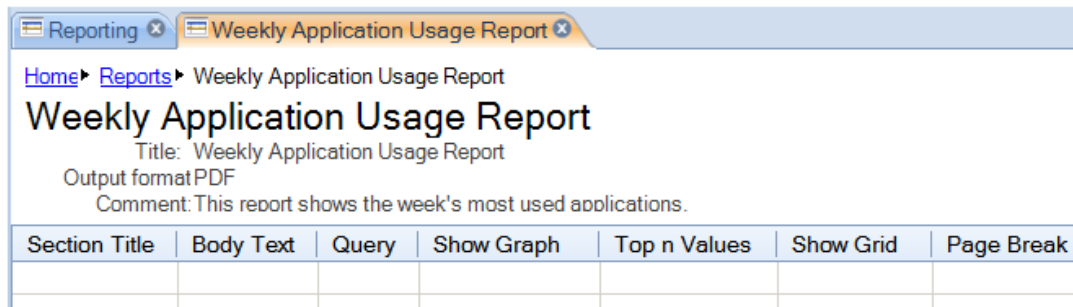
The fields in this dialog are the following:

- **Report Name** - The logical name for this report in InControl.
- **Report Title** - The title of the report which is shown on the report's first page.
- **Comment** - An optional note for the administrator to describe the report in more detail.
- **Output Format** - Either *PDF* or *HTML*.
- **Available to everyone** - Determines if this object will be a shareable library object. See *Chapter 19, The Library Browser* for more about sharing library objects.

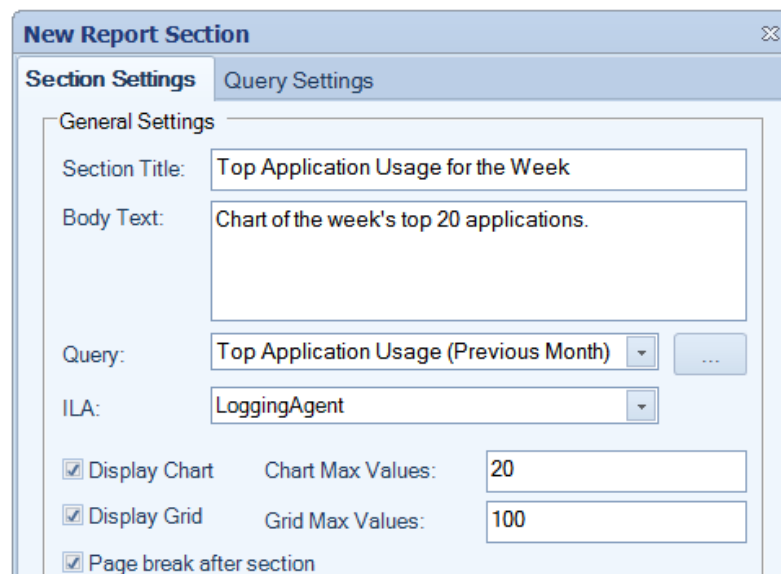
Selecting **OK** in the dialog will save the report to the report list along with the predefined reports. A new report is empty and needs to have one or more sections added to it before it has any meaning. Adding sections is described next.

Adding Report Sections

To add or edit the contents of a report, select the report from the report list. This will open a new tab for the individual report in the InControl client interface.



To add a new section to the report, select *Add*. This will open the following dialog.



The individual fields in this dialog are as follows:

- **Section title** - The title of the section which will appear at the head of the section in bold.
- **Body text** - A short description which will appear in the report after the section title.
- **Query** - Select the log analyzer query. This can be one of the predefined queries or a user defined query.
- **ILA** - The logging agent which is receiving the logs being analyzed.
- **Display chart** - Enable this option if the query data is to be presented as a chart.
- **Chart max values** - Limits the number of values in the chart. Too many values makes it hard to read.
- **Display grid** - Enable this option if the query data is to be shown as a table.
- **Grid max values** - Limits the number of rows displayed in the table.
- **Page break after section** - Enable this to insert a page break after a section in the PDF.

The same dialog also includes fields which allow the size and image types of a chart to be changed. The default chart values are shown below.

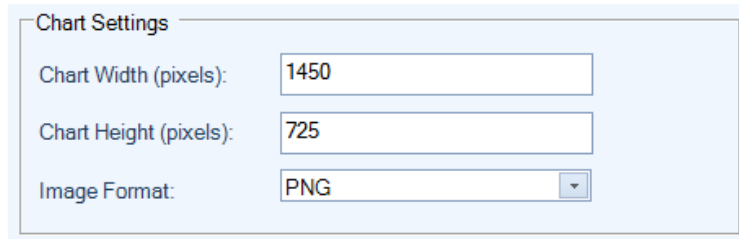


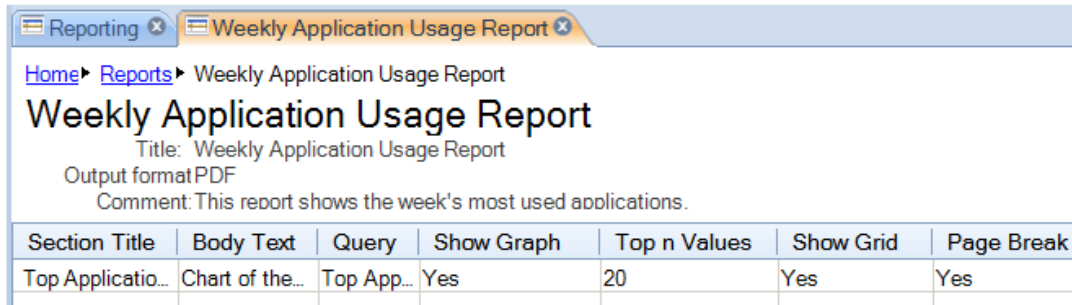
Chart Settings

Chart Width (pixels): 1450

Chart Height (pixels): 725

Image Format: PNG

When all the values in the dialog are satisfactory, select *OK* to save the section so it becomes part of the report.



Reporting Weekly Application Usage Report

Home Reports Weekly Application Usage Report

Weekly Application Usage Report

Title: Weekly Application Usage Report

Output format PDF

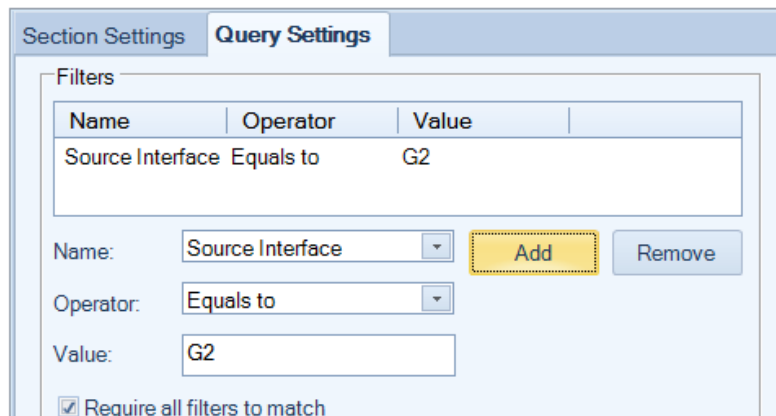
Comment: This report shows the week's most used applications.

Section Title	Body Text	Query	Show Graph	Top n Values	Show Grid	Page Break
Top Application...	Chart of the...	Top App...	Yes	20	Yes	Yes

When the report has all its sections added, it can be generated just like a predefined report by selecting *Generate Report*, as described earlier.

Adjusting the Query Settings

The above dialog has a tab called *Query Settings*. Using this is optional. It allows the query to be refined further so it only applies to traffic that meets specific criteria, such as a specific cOS Core source interface. If the report was only going to apply to the G2 interface of the Clavister Security Gateway then the settings would be as shown below.



Section Settings Query Settings

Filters

Name	Operator	Value
Source Interface	Equals to	G2

Name: Source Interface Add Remove

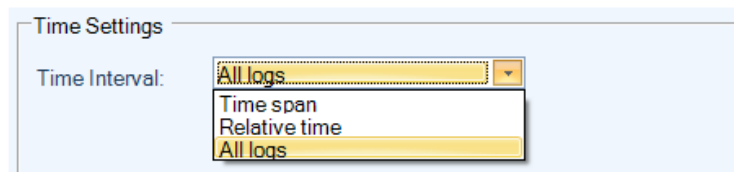
Operator: Equals to

Value: G2

☒ Require all filters to match

Several filters can be added and if the setting "*Require all filters to match*" is enabled all conditions filters must trigger for the data to be included in the report. If this option is not enabled then only any one filter needs to match.

The *Query Settings* tab also allows adjustment to the time criteria of the report. The options are available through a dropdown menu as shown below:

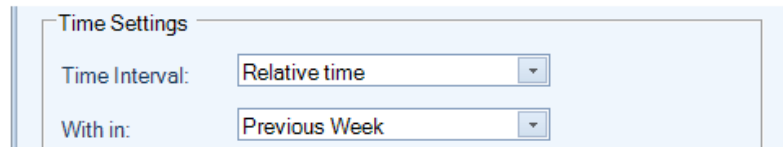


Time Settings

Time Interval: All logs

- All logs
- Time span
- Relative time
- All logs

The default is relative time.

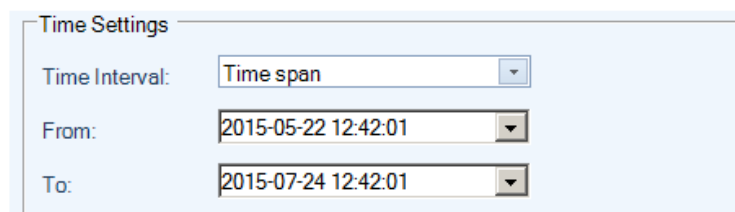


Time Settings

Time Interval: Relative time

With in: Previous Week

Alternately, a specific time interval can be specified.



Time Settings

Time Interval: Time span

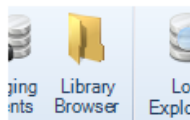
From: 2015-05-22 12:42:01

To: 2015-07-24 12:42:01

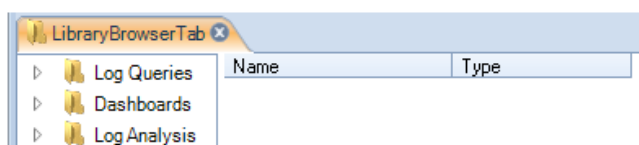
Chapter 19: The Library Browser

The *Library Browser* provides a means to view, manage and select InControl objects that have previously defined and saved in the InControl server database. These objects might be a dashboard or an ILA server query and can be quickly opened to display the relevant information.

The library browser is opened by pressing its button in the *Home* tab.



This opens the browser tab and on the left-hand side is navigation tree for the contents of the library.



The top level navigation tree folders show the types of objects that can be stored in the server database library. Objects can be stored directly under their respective folders and can be further subdivided into subfolders

The library types are as follows:

- **Log Queries**

These are saved queries for the *Log Explorer* that are described in *Section 18.3, "The Log Explorer"*. These same saved queries are also accessible by pressing the lower half of the *Log Query* button in the *Home* toolbar ribbon.

- **Dashboards**

These are the saved dashboard queries described in *Chapter 17, Real-time Monitoring*. These same saved queries are also accessible by pressing the lower half of the *Monitoring Dashboards* button in the *Home* toolbar ribbon.

- **Log Analysis**

These are the saved statistics queries that are described in *Section 18.6, "The Log Analyzer"*. These same saved queries are also accessible by pressing the lower half of the *Log Analyzer*

button in the *Home* toolbar ribbon.

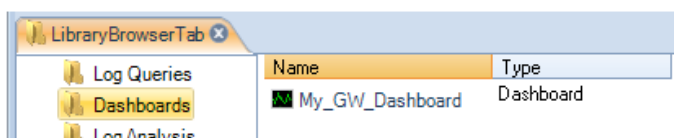
- **Reports**

These are the InControl reports that can be created in PDF or HTML format and are described in *Section 18.7, "InControl Reporting"*. All saved reports can be viewed by selecting the *Reports* button in the *Home* toolbar ribbon.

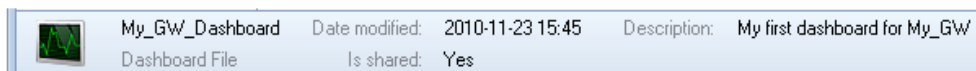
Library Object Information

When an object is selected and opened, the relevant information will be displayed. For example, opening a dashboard will cause the dashboard to become "live" and the information defined in it to be displayed.

For example, a dashboard may have been created and saved with the name *My_GW_Dashboard*. If the *Dashboards* entry in the navigation tree is selected, the dashboard appears in the table display of available dashboards.

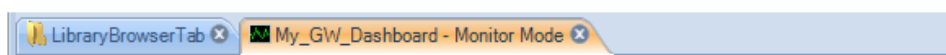


If the dashboard is selected, information about the dashboard appears at the bottom of the library tab.



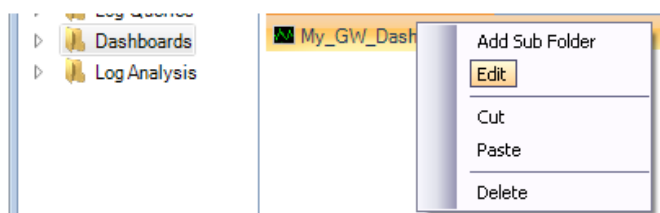
Activating Library Objects

Activating a library object is done by double clicking it. If the dashboard in the example above is now double clicked, it will be activated and the "live" dashboard will appear in a *Monitor Mode* tab.



Object Options

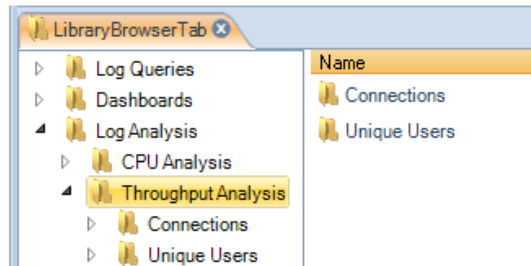
Right clicking a library item will bring up a context menu with options to cut, paste, delete and edit the item plus the ability to create a subfolder.



These same functions are also provided in the toolbar.

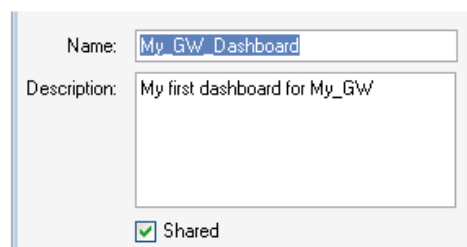


The *New Folder* option is used to create subfolders in the library. These provide a way up dividing up large numbers of objects into more manageable groups. There are no restrictions on the depth of nested folders. An example of subfolder usage with the *Log Analyzer* is shown below.



Editing Properties

Choosing the *Edit* option will display a dialog that allows the properties of the library object to be changed.



The *Shared* Option

The *Shared* option in the *Edit* dialog is enabled by default. This means that the library object is visible to any other client accessing the InControl server database and also that it can be edited by any other client.

If the *Shared* option is disabled then that client can be seen only by the InControl user that saved the object. It will not be visible to any other user and will therefore also cannot be activated or edited either.

Chapter 20: High Availability

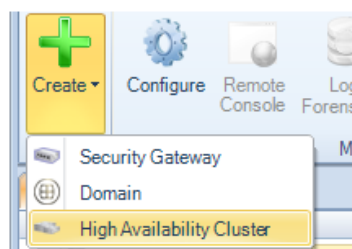
cOS Core *High Availability* allows two Clavister Security Gateways, a *master* and a *slave unit*, to operate as a single security gateway in an *HA cluster*. If the master unit ceases to function, the slave will detect this and a *fail over* occurs in which the slave takes over the master's functions.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

An HA cluster can easily be set up and managed through InControl. This chapter describes how this is done.

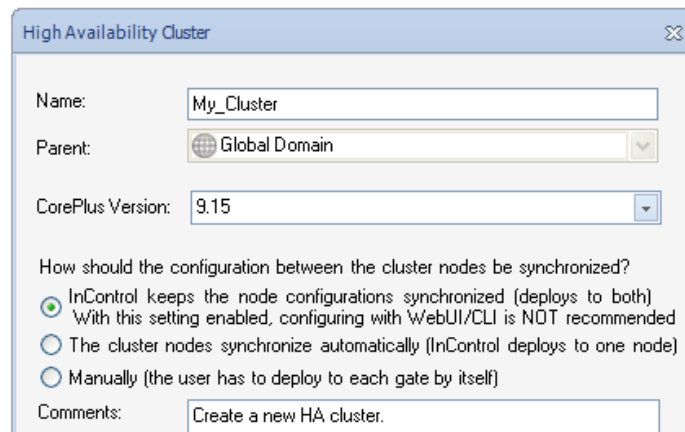
Creating a New HA Cluster

An *High Availability Cluster* is defined as a node in the navigation tree of the InControl *Security Gateways* tab.

To create a new HA cluster node, press the *Create* button in the *Security Gateways* tab toolbar and select the *High Availability Cluster* option.



The *HA Cluster* wizard will start to define the cluster. The step in the wizard is to define the cluster name and method of deploying configurations to the cluster can be set.



High Availability Cluster

Name:

Parent:

CorePlus Version:

How should the configuration between the cluster nodes be synchronized?

☒ InControl keeps the node configurations synchronized (deploys to both)
 With this setting enabled, configuring with WebUI/CLI is NOT recommended

☐ The cluster nodes synchronize automatically (InControl deploys to one node)

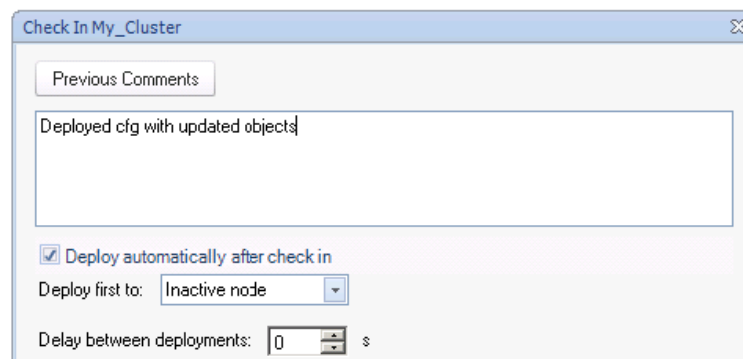
☐ Manually (the user has to deploy to each gate by itself)

Comments:

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, InControl asks which gateway should be deployed to first using the dialog below.



Check In My_Cluster

☒ Deploy automatically after check in

Deploy first to:

Delay between deployments: s

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 in order for 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.

Adding Gateways to the Cluster

Once the HA cluster object is created, two types of security gateways can be added to the cluster:

- **Add an existing gateway**

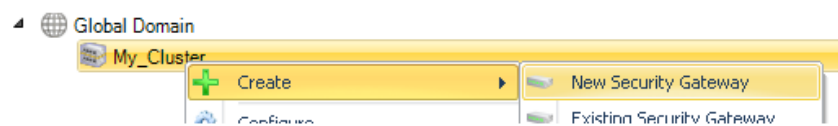
Adding a gateway that is already defined to InControl can be done in one of two ways:

- In the *Security Gateways* navigation tree, drag the gateway's node with the mouse and drop it into the cluster node.
- Right click the cluster node and select the *Existing Security Gateway* option within the *Create* submenu.



- **Define a new gateway**

If the gateway is not yet defined to InControl, it can be defined at the same time it is added to a cluster by right clicking the cluster node and selecting the *New Security Gateway* option.



This starts the new gateway wizard with the cluster set to be the parent.

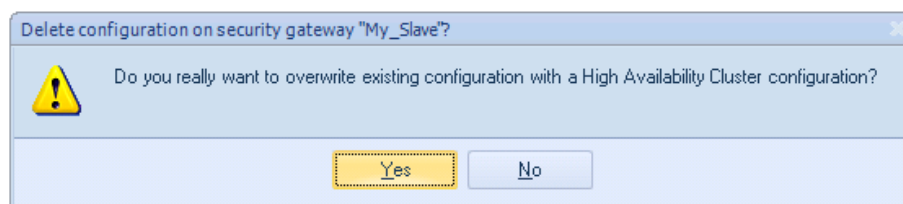
 A screenshot of a 'Security Gateway' configuration dialog box. It has two input fields: 'Name' with the text 'My_Slave' and 'Parent' with a dropdown menu showing 'My_Cluster'.

Selecting the Master and Slave

Although the two security gateway in an HA cluster are peers, cOS Core 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 by default and the second added becomes the *slave*.

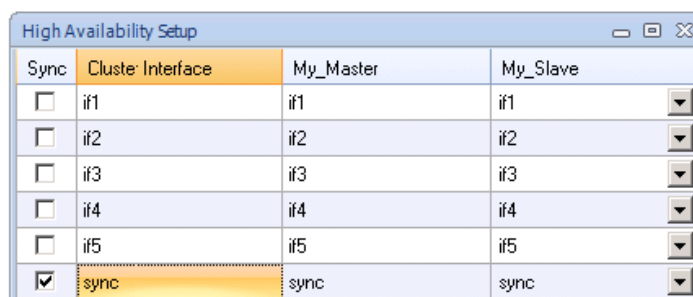
The Slave Configuration is Overwritten

When adding the slave gateway to a cluster, its configuration is automatically overwritten with the master configuration on deployment. InControl displays a warning message so that this is understood.



Selecting the Sync Interface

Whenever a second security gateway is added to an HA cluster, the wizard asks the administrator to select the *sync* interface. An example of this dialog is shown below.



The *Sync* interface on the master and slave in an HA cluster are used to synchronize the two Clavister Security Gateways. Only one pair of interfaces is chosen to be *Sync*. The *cOS Core 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.

Some clusters may have been created outside of InControl but it is desirable to bring them under InControl control. To add an existing cluster, there are two methods:

- **Create a Cluster Node First**

First create a new *HA Cluster* node in the *Security Gateways* tab. Then add the two cluster peers one by one to this cluster as though they were individual gateways.

The order is important! Add the cluster master first since the first added will always become the master in InControl.

- **Create the Gateway Nodes First**

Instead of adding a new cluster object first, add the cluster master as new gateway objects in the *Security Gateways* tab. When this is done, InControl detects that the unit is already part of a cluster and displays a dialog to ask what should be done with it. The options are:

1. Create a new InControl cluster node and add this gateway to it. This is the selected option in the example below, where the cluster is to be called *My_Cluster*. The deployment options are also set in this dialog.
2. Select an existing cluster node as the parent. With this option, InControl displays another dialog to choose an existing cluster. The first gateway added automatically becomes the master. The second automatically becomes the slave.
3. Add as a normal gateway. This changes the cluster membership setting in the gateway's

configuration.

After Adding the Cluster

The cluster now appears under the *Global Domain* in the *Security Gateways* tab display.

Name	Address	Status	Version	Checked out by	Alarms	Comment
Global Domain						The base domain for all
My_Cluster						Create a new HA cluster

Mismatching cOS Core Versions Cause an Alert

It is recommended to always have exactly the same version of cOS Core running on both the master and slave units in a cluster. Some mismatched versions may seem to function correctly but there is always a risk for problems in allowing this.

InControl always signals such a mismatch by producing an alert with a severity of *Error* and a text message indicating that there is a difference in the versions. Such an alert is shown highlighted in the example screenshot below.

Status	Date	Severity	Source	Entity	Name
	2011-10-27 13:10:15	Informational	Management Server	SG50-27	Security Gateway(s) is using the default Manage
	2011-10-27 13:10:15	Informational	Management Server	HA-SG4200	Security Gateway(s) is using the default Manage
	2011-10-27 13:14:30	Error	Management Server	HA-SG4200	CorePlus versions on master/slave device differ.

Removing a Gateway from a Cluster

Once added to a cluster node in InControl, a gateway cannot then be changed to be a standalone gateway node in InControl. Gateways must be first deleted from the InControl cluster and then added back to InControl as a new, standalone gateway.



Important: The Sync flag should not be changed

Once a cluster is under the management of InControl, the administrator should not perform any changes on an individual security gateway that affect this management through either the Web Interface or the CLI.

*In particular, the boolean property **Sync** should not be changed. When the cluster is under InControl management, the **Sync** value on both security gateways is set to **No** and this must **NOT** be changed by using, for example, the CLI command:*

```
Device:/> set HighAvailability Sync=Yes
```

Chapter 21: Configuration Object Groups


The concept of *folders* can be used to organize groups of cOS Core objects into related collections. These work much like the folders concept found in a computer's file system. For example, a group of related address book IP objects can be put into an address book folder.

A compliment and alternative to folders for organizing objects is using *configuration object groups*. Object groups allows the administrator to gather together and color code configuration objects under a specified title text so their relationships are more easily understood when they are displayed in a cOS Core graphical user interface. Unlike folders, they do not require each folder to be opened for individual objects to become visible. Instead, all objects in all groupings are visible at once.

Object groups can be used not only for address book objects but in most cases where cOS Core objects are displayed as tables and each line represents an object instance. The most common usage of this feature is likely to be for either the cOS Core Address Book to arrange IP addresses or for organizing rules in IP rule sets.

An Object Group Example

The example below shows the InControl client display of a simple IP rule set containing just five rules.

 **IP Rule Set**
An IP Rule Set is a self-contained set of IP Rules. Default action is Drop.

Advanced Settings

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	lan-to-internet-http	NAT	lan	lannet	wan	all-nets	http
2	lan-to-internet-dns	NAT	lan	lannet	wan	all-nets	dns-all
3	lan-to-dmz	Allow	lan	lannet	dmz	dmznet	all_tcpudp
4	dmz-to-internet	Allow	dmz	dmznet	wan	all-nets	http
5	Drop-All	Drop	any	all-nets	any	all-nets	all_services

Shown below, is an example of how object groups could be applied to better display the relationships between the individual objects. One group is defined for the *lannet* related rules (green), one for the *dmznet* rules (orange) and another for the single rule that drops and logs remaining traffic (blue). Each group has an explanatory title at its head and each has a distinct color coding for its members.



Object groups are a recommended way to document the contents of cOS Core configurations.

Object groups are used in the same way in both the Web Interface and InControl. The description in this section applies to how the feature is used in either user interface. Both provide the same options for manipulating groups although there are some small layout differences.

It is important to understand that object group feature in the Web Interface or InControl is a means of organizing the visual presentation of information so that the administrator can easily see how objects are related. It does **not** collect together objects into logical groups within cOS Core.

Defining a Group

#	Name	Action
1	lan-to-internet-http	NAT
2	lan-to-internet-dns	NAT
3	Drop-all	Drop

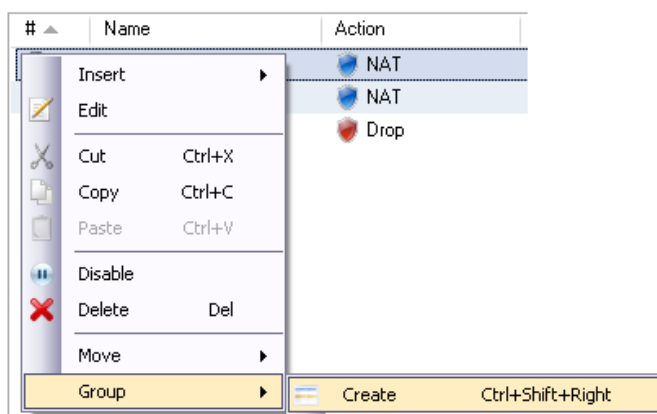


161

The images used in this example show only the first few table columns.

If it is desirable to create an object group for the two web surfing IP rules, this is done with the following steps:

- Select the first object to be in the new group by right clicking it.
- Select the **New Group** option from the context menu.



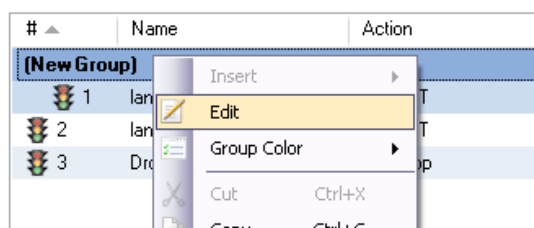
- A group is now created with a title line and the IP rule as its only member. The default title of "(new Group)" is used.

The entire group is also assigned a default color and the group member is also indented. The object inside the group retains the same index number to indicate its position in the whole table. The index is not affected by group membership. The group title line does not have or need an index number since it is only a textual label.

#	Name	Action
	(New Group)	
1	lan-to-internet-http	NAT
2	lan-to-internet-dns	NAT
3	Drop-all	Drop

Editing Group Properties

To change the properties of a group, right click the group title line and select the **Edit** option from the context menu.



A *Group* editing dialog will be displayed which allows two functions:

- **Specify the Title**

The title of the group can be any text that is required and can contain new lines as well as empty lines. There is also no requirement that the group name is unique since it is used purely as a label.

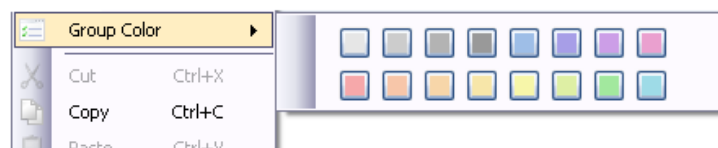
- **Change the Display Color**

Any color can be chosen for the group. The color can be selected from the 16 predefined color boxes or entered as a hexadecimal RGB value. In addition, when the hexadecimal value box is selected, a full spectrum color palette appears which allows selection by clicking any color in the box with the mouse.

In this example, we might change the name of the group to be **WebSurfing** and also change the group color to green. The resulting group display is shown below:

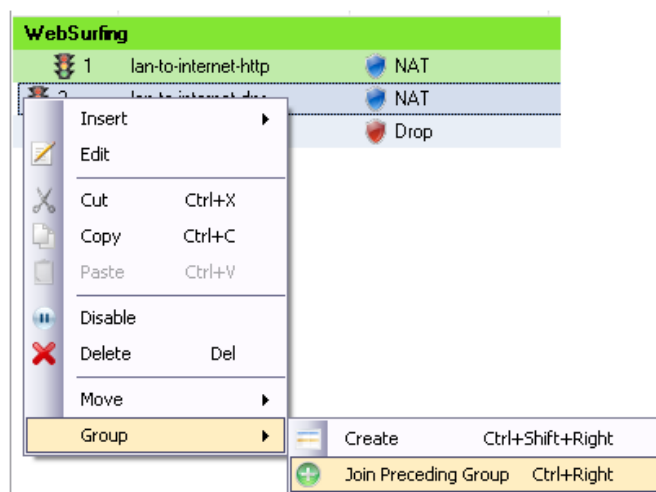
#	Name	Action
WebSurfing		
1	lan-to-internet-http	NAT
2	lan-to-internet-dns	NAT
3	Drop-all	Drop

A change to any color in the 16 color palette can also be achieved by right clicking the group title line and selecting the **Group Color** option.



Adding Additional Objects

A new group will always contain just one object. Now, it is possible to add more objects to the group. By right clicking the object that immediately follows the group, the **Join Preceding** option is selected to add it to the preceding group.



After performing a join for the second IP rule in this example, the result will be the following:

#	Name	Action
WebSurfing		
1	lan-to-internet-http	NAT
2	lan-to-internet-dns	NAT
3	Drop-all	Drop

To add any object to the group we must first position it immediately following the group and then select the **Join Preceding** option. This is explained in more detail next.

Adding Preceding Objects

If an object precedes a group or is in any position other than immediately following the group, then this is done in a multi-step process:

- Right click the object and select the **Move to** option.
- Enter the index of the position immediately following the target group.
- After the object has been moved to the new position, right click the object again and select the **Join Preceding** option.

Moving Group Objects

Once an object, such as an IP rule, is within a group, the context of move operations is within the group only. For example, right clicking a group object and selecting **Move > To Top** will move the object to the top of the group, **not** the top of the entire object list.



The other move operations of **Up**, **Down** and **To Bottom** also only move an object within the context of its group and **not**. However, the index number of a moved object will always change to reflect its new position within the entire list.

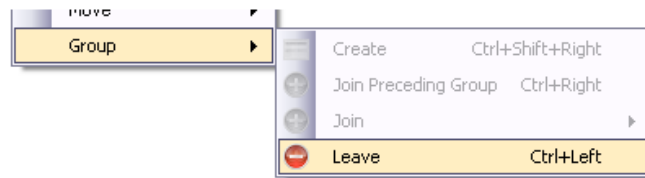
Moving Groups

Groups can be moved in the same way as individual objects. By right clicking the group title line, the context menu appears and includes the full set of **Move** options. For example, selecting the **Move > To Top** option for the group title, moves the entire group to the top of the object list.

Moving a group, moves all its members at the same time and results in all objects in the entire list being assigned a new index number.

Leaving a Group

A single object can be removed from a group by right-clicking it and selecting **Group > Leave** from the context menu.



If the object is not the last object in the group, leaving the group has the additional effect of moving the object down to a position immediately following the group. This is done because all objects in a group must appear consecutively in the object list.

Removing a Group

A group automatically disappears when it has no members left. If a group has just one member left and that member is removed from the group, the group disappears. If a group has a large number of objects then the group can be removed by selecting all of its member objects and choosing the **Group > Leave** option from the context menu.

When a group is removed, the group title line and color coding disappears. Individual object index positions within the table are not affected when a group is removed.

Groups Cannot Contain Folders

It is important to distinguish between collecting together objects using a *folder* and collecting it together using groups.

Either can be used to group objects but a folder is similar to the concept of a folder in a computer's file system. However, a folder cannot be part of a group. Groups collect together related basic objects and a folder is not of this type. It is possible, on the other hand, to use groups within a folder.

It is up to the administrator how to best use these features to best arrange cOS Core objects.

Chapter 22: Troubleshooting Connections

If there are initial problems with communication between a 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. This will only work if an IP rule has already been defined on the gateway that allows ICMP.
- 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 <if-name>
```

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 behavior, 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
```

Chapter 23: MFA Server Administration

- Overview, page 168
- Installation, page 171
- Configuration Objects, page 175
- Scenarios, page 181
- Supported Clients, page 185
- Self Service Portal, page 186
- The Authenticator App, page 188
- System Folders, page 189
- Logging, page 190

23.1. Overview

Multi Factor Authentication

cOS Core supports a feature called *Multi Factor Authentication* (MFA). With MFA (also known as *2-factor authentication* or *2-step authentication*), a RADIUS server can require additional authentication from an external client, in addition to standard credentials such as username/password.

This additional authentication often consists of a single code (sometimes referred to as a *one time password* or OTP). The extra code can be provided to the client by various means, such as the RADIUS server sending an SMS to a mobile device or the client generating the code locally with a mobile app.

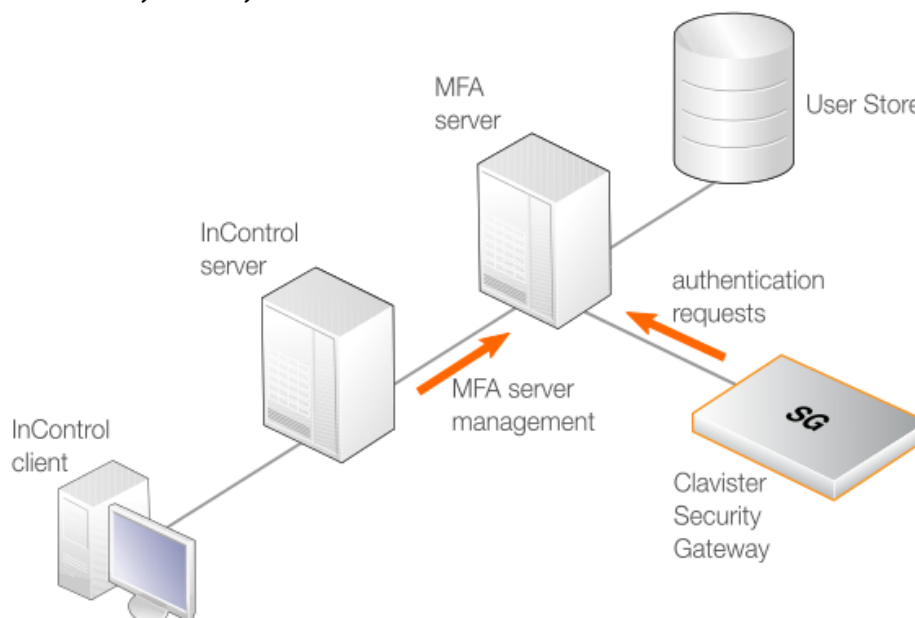
The Clavister MFA Server

Support for multi factor authentication already exists as standard within cOS Core and requires no setup by the administrator. However, Clavister offers its own proprietary RADIUS server implementation to perform multi factor authentication.

This separate software product is called the *Clavister Multi Factor Authentication Server* (Clavister

MFA Server) and it can run on an external computer under the Windows operating system. Administration of the Clavister MFA Server software is performed via the InControl client interface and this chapter describes both the installation and operation of the Clavister MFA Server as well as how it is administered using InControl.

The relationships between Clavister InControl and the Clavister MFA Server product and a Clavister Security Gateway is illustrated below.



Note that the *User Store* in the above diagram is a database which stores all the user credentials. This function is not performed by the Clavister MFA Server product but user store access must be specified for the MFA Server. This is discussed further in *Section 23.3.3, "User Store Object Configuration"*.

Supported OTP Delivery Methods

The Clavister MFA Server product supports the following methods of OTP (one-time password) delivery:

- **SMS**

This requires the MFA Server to be connected to the Internet and that the client's mobile number is available to the MFA Server.

- **Clavister Authenticator App**

The Clavister Authenticator App runs on Android and iOS devices. It can provide OTP codes when they are required.

Supported Client Types

In combination with the MFA Server product, cOS Core supports authentication using any of the following types of software clients:

- The native IPsec IKEv1 client in OS X.
- Third party IPsec IKEv1 clients running under Windows (for example, NCP).
- The native IKEv2 client in OS X and Windows.

- Native L2TP Clients running under OS X or Windows.

Any special steps required for setup with these clients are described in *Section 23.5, "Supported Clients"*.

The MFA Server Authentication Sequence

The usual sequence of events for MFA Server authentication is as follows:

1. The client tries to access protected resources via a Clavister Security Gateway.
2. cOS Core asks for authentication credentials and the client enters a username and password.
3. cOS Core sends the client's username/password credentials to the MFA Server for authentication.
4. The MFA Server can be configured to respond like a standard RADIUS server and authenticate the client without a further challenge. However, if multi factor authentication is configured, the server sends back a request for an additional challenge and this request is then relayed by cOS Core to the client.
5. The client responds to the additional challenge. Usually this will be in the form of a code. A code may be obtained in one of the following ways:
 - i. The MFA Server sends a code to the client. This might be, for example, via SMS.
 - ii. The client is able to supply the response to the challenge independently. This might be by using, for example, the Clavister Authenticator App.
6. cOS Core forwards the client's response to the MFA Server.
7. The MFA Server checks the client's response and sends a RADIUS *ACCEPT* message to cOS Core if the client is authenticated. A *REJECT* message is sent if it is not authenticated.
8. cOS Core allows the client connection if it is authenticated.

Configuring cOS Core

When configuring the usage of the Clavister MFA Server in cOS Core, it is configured like a normal *RADIUS Server* object then an *Authentication Rule* is configured that references that *RADIUS Server*. Configuring these cOS Core objects is discussed further in the authentication section of the separate *cOS Core Administration Guide*.



Important: The cOS Core PPP Agent Options must be PAP only

With the Clavister MFA Server, only the **PAP** option should be enabled from the list of **PPP Agent Options** when configuring the **Authentication Rule** in cOS Core.

The User Store

The Clavister MFA Server does not store the user credential information itself. Instead, it makes use of a *user store*. The user store is a Microsoft Active Directory™ server. Configuring which user store to use is part of Clavister MFA Server setup.

23.2. Installation

This section describes the installation of the MFA Server software.

Minimum Hardware Requirements

The following are the minimum resource requirements for the MFA Server software, and these are the same regardless of the underlying platform:

- 64 bit processor.
- Minimum of 5 Gbytes of disk space.
- Minimum of 2 Gbytes of RAM for up to 10,000 clients.
- Minimum of 4 Gbytes of RAM for up to 100,000 clients.
- Contact Clavister for RAM requirements with higher client numbers.

The Clavister MFA Server software is not a CPU intensive product and a single CPU should be adequate in most scenarios.

Ports Used for Communications

Regardless of the platform, the following communication ports will be used as defaults by the MFA Server for incoming and outgoing traffic and so these ports should not be blocked by firewall software:

Usage	Type	Port	Direction
InControl server / Self service server	TCP	8443 (default)	Incoming
RADIUS queries	UDP	1812	Incoming
LDAP queries	TCP	389 / 636	Outgoing

23.2.1. Windows Installation

Installation of the MFA Server product on a Windows system is done by running an .exe installation file which takes the administrator through an installation wizard. This installation process is completely separate from installing InControl and uses its own .exe file.

The installation steps for Windows are as follows:

- Download the installation .exe file from the Clavister website.
- Double-click the .exe file to start the installation wizard.
- On the **Welcome** step, click *Next*.
- On the **License Agreement** step, read the agreement and select *I accept*, then click *Next*.
- On the **Select License File** step, click *Browse...* to locate and select the license file for the product, then click *Next*. This assumes that the license has already been downloaded from the Clavister website to the local disk. License downloading is described in *Section 23.2.2, "License Installation"*.

Note that if the license file is out of date or missing then the MFA Server will not start.

However, the license can be installed manually into the MFA Server's *License* folder later.

- On the **Select Destination Directory** step, click *Browse...* to select installation location or accept the default destination directory, then click *Next*.
- Enter the username and password for management access. The installer will provide a default username but this can be changed. A password must be entered.

This username/password combination is repeated as properties of the *MFA Server* object which is created in InControl for this MFA Server installation.

- On the **HTTP port** step, enter the port for administration connection. This does not usually need to be changed from the default value of 8443, unless this port number is used for another purpose.

This same port number is repeated as a property of the *MFA Server* object which is created in InControl for this MFA Server installation.

- The software will be installed. Click *Finish* to close the wizard.

Starting the MFA Server Under Windows

The MFA Server can be run under Windows in either of the following ways:

- **As a Service**

This is done by locating the MFA Server service and setting its mode to *Automatic* and then starting the service.

- **As an Application**

In a Windows console, run the *Clavister MFA Server* file which is found in the MFA system's *bin* folder (for example, in *C:\Program Files\Clavister\MFA\bin* with a typical installation).

Note that if the server is started in this way, the option *Run as Administrator* **must** be chosen, otherwise the server will not start.

Checking for Startup Problems

Once the server is running, it will appear in the Windows task manager process list as *Clavister MFA Server.exe*. The *server.log* and *event.log* files can be checked to make sure there were no startup issues.

23.2.2. License Installation

In order to run, the Clavister MFA Server product requires a license file to be installed on the server in the folder called *license*. This license file is completely separate from the license files required for InControl and cOS Core. The file must be first downloaded from the Clavister website to a local computer disk and then installed in one of two ways:

- When running the Windows installation wizard, the license file can be selected in one of the installation steps.
- The license can be manually installed by placing the file in the MFA Server's *license* folder.

License File Download

The following steps are required for downloading a license:

- Buy an *MFA Voucher* from a Clavister reseller. The voucher cost will depend on the maximum number of users that can be concurrently authenticated by the MFA Server.
- Go to the Clavister website, select the *Login* option and log in to the *My Clavister* part of the website. Registering as a user may be required first for this step if registration has not been done before.
- Select *Multi Factor Authentication* and enter the MFA voucher code.
- After the code is accepted, the licensed number of users will appear in the *Named Users* field.
- The license download option can now be selected and the license file downloaded to the local disk. The license download option is disabled if the *Named Users* value is zero.
- Copy the license file to the *licenses* folder of the MFA Server installation. Alternatively, select the file in the relevant step when running the Windows installation wizard if the MFA Server software has not yet been installed.

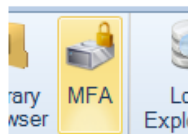
License Expiry Behavior

If an installed MFA Server license expires during operation, the server software will stop running and cannot be restarted until a valid license is installed into the *license* folder.

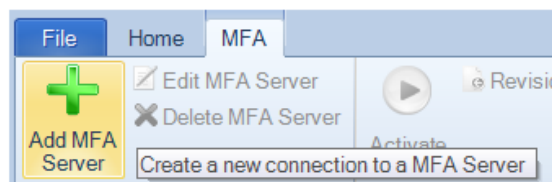
23.2.3. Adding to InControl

Once the MFA Server is running, it must be added to InControl so that it can be managed using InControl. Use the following steps to do this:

- Open the InControl client and press the *MFA* button.

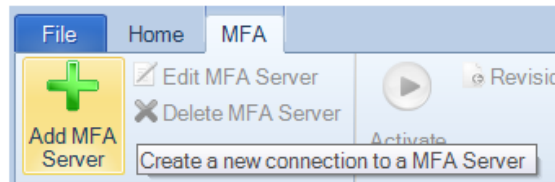


- Open the InControl client and press the *Add MFA Server* button.

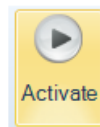


- The dialog to add/edit the MFA server is now displayed. The default IPv4 address of *localhost* indicates that the MFA Server is on the same computer as the InControl server. The

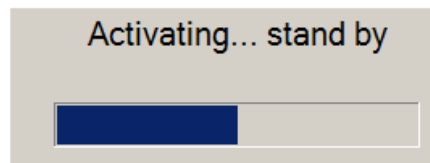
username/password pair must match the pair specified when running the MFA Server installation wizard.



- After closing the dialog, an *MFA Server* object is created in InControl with a default (empty) configuration but this may not match the configuration on the MFA Server itself. To synchronize the two, press the *Activate* button. This will overwrite the MFA Server's current configuration with the InControl configuration.



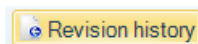
- A dialog will be displayed to show the activation is in progress.



- Following activation, further changes can be made to the MFA Server configuration, such as adding a *Scenario* object. All later changes must also be activated in order to deploy them to the MFA Server.

23.2.4. The Revision History

Starting from the time that an MFA Server is added to InControl, all subsequent changes made to the server in InControl are added to a *Revision History* at the time they are activated. The revision history can be viewed by pressing the *Revision History* button.



The revision history shows a chronology of all changes made to an MFA Server.

MFA: Configuration		MFA Revision History		
Date and Time (UTC)	Date and Time (local)	Revision	Username	Comment
2016-08-01 07:01:19	2016-08-01 09:01:19	1	admin	Checked in new configuration

It is possible to roll back the current MFA Server configuration to any entry in the history by double clicking that entry.

23.3. Configuration Objects

23.3.1. Overview

This section describes the objects that need to be created when setting up authentication with the InControl interface. Setting up authentication involves two steps:

- Create an *MFA Server* object. Each of these objects corresponds to a single installation of the MFA Server.

Note that InControl version 1.60 allows only a single instance of this object and the server software must be installed on the same computer as the InControl server.

- Under the *MFA Server* object, create one or more child *Scenario* objects which define the authentication to be performed and the LDAP source to be used. A *Scenario* object will require the usage of various other object types which must also be created under the *MFA Server* object.

The various objects to be created under an *MFA Server* object are displayed in the InControl interface.



All of these object types are described next:

- **Scenario**

One or more *Scenario* objects can be added to InControl. Each *Scenario* describes a set of authentication parameters used by a set of external authenticating clients. This object is the key building block for enabling authentication and uses many of the other objects described in this section. Configuring the *Scenario* object itself is described in Section 23.4, “Scenarios”.

- **User Store**

Each *Scenario* object requires a *User Store* object which specifies the user database source.

- **RADIUS Server**

Each *Scenario* object requires a *RADIUS Server* object. This defines the behavior of the MFA Server and specifies the IPv4 address and port number which the MFA Server will use to listen for incoming connections from cOS Core.

- **RADIUS Client**

Each *Scenario* object requires a *RADIUS Client* object. This defines the interface IPv4 address and shared secret of the connecting cOS Core client.

- **Self Service**

Using the Clavister *Self Service Portal* allows a user to themselves enable multi factor authentication and manage some aspects of the authentication process. By default, there is always one predefined *Self Service* object that is disabled. This predefined object must be enabled to switch on the feature.

Note that the *Self Service* object type is standalone and is not used in conjunction with the other object types listed above.

Setting up the above object types and then setting up the supported *Scenario* types is discussed next.

23.3.2. MFA Server Object Configuration

An *MFA Server* object is created as the parent object for all other configuration objects involved in configuring authentication. Each *MFA Server* object corresponds to a single installation of the Clavister MFA Server software.

Listed below are the properties of an *MFA Server* object:

- **Name**

A descriptive name for the server which is used only for display in the InControl interface.

- **Address**

The IPv4 address of the server for the management connection.

With InControl version 1.60, this value is set as *localhost* and cannot be changed. This means that the MFA Server must be installed on the same computer as the InControl server.

- **Port**

The port number on the MFA Server to use for management connections. This is usually the default value of 8443 but can change if a different value was specified during MFA Server installation.

- **Username**

This is the username specified during MFA Server installation and will be used by InControl for management connection.

- **Password**

This is the password specified during MFA Server installation and will be used by InControl for management connection.

23.3.3. User Store Object Configuration

The *User Store* object defines an LDAP server that holds a database of valid users with their username/password credentials. The properties of a *User Store* object are the following:

- **Name**

A logical name that will be used only in the InControl interface.

- **Host**

The IPv4 address of the LDAP server.

- **Port**

The port number for access to the LDAP server.

- **TLS**

By default, connection to the user store utilizes a standard LDAP connection. Enabling this option means the connection uses the more secure LDAPS.

- **Trust All**

If the previous option *TLS* is enabled, this option can also be enabled so all certificates are trusted.

- **User DN**

The user domain name. For example:

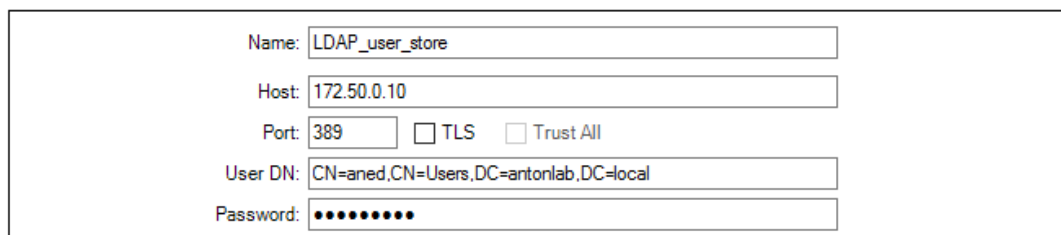
```
cn=administrators,cn=users,dc=example,dc=com
```

This must be specify a user with the access right to perform the search. It cannot specify a container.

- **Password**

The password for LDAP server access.

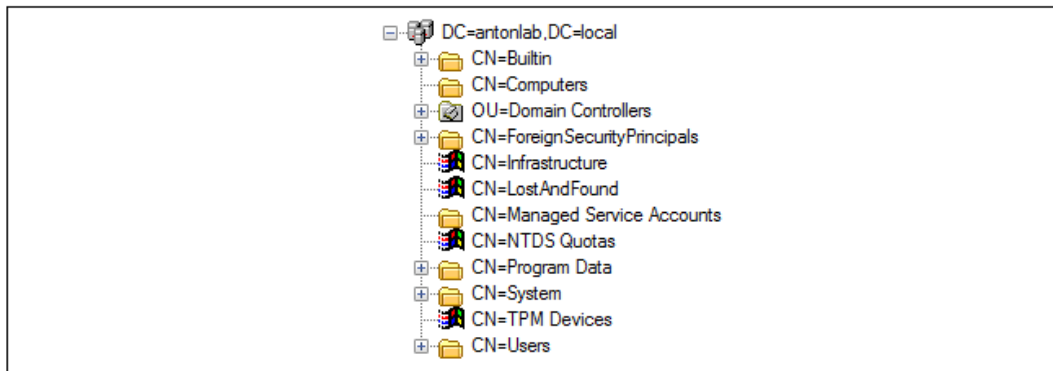
Below is a screenshot from InControl which shows configuring a *User Store* object.



The screenshot shows a configuration form for a User Store object. The fields are as follows:

- Name:** LDAP_user_store
- Host:** 172.50.0.10
- Port:** 389
- TLS:** ☐ (unchecked)
- Trust All:** ☐ (unchecked)
- User DN:** CN=aned,CN=Users,DC=antonlab,DC=local
- Password:** [Masked with dots]

Below is a screenshot of the Windows Active Directory browser which shows the corresponding LDAP directory structure.



23.3.4. RADIUS Server Object Configuration

A *RADIUS Server* object defines the IP address/port for access by a Clavister Security Gateway. Within an *MFA Server* object there can be multiple *Scenario* objects and each of these can use a different *RADIUS Server* object which specifies different IP address/port access.

- **Name**

A logical name for the object which is just used for display within InControl.

- **Address**

The IPv4 address for client access.

- **Port**

The port number for client access.

23.3.5. RADIUS Client Object Configuration

The *RADIUS* client object defines the properties of authenticating clients and it is used by *Scenario* objects. The properties of a *RADIUS Client* object are the following:

- **Name**

A logical name for this object that is just used for display in the InControl interface.

- **Address**

The IP address of the connecting client. Normally, the client will be a Clavister Security Gateway. It is mandatory to specify a single IPv4 address.

- **Secret**

The shared secret that is used by the connecting client.

In order for the connection from the InControl to succeed there must be a corresponding *RADIUS Server* object configured in cOS Core which connects to the IP address/port specified by the associated scenario's *RADIUS server* object.

Below is a screenshot from InControl which shows configuring a *RADIUS client* object.

RADIUS Client
IP Addresses of the SGW authentication source.

Name:

Address:

Secret:

23.3.6. Self Service Object Configuration

The *Clavister Self Service Portal* allows authenticating users to have the ability to manage certain aspects of their authentication, including enabling or disabling multi factor authentication. There can only be one *Self Service* object and this is already predefined and this is also disabled by default. The self service portal software is installed along with the standard MFA Server installation.

When the predefined *Self Service* object is enabled, it means that a user can connect to it via the IP address of the InControl server (this is the same IP address that InControl clients use when connecting). If the InControl server IP address is a protected private IP, a SAT translation from a public IP address may have to be done by some other device (such as a Clavister Security Gateway).

How the end user utilizes the self service portal is described separately in *Section 23.6, "Self Service Portal"*.

The *Self Service* object has the following properties:

- **Enable Self Service**

This option switches on the self service option.

- **User Store**

This is the LDAP server where the users can be found. This must specify a container which either contains the users or has the users as its children. Typical this is specified as the root of the domain, for example:

```
dc=example,dc=com
```

- **Base DN**

This is the base DN and describes where to start search for users on the LDAP Server.

Below is a screenshot from InControl which shows configuring a *Self Service* object.

Self Service
Configuration of the MFA Self Service portal

☒ Enable Self Service

User Store:

Base DN:

This dialog will also display a URL which can be used for connection to the portal by users. If the MFA Server is local (on the same computer when the dialog is displayed) this will default to:

```
https://localhost:8443/otpenrollment/
```

.

Logging in to and utilizing the self service portal is described in *Section 23.6, "Self Service Portal"*.

23.4. Scenarios

23.4.1. Adding a Scenario

A *Scenario* object needs to be configured so that authentication becomes active. There are three scenario types:

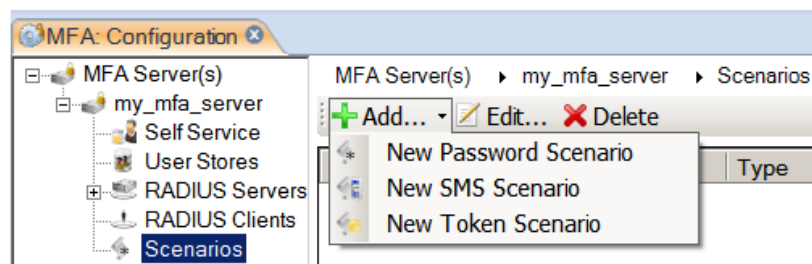
- **Password Scenario.**
- **SMS Scenario.**
- **Token Scenario.**



Note

The word **Token** refers to OTPs generated by the Clavister Authenticator App.

Any one of these can be created by selecting the *Scenarios* node from the MFA navigation tree and then choosing the *Add* option.



The configuration of each of these scenario types will be discussed in the sections that follow.



Note: The Base DN can be used to separate scenarios

Each scenario requires that a **Base DN** property is specified. This describes where to start searching for users on the LDAP Server and it must specify a container.

This property can be used to apply a scenario only to a limited user group. For example, if the requirement is to apply a scenario only to the accounting department of an organization, the **Base DN** might be specified as the following:

```
ou=accounting,ou=departments,dc=example,dc=com
```

23.4.2. Password Scenario Configuration

This type of *Scenario* object is created when the MFA Server is to be used like a conventional RADIUS server. Only username/password credentials are used for authentication and there is no extra factor.

The properties that are entered for this are the following:

- **Name**

A logical name for this scenario object.

- **User Store**

The previously defined *User Store* object that will be used with this scenario.

- **RADIUS Server**

The previously defined *RADIUS Server* object that will be used with this scenario.

- **RADIUS Client**

The previously defined *RADIUS Client* object that will be used with this scenario.

- **Base DN**

This is the base DN and describes where to start searching for users on the LDAP Server. It must specify a container.

23.4.3. Token Scenario Configuration

This type of *Scenario* object is created when username/password credentials are used with an OTP that is generated by the *Clavister Authenticator App* running on an Android or iOS device. Using the app is described further in *Section 23.7, "The Authenticator App"*.

The properties that are entered for this are the following:

- **Name**

A logical name for this scenario object.

- **User Store**

The previously defined *User Store* object that will be used with this scenario.

- **RADIUS Server**

The previously defined *RADIUS Server* object that will be used with this scenario.

- **RADIUS Client**

The previously defined *RADIUS Client* object that will be used with this scenario.

- **Base DN**

This is the base DN and describes where to start searching for users on the LDAP Server. It must specify a container.

- **Combine password and OTP**

Enabling this option will concatenate the password and OTP to form the password.

This is required sometimes when the client does not support asking for the OTP in an extra step. This is described further in *Section 23.7, “The Authenticator App”*.

Below is a screenshot from InControl which shows configuring a *RADIUS client* object.

Token Scenario
A Scenario based on a Token kept by the user

Name:

User Store:

Base DN:

RADIUS Server:

RADIUS Client:

☒ Combine Password and OTP

23.4.4. SMS Scenario Configuration

This type of *Scenario* object is created when username/password credentials are used with an OTP delivered via SMS to the user.



Important: SMS scenarios require My Clavister credentials

*For this scenario to function, InControl will need to be able to automatically connect to the Clavister user database and be able to read the available SMS credit. To allow this, the **My Clavister** login credentials must be entered in the InControl **License Center**.*

The properties that are entered for this are the following:

- **Name**

A logical name for this scenario object that is just used for display in the InControl interface.

- **User Store**

The previously defined *User Store* object that will be used with this scenario.

- **RADIUS Server**

The previously defined *RADIUS Server* object that will be used with this scenario.

- **RADIUS Client**

The previously defined *RADIUS Client* object that will be used with this scenario.

- **Base DN**

This is the base DN and describes where to start searching for users on the LDAP Server. It must specify a container.

- **Length**

This is the length of the OTP

- **Valid time**

This is how long in seconds that the OTP is valid for.

- **Is Alphanumeric**

This property specifies if the OTP is alphanumeric.

SMS messages are generated by the Clavister server network and this requires *SMS credits* to be added to the user account. Doing this is described next in *Section 23.4.5, "SMS Credits"*.

23.4.5. SMS Credits

The scenario described in Section 23.4.4, "SMS Scenario Configuration" requires SMS messages sent via the Clavister server network. This requires that a positive balance of *SMS credits* exist for the Clavister user account to which the MFA Server license is linked.



Note: SMS credits are shared across multiple servers

The user account SMS credit balance is shared across all MFA Server installations that are licensed to that user account.

Getting a positive SMS credit balance is achieved with the following steps:

- Buy an MFA *SMS Voucher* from your Clavister reseller.
- Go to the Clavister website and choose the *Login* option and log in as a customer.
- Go to the *Multi Factor Authentication* section and the current SMS credit balance for the user account can be viewed.
- Enter the voucher details to increase the balance.

Reaching a Zero Balance

When all SMS credits are exhausted and the SMS balance reaches zero, authentication using SMS will continue to function, providing a period of time to buy additional credits.

23.5. Supported Clients

This section describes the supported client types and any specific setup steps. They are the following:

- **The native OS X IPsec IKEv1 client.**

The following setup in cOS Core is required:

- i. The IPsec tunnel needs to be configured with IKE config mode so that IP addresses are allocated from a pool.
- ii. The *Local Network* of the IPsec tunnel should be configured as *all-nets*.
- iii. A remote network does not need to be specified with this client.

- **Third party IPsec IKEv1 clients running under Windows (for example, NCP).**

- **Native L2TP Clients running under OS X or Windows.**

This client will only work with the codes generated with the Clavister Authenticator App and also only with the password and OTP combined since the clients do not allow an extra challenge.

Combining the Password with the Authenticator OTP

In some cases, such as with L2TP clients, the OTP generated by the Clavister Authenticator App must be added to the password for input. Configuring this in the MFA Server is done using the *Combine password and token as password* option in the *User Password Token Scenario* object (by default, it is disabled).

This is described further in *Section 23.7, "The Authenticator App"*.

23.6. Self Service Portal

The self service portal allows users to themselves configure authentication parameters. It is activated by configuring the predefined *Self Service* object and doing this is described in *Section 23.3.6, "Self Service Object Configuration"*.

This section describes how an end user makes use of the self service portal once it is activated. The initial usage steps are as follows:

1. Browse to the URL of the self service portal. If the browser is on the same computer as the MFA Server, the defaults to

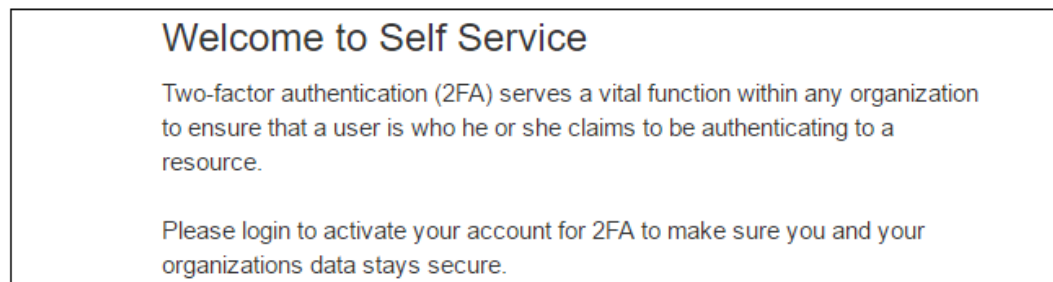
```
https://localhost:8443/otpenrollment/
```

From another computer, the URL will be:

```
https://<ip-address>:8443/otpenrollment/
```

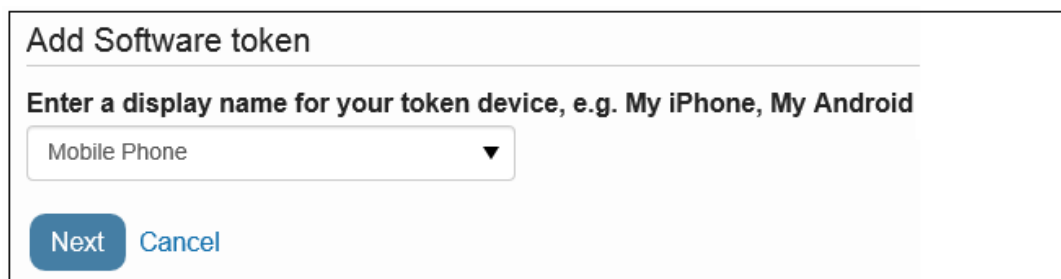
Where *<ip-address>* is the same IP address as the MFA Server uses for administrator management access.

2. Log in to the portal using the credentials which are defined in the *User Store* that has been configured in the *Self Service* object (this is described in *mfa_self_service_config*).



3. If one time passwords are to be generated by a mobile device (the *Token Scenario*) then the device needs to be associated with the portal. If passwords will be sent using email and/or SMS then this step, as well as the next, can be skipped.

Add one or more devices (such as a smartphone) that may be used with the portal and give each a logical name. Each device will need to have the *Clavister Authenticator App* installed before going to the next step. The app is described further in *Section 23.7, "The Authenticator App"*.



4. To link a device with the portal, open the *Clavister Authenticator App* and scan the QR code presented with device's camera. Alternatively, manually key in the code displayed by the portal into the app. Then, enter the one time password generated by the app into the entry box on the portal's webpage (shown at the bottom of the screenshot below).

Step 1. Add unique key to your device application.
Either scan the QR code or enter in the code provided below manually.

Step 2. When added to device you need to generate and add a One-Time Password



OR

Add code manually

1. On your mobile device, select "Manually"
2. Give the key a friendly name
3. Add key: KTOHAR5LXBZONZ7W
4. Choose type Time-based

Generate and add a One-Time Password for verification

Verify and Complete Cancel

5. Now enter an email address and telephone number. This will allow delivery of one time passwords if the relevant *Scenario* object has been configured.

E-mail

E-mail address

Enroll

SMS/Voice

Telephone number

Enroll

6. In addition, select the device (such as smartphone) which will be used for authentication with the *Token Scenario*. The choice will be from the logical names specified in step 2.

Software tokens

Token

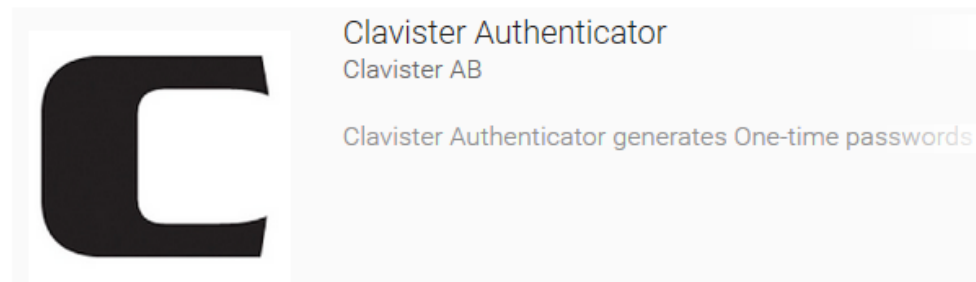
Enrolled

Add Software token

23.7. The Authenticator App

One of the means for a client to obtain the *One time code* (OTP) needed with multi factor authentication is by using the *Clavister Authenticator App* running on a mobile device. The app is used when the authentication method is controlled by a *Token Scenario* object. Configuring that *Scenario* object is described in *Section 23.4.3, "Token Scenario Configuration"*.

The app is free and can be installed on any Android or iOS based mobile device such as a smartphone or tablet. Below is the app's product image as it appears on the Google Play Store.



App Usage

The client uses the Clavister Authenticator App with the following steps:

- Download and install the app on a suitable Android or iOS device.
- Start the app for the first time and link the app to a Clavister MFA Server installation by using the *Self Service Portal*. This is done by either entering a code given by the portal or use the device's camera to scan a QR code on the portal's webpage.

Using the self service portal is described in *Section 23.6, "Self Service Portal"*.

- Once linked to the Clavister MFA Server software, the app can be used at any time to generate an OTP that can be entered during the multi factor authentication process.

Combining Password and App Generated OTP

When using the Clavister MFA Server, the OTP code generated by the app can be entered either on its own as a final challenge or concatenated on the end of the password with clients that do not support an additional challenge. The method that the MFA Server expects is configured by enabling or disabling the *Combine password and token as password* option in the *User Password Token Scenario* object (by default, it is disabled).

For example, if the user's password is *mysecretpassword* and the authenticator app generated code is *1234*, then the combined password would be *mysecretpassword1234*.

The reason why this combination is needed is that some clients, such as the Windows's native L2TP client, do not support entering the OTP as an extra challenge.

23.8. System Folders

The following are a list of the folders in the MFA Server installation directory and their purpose:

- **bin** – Contains startup scripts and configuration files for customizing system operation. This is done by changing settings in the *.vmoptions* files. Please consult Clavister support before changing anything in any of these files.
- **config** – Contains configuration files. These consist of the following:
 - i. *boot.json* is the main bootstrap file. It contains the bare minimum to get the server started.
 - ii. *store.json* file contains most of the MFA Server settings.
 - iii. *log4j.xml* regulates the level of logging and the logging mechanism.
- **license** – The location of the license file.
- **logs** – Contains the following log files:
 - i. *server.log* – Contains system information used for troubleshooting.
 - ii. *event.log* – Contains server events like startup, deployment and more
- **mods** – contains temporary data. Do not add or remove anything from this directory if not instructed to do so by Clavister support personnel.
- **webroot** – the location of HTML templates, images and scripts used when serving HTML content. Changes to any files in this directory will be overwritten on upgrade.

23.9. Logging

The Clavister MFA Server generates *event messages* which are stored in the following two files: *event.log* and file.

- **event.log**

These are events that relate to the operation of the server as it services authentication requests.

- **server.log**

These are system events that relate to the operation of the server itself.

The event format used is the *Common Event Format* (CEF). Events can also be configured so they are sent to an external syslog server. Logging configuration is controlled by the *log4j.xml* file.

Log Event List

Below is a list of MFA Server events:

- EVT_000000("Server initializing").
- EVT_000001("Server initialized").
- EVT_000002("Server starting").
- EVT_000003("Server started").
- EVT_000004("Server stopping").
- EVT_000005("Server stopped").
- EVT_000006("Server initialization failed").
- EVT_000007("Server start failed").
- EVT_000008("Server stop failed").
- EVT_000009("Server configuration reloaded").
- EVT_000010("Server configuration reloaded failed").
- EVT_000011("Server configuration updated").
- EVT_000012("Server node joined cluster").
- EVT_000013("Server node left cluster").
- EVT_000014("License expired").
- EVT_000030("Session expired").
- EVT_000031("Service started").
- EVT_000032("Service stopped").
- EVT_000033("Module stopped").
- EVT_000034("Module started").
- EVT_000035("Scheduled job performed").
- EVT_000036("Scheduled job failed").
- EVT_000040("Session NOT found").
- EVT_000041("Module reconfigured").
- EVT_000050("Connection established").
- EVT_000051("Connection failed").
- EVT_000100("Hardware Tokens imported from PSKC file").
- EVT_000101("Hardware Tokens imported from CSV file").
- EVT_000102("Hardware Token assigned to user").
- EVT_000103("Hardware Token unassigned from user").
- EVT_000105("Hardware Tokens imported from Yubico CSV file").
- EVT_000110("Hardware Token deleted from token store").
- EVT_001000("Token authentication failed, token locked").
- EVT_001001("Token authentication success").
- EVT_001002("Token authentication failed, wrong OTP").
- EVT_001003("Allowed access from location").
- EVT_001004("Disallowed access from location").

- EVT_001005("Message sent").
- EVT_001006("User authentication success with username & password").
- EVT_001007("PIN code validation success").
- EVT_001008("User authentication failed").
- EVT_001009("PIN code validation failed").
- EVT_001010("User authentication failed, user is locked").
- EVT_001011("User authentication failed, incrementing lock state counter").
- EVT_001012("User authentication failed, temporary locking user").
- EVT_001013("Question And Answer authentication failed, no or not enough questions for user").
- EVT_001014("Question And Answer authentication failed, user failed authentication").
- EVT_001015("User authentication success with question and answer").
- EVT_001016("Geo location translated").
- EVT_001017("Wrong OTP provided").
- EVT_001018("Provided OTP was correct").
- EVT_001019("Token enrolled").
- EVT_001020("OTP delivery success").
- EVT_001021("OTP delivery failed").
- EVT_001022("User authentication success with username, password & OTP").
- EVT_001023("User authentication failed with username & password, safe mode enabled, sending Access Challenge").
- EVT_001024("OTP delivery failed, no OTP in request").
- EVT_001025("OTP delivery failed, no recipient address in request").
- EVT_001026("Message delivery success").
- EVT_001027("Message delivery failed").
- EVT_001028("Message delivery failed, no recipient address in request").
- EVT_001029("Generated OTP was not found").
- EVT_001030("User authentication failed, permanently locking user").
- EVT_001031("User authentication failed, incrementing failed login attempts").
- EVT_001032("Token revoked").
- EVT_001033("Hardware Token auto enrolled").
- EVT_001034("User authentication based on header performed successfully").
- EVT_001035("User authentication, windows integrated, performed successfully").
- EVT_001036("Successful OTP response").
- EVT_001037("Failed OTP response").
- EVT_001100("Successfully looked up user").
- EVT_003000("Successfully validated X509 certificate").
- EVT_003001("X509 certificate failed revocation checking").
- EVT_003002("X509 certificate issuer not trusted").
- EVT_003003("X509 certificate failed basic validation").
- EVT_003004("User authentication success with certificate").
- EVT_004000("Successfully authenticated with Swedish BankID").
- EVT_004001("Swedish BankID Authentication Failed").
- EVT_004002("IDP meta data loaded").
- EVT_004003("SP meta data loaded").

Appendix A: Cube Log Messages

This reference appendix specifies the log messages included in the predefined *Cubes* that are used when specifying log analyzer queries in the InControl client. Cubes are discussed further in *Section 18.6, "The Log Analyzer"*.

URL Requests

- 200125
- 200126
- 200135
- 200136
- 200137

Bandwidth Usage

- 600002
- 600003
- 600005
- 600102
- 600103

IDP Events

- 1300001
- 1300002
- 1300003
- 1300004
- 1300005
- 1300006
- 1300007
- 1300008
- 1300009
- 1300010
- 1300011
- 1300012
- 1300013
- 1300014
- 1300015
- 1300016

AntiVirus Alerts

- 5800001
- 5800002
- 5800003
- 5800004
- 5800005
- 5800006
- 5800007
- 5800008
- 5800009

- 5800010
- 5800011
- 5800012
- 5800015
- 5800016
- 5800017
- 5800018
- 5800024
- 5800025
- 5800182
- 5800183
- 5800184
- 5800185

RADIUS Accounting User Statistics

- 3700008

DNS Errors

- 200545
- 1800308
- 1800309
- 2700002
- 2800002

DHCP Client Events

- 700002
- 700003
- 700004
- 700005
- 700007
- 700008
- 700009
- 700010
- 700011
- 700012
- 700013
- 700014
- 700015

DHCP Server Events

- 900006
- 900007
- 900008
- 900011
- 900012
- 900013
- 900017
- 900018
- 900019
- 900027

ARP And ARP Poison Events

- 300001
- 300002
- 300003
- 300004
- 300005
- 300006
- 300007
- 300008
- 300009
- 300049
- 300050
- 300051
- 300052
- 300053
- 300054
- 300055

Network Errors

- 500001
- 600003
- 3900001
- 3900003
- 3900004

L2TP Tunnel Events

- 2800018
- 2800011
- 2800016
- 2800007
- 2800008
- 2800009

PPPOE Tunnel Events

- 2600001
- 2600002

PPTP Tunnel Events

- 2700006
- 2700008
- 2700012
- 2700013
- 2700014
- 2700015
- 2700019
- 2700021

- 2700022

SSLVPN Tunnel Events

- 6300010
- 6300011
- 6300205

Connection Statistics

- 600001
- 600002
- 600003
- 600005
- 600102
- 600103
- 600004
- 600010
- 600011
- 600012
- 600013
- 600014
- 600015
- 600020
- 600021
- 600022
- 600100
- 600101

System Events

- 3201000
- 3201010
- 3201011
- 3201020
- 3201021
- 3202000
- 3202001
- 3202500
- 3203000
- 3203001
- 3203002
- 3204001
- 3204002
- 3206000
- 3206001
- 3206002

High Availability Events

- 1200001
- 1200002
- 1200055
- 1200500

User Authentication Events

- 3700020
- 3700021
- 3700100
- 3700101
- 3700102
- 3700104
- 3700106
- 3700107
- 3700110

Email Events

- 200156
- 200157
- 200158
- 200158
- 200160
- 200164
- 200165
- 200166
- 200167
- 200172
- 200176
- 200195
- 5800182
- 5800184

Application Usage

- 07200003

Appendix B: Netcon Key Generation

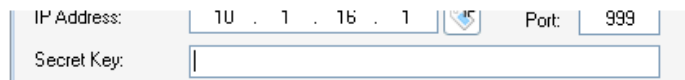
The Netcon Protocol

All remote management of Clavister Security Gateways, including configuration, monitoring and upgrades by InControl is secured using 128-bit encryption and authentication. The proprietary protocol used for this is called *Netcon*.

Netcon uses CAST-128 encryption between the InControl server and Clavister Security Gateways. It uses AES-256 (Rijndael) encryption between clients and the server. Netcon also uses both TCP and UDP as a transport protocol on destination port 999.

New Gateways Require a Netcon Key

As explained in *Chapter 7, Adding Security Gateways*, when setting up communication with a gateway, InControl requires that a *Netcon* key is pasted into the *Secret Key* field in the new gateway dialog.



The screenshot shows a configuration dialog with three fields: 'IP Address' containing '10 . 1 . 16 . 1' with a dropdown arrow, 'Port' containing '999', and 'Secret Key' which is an empty text box.

The required Netcon key is obtained from cOS Core outside of InControl using 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.

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 cOS Core Web Interface of the Clavister Security Gateway which is to be defined with InControl.
2. Go to **Objects > Key Ring > Add Pre-Shared Key** and the page for creating a Pre-Shared Key object will be displayed.

Key Ring

+ Add ▼

Type	Type
Certificate	
Pre-Shared Key	
SSH Client Key	
2	auth agent nsk
	Pre-Shared Key
	HFx

3. Select a suitable name for the key, for example *my_key*.
4. Select *Hexadecimal Key*.
5. Select *512* from the bit size choices and press the *Generate Random Key* button.
6. 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.

Type: ▼

Passphrase:

Generate Random Key of size ▼ bits.

7. Press the *OK* button.

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

1. Still in the Web Interface, go to **System > Remote Management > Add > InControl Management (Netcon)** and the page for Netcon management will be displayed.

Remote Management

Setup and configure methods and permissions for remote management of this system.

+ Add ▼ **Advanced Settings**

	Mode	Interface
HTTP/HTTPS Management		
SNMP Management		
SSH Management		
InControl Management (Netcon)		
HTTP/HTTPS Manage...	Admin: HTTP, HTTPS	G1
Management	Admin: Password, Publ...	G1

2. Set the *PSK* field to the key called *my_key* created previously.
3. Select the interface and network where the InControl workstation is located. Any network can be specified by using the value *all-nets* but it is more secure to specify a narrow IP range.

InControl Management (Netcon)

Configure Netcon management to enable remote management to the system.

Mode: Configure

Idle timeout: 900

PSK: my_key

Access Filter

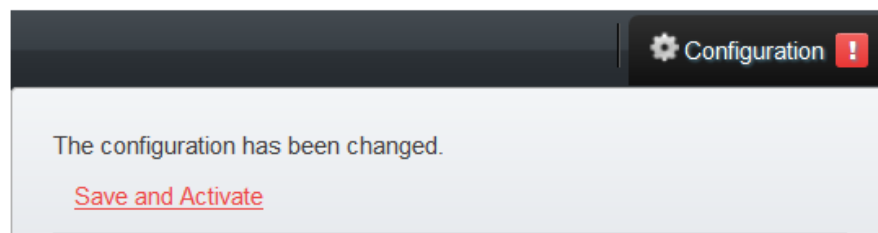
Interface: If1

Network: all-nets

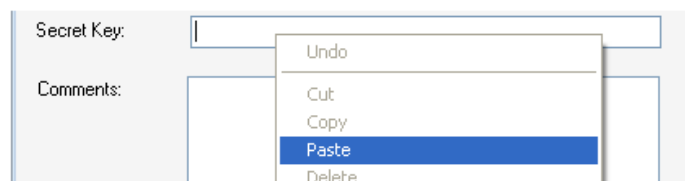
4. Press the OK button.

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

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



2. Finally, the key can be pasted into the InControl new gateway dialog in InControl. The Web Interface browser window can be closed.



An example of a Netcon key pasted into the secret key field is shown below.

IP Address: . . . Port: 999

Secret Key: AA39634830E1EEE1F406B812C550EBCDDCC447307C8E

Using the CLI

When the CLI is used instead of the Web Interface to get the secret key, 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.

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

```
Device:/> set RemoteManagement RemoteManagementNetcon
          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.

Activate the configuration changes.

```
Device:/> activate
```

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

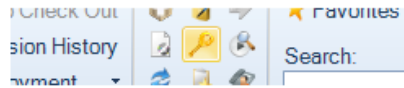
```
Device:/> commit
```

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

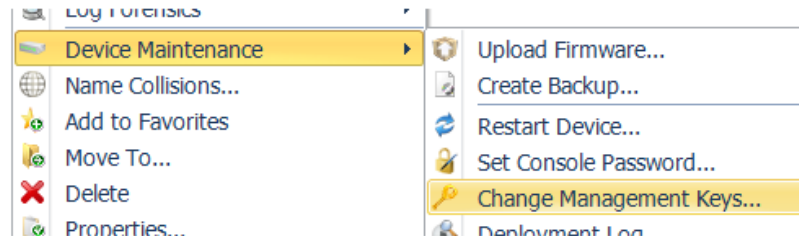
Changing the Netcon Key

Once a gateway is added to InControl, the InControl client provides the ability to automatically change the Netcon key to a new matching value on both server and gateway. If the gateway is still using the default key, an alert is automatically generated in InControl client and it is highly recommended that this is changed as soon as possible. The new key is generated randomly by InControl and does not need to be input manually.

This function can be found in the *Security Gateways* tab toolbar.



Alternatively, this function can be found in the context menu displayed after right clicking the gateway.



It will not be possible to change the keys in this way if:

- The security gateway does not have a cOS Core license and is in 2 hour demonstration mode.
- The gateway's configuration is checked out. Either a check in must be performed or the check out must be undone.

Appendix C: Certificate Requests

Some security features in cOS Core 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.

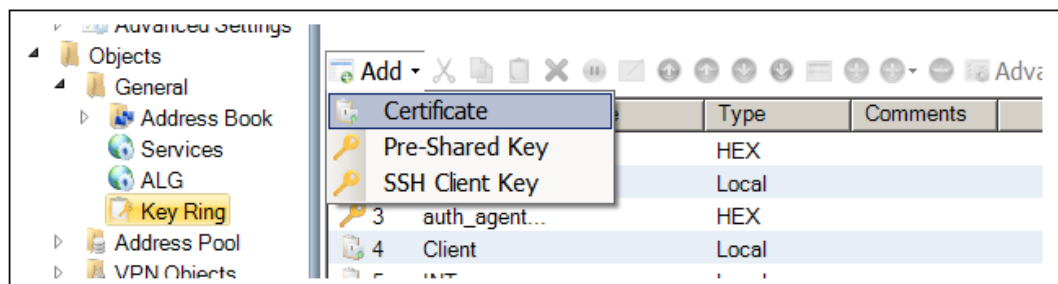
The sequence of steps for certificate requests is:

- A. Create a certificate request.**
- B. Export the request file and send it to the CA.**
- C. Import the certificate file sent back by the CA.**

These steps will now be described in detail:

A. Create a certificate request.

To do this, select: **Objects > General > Key Ring > Add > Certificate.**



The new certificate dialog will open. Choose **Create new.**



The wizard to create a certificate will start. The wizard steps are as follows:

- Select the **Create certificate request** option and enter an appropriate name and comment.

Choose Certificate Type

☐ Create self-signed certificate
 Others need a copy of the public certificate file in order to verify it.

☒ Create certificate request
 Certificate requests are first passed to certificate authorities for signing. When signed, others only need a copy of the public CA cert to verify your certificate.

General Parameters

Name:

Comment:

- Specify the public key algorithm. The validity date will be decided by the CA.

Public Key Algorithms

☒ RSA

☐ DSA

Certificate Validity

Valid From:

Valid To:

- Specify the subject-name parameters.

Subject Name Parameters

Common Name:

Organization Name:

Organization Unit:

Country:

Enter the most common types above or as a comma separated list of types below.
 For example "ST=my_state, L=my_locality" for state and locality.

- Specify the subject-alt-name parameters.

Subject Alternative Name Parameters

Email:

DNS:

IP Address:

Extra Parameters

☒ Dont Require CRLs

- The wizard now creates the certificate object but with the *Type* property set to *Request*. Press the **Finish** button to close the wizard and return to the properties of the new certificate.

Action	Progress
✓ Creating encryption keys - ph..	Done
✓ Creating encryption keys - ph..	Done
✓ Creating certificate	Done

The request file for the certificate still needs to be created and that is the next step.

B. Export the request file and send it to the CA.

To export the request, select the **Export** option.

Options


A file chooser will appear allowing the name of the request file to be specified. The filetype should be left as *.req*.

File name:

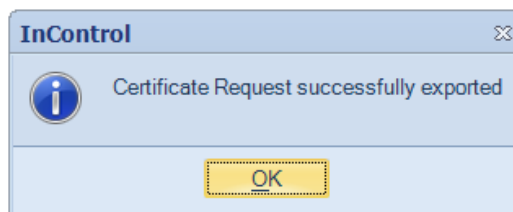
Save as type:

A dialog will appear to ask if the private key should be included. Answer **No**. The private key file (with filetype *.key*) is not required to be exported since this should never be transmitted to third parties.

InControl

 Do you want to export the private key as well?
Note that this might be a security risk.
Choose 'Yes' only if you are sure of this

The request file is now written to disk with a filetype of *.req*.



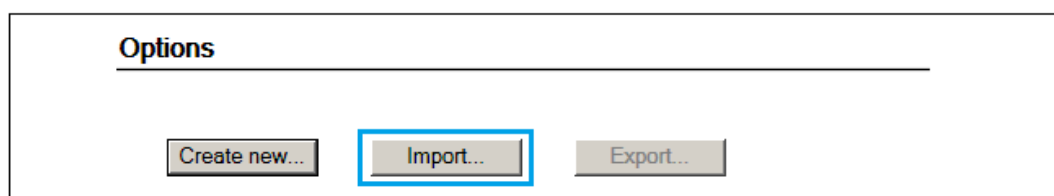
Press the **OK** button for this *Certificate* object to save it in the cOS Core configuration as a request so it can be completed later when the public key file is received.

This request file can now be emailed to the CA for issuance of the signed public key file.

C. Import the certificate file sent back by the CA.

The CA will send back the signed server certificate (gateway certificate) which consists of a single file with a filetype of *.cer*.

Now, import the certificate file into InControl by choosing the **Import** option.



A file chooser will open allowing the *.cer* file to be selected.



The certificate is now imported into cOS Core and available for use.

Using an Internal CA

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

Creating Self-signed Certificates

The procedure for creating a self-signed certificate is a subset of the steps for creating a certificate request. Add a new *Certificate* object as described above, select **Create new** as before to start the wizard, but instead of creating a request select the option to create a self-signed certificate.

A *Certificate* object with the *Type* property set to request is essentially a self-signed certificate which is waiting to be signed, although it cannot be used with other configuration objects.

Choose Certificate Type

☒ Create self-signed certificate
Others need a copy of the public certificate file in order to verify it.

☐ Create certificate request
Certificate requests are first passed to certificate authorities for signing. When signed, others only need a copy of the public CA cert to verify your certificate.

General Parameters

Name:

Comment:

Go through the wizard, entering the certificate details. After the wizard finishes, select **OK** to save the self-signed certificate. This can then be used with, for example, VPN tunnels.

If the certificate needs to be imported on another Clavister Security Gateway, the `.cer` and `.key` files can be saved to the local disk using the certificate **Export** option. It can then be re-uploaded to another gateway through the certificate **Import** option in InControl or using the Web Interface.

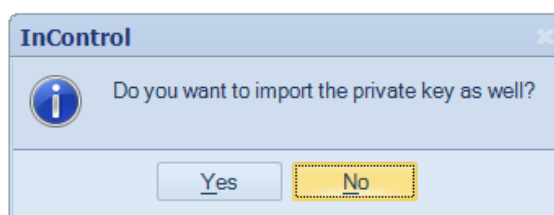
The cOS Core Web Interface also offers a way to create self-signed certificates but with less options. Go to **Objects > Key Ring > Add > Certificate** in the Web Interface, then choose the *Generate (RSA)* from **Source** options for the new certificate. This is described in the separate *cOS Core Administration Guide*.

Importing Existing Certificates

If a new certificate is to be defined based on existing certificate files then this is done by first creating a named *Certificate* object in InControl and then using the **Import** option to select the `.cer` file which contains the new certificate's public key.

If the `.key` file containing the private key is present in the same directory as the `.cer` file, InControl will automatically import both files and the *Type* for the object will be set to *Local*.

If the `.key` file is not found, InControl will ask if it is to be imported as well.



If the answer is *No*, the *Type* property is set to *Remote*. If the answer is *Yes*, a file chooser dialog appears to select the private key file and the *Type* property becomes *Local*.

Appendix D: 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+C	Check In/Out.
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.
Alt + Left Arrow	Move backwards in the client history to a previous central pane.
Alt + Right Arrow	Move forwards in the client history to a previous central pane.

InControl Glossary

Clavister Hardware Series	The series of Clavister hardware appliances that run the cOS Core operating system.
Clavister Security Gateway	A hardware device which is running the cOS Core operating system.
Clavister Software Series	Versions of the cOS Core operating system which run on generic, non-Clavister hardware.
CLI	The <i>Command Line Interface</i> for cOS Core. 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.
cOS Core	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 cOS Core 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 cOS Core 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 cOS Core management interface made possible by connecting to cOS Core 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, 12

A

Active Directory server authentication
 required additional steps, 93
 setting the authentication source, 28
 setting up a group, 91
adding configuration objects, 56
adding security gateways
 using gateway initiated Netcon, 36
 via the InControl client, 39
alarm, 77
 acknowledging, 79
 action, 77
 center, 78
 clearing, 79
 search criteria, 80
API for InControl, 8
architecture, 7
audit trail, 82
 filtering messages, 83

B

backup
 creating from database, 63
 creating from gateway, 62

C

certificate requests, 203
certification authority, 203
changing management keys, 63
checking in, 48
 domains, 52
checking out, 47
 keyboard shortcut, 47
CLI
 diagnostics, 167
 remote console opening, 95
client
 autosave, 29
 file tab, 27
 installation, 14
 interface, 26
 interface history, 27
 login, 14
 progress view panel, 30
 runtime options, 31
 security gateways tab, 26
 settings, 27
configuration errors/warnings/notices, 59
configuration object groups, 160
 and folders, 165
 and the CLI, 161
 editing properties of, 162
configuration versions (see revision management)
control properties, 102

D

dashboard
 activating, 105
 designing, 100
 managing saved, 105
 opening, 105
 quick monitor, 106
 reducing dampening, 30, 106
 saving, 104
 sharing, 105
database
 backup, 22
 installer created backups, 17
 moving between computers, 24
 restore, 23
 restoring installer backup, 17
data bindings, 102
deleting security gateways, 43
demonstration mode, 66, 71
deploying configurations changes, 49
 deployment log, 49
deploying multiple configurations , 50
deployment log, 63
design mode, 103
device maintenance, 62
domains, 84
 and the CLI, 88
 checking in and out, 86, 86
 creating, 84
 flagging unused objects, 29, 88
 global, 84
 inefficiency from misuse, 84
 inefficiency from misuse, 39
 name duplication, 86
 resolving name collision, 87
 sub-domains, 85
dynamic maximums, 102

E

editing configuration objects, 60

G

gateway initiated Netcon, 36
groups
 configuration objects, 160

H

high availability cluster, 154
 adding cluster members, 156
 adding existing clusters, 157
 changing the sync flag, 158
 choosing master and slave, 156
 creating a cluster, 154
 node ID change in revisions, 54
 removing cluster members, 158
 version mismatch alerts, 158

I

ILA, 110
 adding query parameters, 124
 changing sending IP address, 114
 changing the secret key, 116
 configuration editing, 113
 configuring cOS Core, 113
 database files, 111
 database management, 116

- data folder/file naming, 117
- filter similar option, 125
- ILA.exe, 111
- installation, 110
- library browser, 151
- log explorer, 119
- logging without InControl management, 117
- LogReceiver.exe, 111
- port needed for communication, 111
- query filter, 123
- restarting services, 112
- services, 111
- using LQS files, 19
- importing certificates, 207
- in-cell editing, 60
- InControl logging agent (see ILA)
- InfoBright™, 141
 - empty report issue, 142
 - RAM memory requirements, 142
- installation, 10
 - .NET requirements, 12
 - client, 14
 - recommended configuration, 10
 - server, 12
- internal CA servers, 206
- IP rules
 - adding, 56
 - allowing ICMP ping example, 55
 - editing, 60

K

- keyboard shortcuts, 208

L

- library browser, 151
 - activating objects, 152
 - editing properties, 153
 - information display, 152
 - library types, 151
 - sharing objects, 153
- license center website, 69
- licenses, 65
 - CENTRALIZED_MANAGEMENT parameter, 66
 - demo mode, 71
 - enabling automatic download, 69
 - for cOS Core, 71
 - for the server, 66
 - importing from disk, 73
 - InControl, 65
 - licenses tab, 65
 - network access for download, 73
 - repository, 72
 - server license binding, 68
 - updating, 74
- log analyzer, 132
 - auto drill down, 140
 - changing back to SQLite, 142
 - changing the database software, 140
 - constructing queries, 134
 - cube, 133, 135
 - database update frequency, 137
 - deselecting statistics, 133
 - drill down, 139
 - enabling, 132
 - generating reports, 133
 - limiting slices processed, 137

- predefined queries, 139
- query columns, 136
- query delays, 137
- query filters, 136
- query rows, 135
- query time window, 136
- query values, 135
- re-scan logs option, 143
- retention time setting, 143
- running queries, 137
- saving queries, 138
- temporary data location setting, 143
- UTC/GMT timestamps, 137
- log event monitoring, 108
- log explorer, 119
 - color coding of messages, 120
 - filters, 121
 - real-time display, 119
 - running a query, 120
 - using relative time, 120
 - using time span, 121
- logging, 110
- log monitoring
 - memlog, 108
- log query language (see LQL)
- LQL, 126
 - gateway/time statements, 131
 - logical operators, 127
 - output types, 129
 - search variables, 128
 - statement syntax, 126
- LQS
 - backing up, 18
 - moving files to ILA, 19
 - uninstalling, 18

M

- memlog, 108
- mfa server, 168
 - adding server to InControl, 173
 - app, 188
 - combining password and otp, 188
 - configuration objects, 175
 - configuring cOS Core, 170
 - folders, 189
 - installation, 171
 - license, 172
 - license file download, 172
 - license installation, 172
 - logging, 190
 - mfa server object, 176
 - Overview, 168
 - RADIUS client configuration, 178
 - RADIUS server configuration, 178
 - revision history, 174
 - scenario, 175, 181
 - scenario types, 181
 - self service configuration, 179
 - self service portal, 186
 - SMS credits, 184
 - starting the server, 172
 - supported clients, 185
 - user/pass scenario, 181
 - username/password/SMS scenario, 183
 - username/password/token/OTP scenario, 182
 - user store configuration, 177
- MFA Server

- default port numbers, 171
- hardware requirements, 171
- monitoring
 - quick monitor, 106
 - real-time, 98
- MySQL™, 141

N

- name collision resolution, 87
- Netcon, 198
 - changing keys automatically, 201
 - creating keys with CLI, 200
 - creating keys with WebUI, 198

O

- offline/online status switching, 44

P

- ping
 - checking connections with, 166
 - IP rule allowing, 55
- preparing cOS Core, 33

R

- remote console, 95
 - logging, 96
 - logging settings, 29
 - multiple sessions, 96
 - time-out, 96
- remote management cOS Core objects, 33
- reporting, 144
 - adjusting query settings, 148
 - archive, 145
 - background generation, 145
 - background processing, 144
 - generating, 145
 - prerequisites, 144
 - sections, 146
- restarting a gateway, 64
- revision history, 53
 - displaying differences, 53
 - displaying statistics, 54
- revision management, 46
 - concurrent CLI/WebUI changes, 52
 - HA node ID changing, 54
 - revision history, 53
 - revision numbers, 52

S

- saving dashboards, 104
- SDK for InControl, 8
- secret key (see Netcon)
- self-signed certificates, 206
- server
 - applying changes, 22
 - audit level, 21
 - AutoCleanupDatabase setting, 24
 - changing status, 13
 - console, 21
 - disk space management, 24
 - effect of stop on clients, 21
 - installation, 12
 - interface, 12
 - management, 20

- MaximumDaysToKeepConfigurations setting, 25
- MinimumConfigurationsToKeep setting, 25
- MinimumRequiredDisk setting, 25
- processes, 13
- stopping and pausing, 20
- syslog server config, 21
- transfer limit, 21
- Type setting, 25
- VacuumDatabase setting, 25
- server license, 66
 - binding, 68
 - download, 67
- service account
 - server interface access, 20
 - with InControl Server, 11
 - with the ILA, 112
- setting the console password, 63
- speedometer, 101
- SQLite™, 25, 140

T

- tech support file generation, 64
- text captions, 104
- themes, 104
- troubleshooting connections, 166
 - CLI diagnostics, 167
 - routing problems, 167

U

- undo check out, 51
- upgrading
 - from InControl 1.10, 18
 - InControl, 17
 - resolving name collision, 87
 - using 1.10 files, 18, 19
- user accounts, 89
 - groups, 90
- user groups, 90

V

- volume license (see server license)

W

- Windows™ processes, 13



CLAVISTER®

CONNECT • PROTECT

Clavister AB
Sjögatan 6J
SE-89160 Örnsköldsvik
SWEDEN

Phone: +46-660-299200
www.clavister.com