



Administrators Guide

Clavister Secure Access Gateway Version 6.20

Clavister AB
Torggatan 10
SE-891 33 Örnsköldsvik
SWEDEN

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

www.clavister.com

Build: 62000-Edition-2
Published 2008-10-07
Copyright © 2008 Clavister AB

Administrators Guide Clavister Secure Access Gateway Version 6.20

Published 2008-10-07
Build: 62000-Edition-2

Copyright © 2008 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 written consent of the author.

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person 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. Initial Setup	6
2. Configuration and Administration	8
3. Monitoring and Status	10
3.1. Status	10
3.2. Sessions	12
3.3. View Logs	15
3.4. Statistics	16
4. Administration	18
4.1. Users and Groups	18
4.2. Address Pools	27
4.3. Resources	28
4.3.1. Resource Administration	28
4.3.2. Access Control	38
4.3.3. Cache Control	45
4.4. The Navigator	47
4.4.1. Creating New Menu Entries	49
4.4.2. Edit a Menu Entry	56
4.4.3. Change View Order	57
5. The Authenticator	61
6. Server Settings	63
6.1. General Settings	63
6.2. Supervision Settings	66
6.3. Node Settings	67
6.4. Network Connector	72
6.5. Local Database Settings	77
6.6. URL Converter	83
6.7. Virtual Hosts	84
7. Client Settings	86
7.1. User Agents	86
7.2. Timeout Settings	89
7.3. Layout Settings	91
8. Authentication	93
8.1. RADIUS Servers	93
8.2. Web Authentication	94
8.3. Authentication Methods	100
8.4. Authentication Groups	102
9. Maintenance	104
10. Activate Changes	109
11. Modification of Pages	111
A. Load Balancing	113
B. Parameters	114
C. External LDAP Attributes and Objects	118
D. Microsoft Active Directory Integration	119
E. Novell eDirectory Integration	123
F. Message Center	127
Alphabetical Index	132

List of Figures

2.1. The Clavister SAG Control Center	8
2.2. The Virtual Host Selector	9
3.1. The Monitoring and Status Menu	10
4.1. The Administration Menu	18
4.2. New Address Pool	27
4.3. FTP Resources	37
4.4. Windows Share Resources	37
4.5. An Access Control List	38
4.6. ACL for a Web and FTP Server	39
4.7. ACL for a Tunnel	39
4.8. Access Control Groups	42
4.9. Creating New Menu Entries	49
5.1. The Authenticator Menu	61
6.1. Request Remote Assistance	65
7.1. The Client Settings Menu	86
8.1. The Authentication Menu	93
8.2. The Java Keypad	95
8.3. A Randomized Javascript Keypad	95
9.1. The Maintenance Menu	104
10.1. The Activate Changes Option	109

Preface

Target Audience

The target audience for this publication is the administrator of a Clavister Secure Access Gateway installation.

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 Section 4.2, "Address Pools".

Web links

Web links included in the document are clickable eg. <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.

Chapter 1. Initial Setup

After receiving a brand new Clavister SAG appliance, you should first follow the steps described in the accompanying document entitled *Clavister_SAG_Quick_Start_Guide.pdf*. This document explains the initial steps of switching on the unit and performing initial configuration. Once you have gone through those steps you should return to this guide.

As explained in the Quick Start Guide, a default administration user account called *testlogon* is already available for the initial configuration. This user does not have a password and authentication is done solely by checking on the originating IP address. Once the product is up and running, the following should be done:

- Set up a new user with administration privileges and secure authentication.
- Disable the *testlogon* user account since it lacks good security.

The steps to achieve this are described below:

A. Set up a new administrative user

1. Open an internet browser on a computer which has the same management IP address already specified in the Quick Start Guide Steps. "Popups" should be allowed in the browser since these are used extensively by the user interface.
2. Surf to the management IP address. The initial CSAG screen will appear asking for the authentication method. Select the *testlogon* option.
3. Select **Control Center**.
4. Select **User & Groups** from the **Administration** menu. No users are defined yet so click on **Create User...**
5. Specify an appropriate name for the user (such as *admin_user*) as the the **User Login ID** and press the **Create** button.
6. As a minimum, select the options following for this first administrative user:
 - Make the user a member of the group called *admins*.
 - For password authentication select the **Enable** option for **Web Token Basic** and **Never Expires** option and enter a password followed by retyping the password.
 - Press the **Save** button.
7. Finally add a new access control rule for the *admins* group:
 - Go to **Resources > Access Control**.
 - The ACL Resource List is displayed.
 - From the **Local Services** list, choose **Control Center**.
 - Choose **Access Control...**
 - Select **Add new rule**.
 - Select *admins* from the drop-down list under **Groups**.
 - Other fields is the rule can be changed if desired, in this case the *Web token*.

- Press the **Save** button and then **Return**.
8. Choose **Activate Changes** and then **Reload Configuration**.
 9. Now logout and close the web browser

B. Disabling *testlogon*

1. Open the browser again and surf to the management IP.
2. Choose **Login with web token**
3. Enter the user name (in this case *admin_user*) and enter the password. The keypad can be used if the password for any numbers in the password. The "E" is the keypad can be used as the Enter key.
4. Select **Control Center**.
5. Using the new administration user, go to **Authentication > Authentication Methods**
6. Uncheck the **Enable** box for testlogon and then press the **Save/update** button followed by **Reload now**. Then click on **OK** to confirm.
7. Logout and close the browser. Reopen the browser and surf to the management IP. This time the *testlogon* option should be disabled and will not be visible in the initial authentication menu.



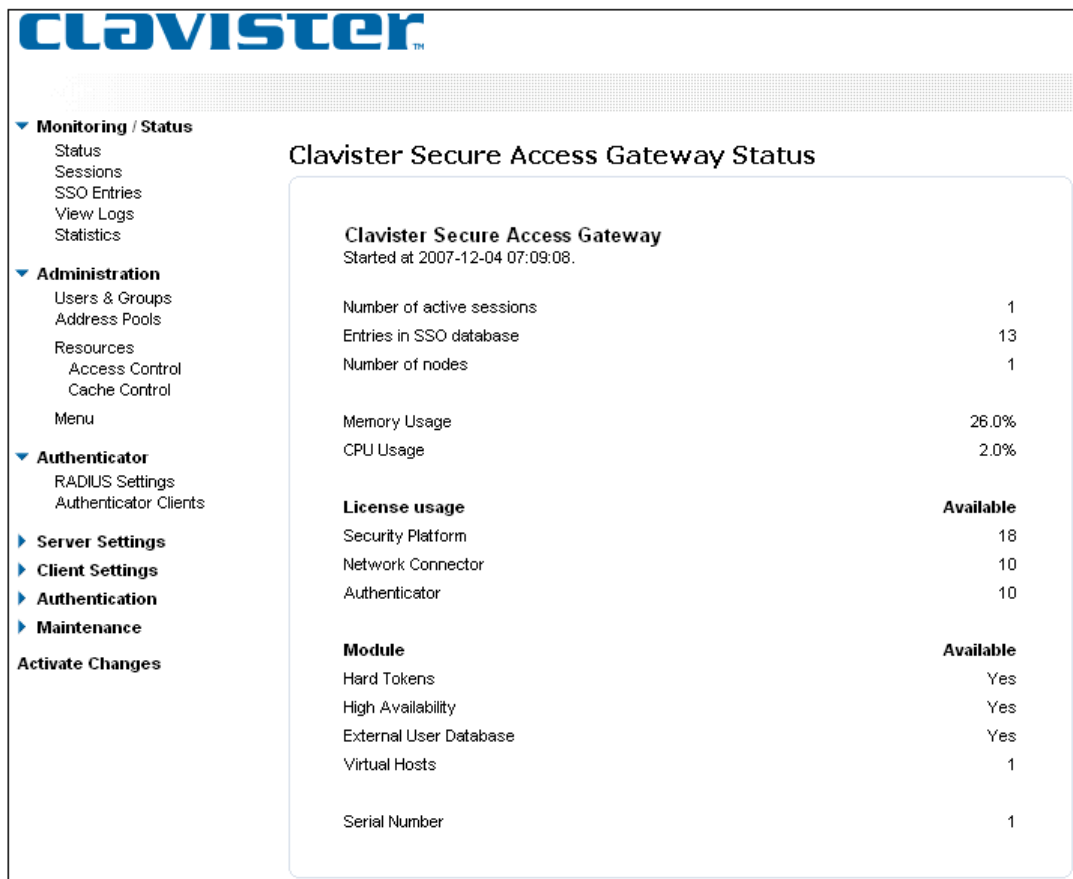
Note on Logging Out

In the procedure described above, logout from Clavister SAG is recommended before closing the browser. Although closing the browser should be enough on it's own, logging out beforehand forces a cleanup of the resources used on the Clavister SAG server.

Chapter 2. Configuration and Administration

Clavister SAG can easily be configured and administered using a web-based interface called the *Control Center*. Control Center is accessible from the Clavister SAG navigation menu.

Figure 2.1. The Clavister SAG Control Center



The Control Center interface is divided into seven sections:

- **Monitoring**
Status Monitoring functions such as server status, log files and current users.
- **Administration**
Administration functions for resources, groups and users.
- **Authenticator**
Settings for the Clavister SAG Authenticator. This section is only visible when the Clavister SAG Authenticator is installed.
- **Server Settings**
Settings for the Clavister SAG server.
- **Client Settings**
Settings for clients such as timeouts and web browser settings.

- **Authentication**
Settings for the authentication methods.
- **Maintenance**
Maintenance functions, such as installing new license file, backup configuration and upgrading Clavister SAG.

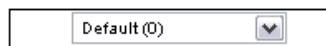
This guide will follow the structure of the administration interface of the Control Center.

Each section can be expanded and collapsed with a click on the sections arrow or label. What sections that is shown here depends on the ACL-settings for the Control Center and the license installed.

The Virtual Host Selector

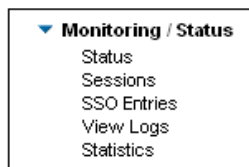
On the top of the menu on the left is the virtual host selector. It is only visible if one or more virtual host has been configured. It lets the administrator select which one of either the default host or virtual hosts to configure. More information can be found in Section 6.7, “Virtual Hosts”.

Figure 2.2. The Virtual Host Selector



Chapter 3. Monitoring and Status

Figure 3.1. The Monitoring and Status Menu



3.1. Status

The status information contains general system information such as information of license, system load, platform and current sessions.

Clavister Secure Access Gateway - version 6.1.3 TR36 (Build: 12938 / Rev: 598)
Started at 2007-12-04 07:09:08.

Number of active sessions	1
Entries in SSO database	13/13
Number of nodes	1
Memory Usage	26.0%
CPU Usage	0.0%
License usage	Available
Security Platform	18
Network Connector	10
Authenticator	10
Module	Available
Hard Tokens	Yes
High Availability	Yes
External User Database	Yes
Virtual Hosts	1
Serial Number	1

The current version of Clavister SAG and the time when Clavister SAG was last started is shown at the top of the dialog.

- **Number of Active Sessions**
Shows number of active sessions at present. For a more detailed list, click the text or the number to the right.
- **Memory Usage**
Shows percentage of memory usage compared to the amount of memory that Clavister SAG has allocated. The product can dynamically allocate more memory if necessary. If it is running in a clustered environment, then the percentage of total memory is calculated from all nodes within the cluster. It is possible to click the Number of Nodes text to get information for each node.
- **CPU Usage**

Shows the average CPU load over the last 10 seconds. If Clavister SAG is running in a clustered environment, then the percentage of total CPU Usage is calculated from all nodes within the cluster. It is possible to click the Number of Nodes text to get information for each node.

- **Platform**
Shows in which environment Clavister SAG is running.
- **License Info**
Shows the number of available licenses for the Security Platform and the Authenticator. Click on the text for a more detailed view.
- **License Expires**
Shows the date the license expires, or Never if the license is valid until forever.
- **License Valid From**
Shows the date the license was issued.
- **Issued By**
Shows the organization the license was issued by.
- **License Holder**
Shows the person/organization the license is issued to.

**Note**

The license information may be hidden if there is no specified data in the license file.

No license will be available when Clavister SAG is first installed, in which case the following status dialog will be shown:

3.2. Sessions

Click the **Sessions** link to get a view of all the current sessions. If a user logs out or is logged out automatically, the session will soon be removed. See Section 7.2, “Timeout Settings” for more information on how to configure a session that will be removed after logout.

User	Auth Method	Encryption	Client IP	Last Activity	Status	Client	Node	VHID	More Info
test	webtoken	High	85.11.194.1	10:06:11	Active	Firefox 2.0.0.11 / Windows	200	0	More

The following attributes are presented in the sessions dialog:

- User**
 The users login id. The user login id may be displayed with the character sequence "???" if the user has not been authenticated.
- Auth Method**
 The authentication method used, for example *Web Token*, *SMS Token* or *SecurID*.
- Encryption**
 The encryption grade used on the connection between the client and Clavister SAG. The possible values are:
 - Very high* - 256 bit AES
 - High* - 128 bit or longer key length.
 - Medium* - 56 to 127 bit key length.
 - Low* - 40 to 43 bit key length.
 - None* - Clear text.
- Client IP**
 The client's IP address.
- Last Activity Output**
 The time when the user was last active. This is used to decide when a user will be automatically logged-out from Clavister SAG due to inactivity. If the mouse pointer is placed above the text, an information dialog will appear including information about when the session will time out.
- Status**
 Shows the status of a session and can be one of the following:
 - New*
A user who has not yet logged-in to Clavister SAG.
 - Active*
A user presently logged-in to Clavister SAG.
 - Logged out*
A user who has logged-out from Clavister SAG.
- Client**
 Shows which web browser and operating system the client is using.
- Node**
 This information is only available when Clavister SAG is running within a cluster. It indicates which node or nodes the session is located in.
- VHID**
 VHID is the ID-number which signifies which virtual host the user is connected to.

By pressing the **More** button a separate window with more information about that session is opened.

Information

User:	<i>test</i>
Ticket ID:	<i>N/A</i>
Virtual Host:	<i>Default (0)</i>
Authentication:	<i>webtoken</i>
Encryption Grade:	<i>High</i>
Remote Tunnel Online:	<i>No</i>
Session ID:	<i>c81281ec7e5b913d86d5729ae5b5411366</i>
Client IP:	<i>85.11.194.1</i>
Browser:	<i>Firefox</i>
Browser Version:	<i>2.0.0.11</i>
Operating System:	<i>Windows</i>

Control

Kill this session

Some of the information is the same as in list above, however some is extra and is found only in this dialog:

- **User**
The user ID of the logged in user in the session.
- **Ticket**
The ticket ID is used to distinguish between different remote assistance requests. This field is only set if the user has requested remote assistance.
- **Remote Tunnel Online**
Tells the administrator if the remote side of the dynamic tunnel is active or not.
- **Kill this session**
Clicking on the **Kill** link will force Clavister SAG to logout the user. The user will be presented with the login screen the next time the user sends a request to Clavister SAG.
- **Remote Assistance**
The remote assistance **Connect with...** texts are only visible when a user has made a remote assistance request. The administrator can connect to the user's host with one of the protocols RDP, VNC or SSH.

The most useful protocol is VNC which works well on Windows (Clavister SAG provides a special executable for windows that the user can start by clicking on the remote assistance page), as well as Linux and Mac OS X.

- **Connect with RDP**
In newer versions of Microsoft Windows, a user can create an invitation for someone to provide remote assistance. To connect with RDP through Clavister SAG, an invitation must be created and sent to the person providing the assistance. Another way to use RDP for remote assistance is if the client machine accepts more than one session at a time (in other words, it is a Terminal Server). However, this way the person giving the assistance will have to have an account on the client machine and will get a separate session on the client's machine (the user and the administrator will not see the same thing).

**Note**

If the client machine is not a Terminal Server, logging in through normal RDP (without the special Remote Assistance mode) will cause the user to be logged out thus losing the Clavister SAG session.

- **Connect with VNC**
To use VNC for remote assistance the user must be running a VNC server listening at port 5900. Clavister SAG recommends TightVNC, which can be downloaded and easily started from the remote assistance page.
- **Connect with SSH**
To allow SSH for remote assistance the user must be running a SSH server listening at port 22. Most *NIX systems, most Linux distributions and *BSD systems have an SSH Server pre-installed.

3.3. View Logs

The log viewer makes it possible to view and remove the log files. The log files are compressed and rotated every day at midnight, local time.

Click the "Merge" button to merge the log files from all nodes

Main	Auth	Request	Error	
2007-12-06	2007-12-06	2007-12-06	2007-12-06	
2007-12-05	2007-12-05	2007-12-05	2007-12-05	Delete
2007-12-04	2007-12-04	2007-12-04	2007-12-04	Delete
2007-12-03	2007-12-03	2007-12-03	2007-12-03	Delete
2007-12-02	2007-12-02	2007-12-02	2007-12-02	Delete
2007-12-01	2007-12-01	2007-12-01	2007-12-01	Delete
2007-11-30	2007-11-30	2007-11-30	2007-11-30	Delete
2007-11-29	2007-11-29	2007-11-29	2007-11-29	Delete
2007-11-28	2007-11-28	2007-11-28	2007-11-28	Delete
2007-11-27	2007-11-27	2007-11-27	2007-11-27	Delete
2007-11-26	2007-11-26	2007-11-26	2007-11-26	Delete
2007-11-25	2007-11-25	2007-11-25	2007-11-25	Delete
2007-11-24	2007-11-24	2007-11-24	2007-11-24	Delete
2007-11-23	2007-11-23	2007-11-23	2007-11-23	Delete
2007-11-22	2007-11-22	2007-11-22	2007-11-22	Delete
2007-11-21	2007-11-21	2007-11-21	2007-11-21	Delete
2007-11-20	2007-11-20	2007-11-20	2007-11-20	Delete
2007-11-19	2007-11-19	2007-11-19	2007-11-19	Delete
2007-11-18	2007-11-18	2007-11-18	2007-11-18	Delete
2007-11-17	2007-11-17	2007-11-17	2007-11-17	Delete
2007-11-16	2007-11-16	2007-11-16	2007-11-16	Delete
2007-11-15	2007-11-15	2007-11-15	2007-11-15	Delete

The Merge button is only present when Clavister SAG is running in a cluster. It merges log files from different nodes into single files to be displayed. To view log information from a certain date and subject, click on the date and log type.

```

2007-12-06 09:58:09 [200] CREATED - (c81281ec7e5b913d86d5729ae5b5411366) (85.11.194.1)
2007-12-06 09:58:57 [200] LOGIN - test 85.11.194.1 webtoken
(c81281ec7e5b913d86d5729ae5b5411366) (Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11)
2007-12-06 10:14:43 [200] LOGOUT - test (c81281ec7e5b913d86d5729ae5b5411366)
2007-12-06 10:14:53 [200] LOGIN - test 85.11.194.1 webtoken
(c81281ec7e5b913d86d5729ae5b5411366) (Mozilla/5.0 (Windows; U; Windows
NT 5.1; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11)

```

3.4. Statistics

The Clavister SAG Statistics section allows the administrator to get information about how the Clavister SAG server is being used.

License History

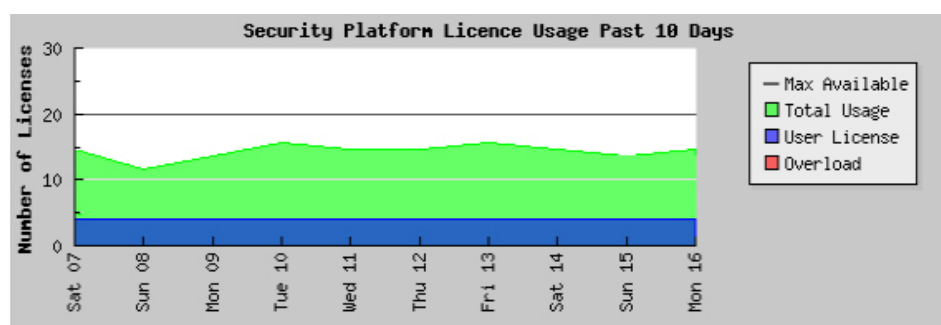
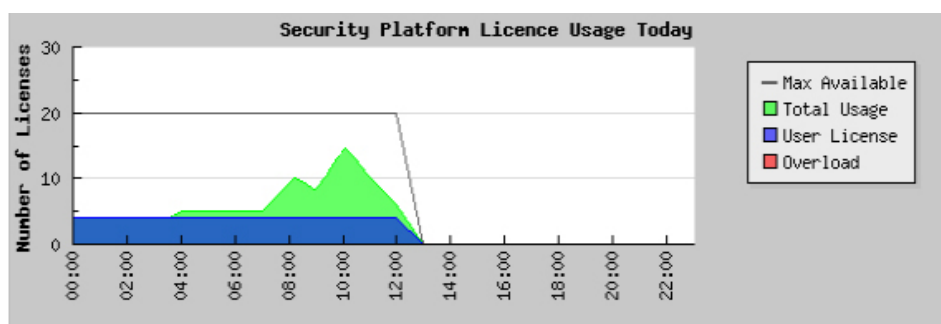
- Security Platform
- Network Connector
- Authenticator

Login and SMS History

- Login Requests
- Sent SMS

The License History

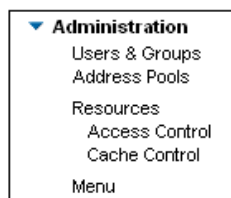
The license history statistics show the maximum number of licenses that have been used at the same time during a particular hour or day. These are examples of two of the time frames that are displayed:



The black line shows the number of installed licenses. The blue field shows the number of licenses that are locked as user licenses (in other words, how many users are members of the priouser group). The green field shows the total number of licenses used. If the number of installed licenses is exceeded, the number of users rejected is displayed with a red field.

Chapter 4. Administration

Figure 4.1. The Administration Menu



4.1. Users and Groups

All user and group related settings are gathered here. Available settings depend on whether a local database or an external LDAP directory is used.

Clavister SAG includes a local database. This local database can be used if no external LDAP directory, such as eDirectory or Active Directory, is available or if external users shall be stored in Clavister SAG only. If the local database is used, all user and group administration can be managed from Control Center.

If Clavister SAG uses an external LDAP directory, most of the user and group administration is managed from the administration interface for the directory.

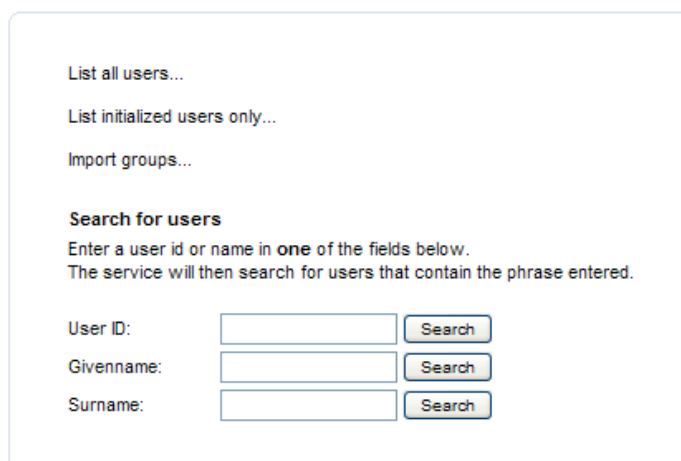
The following table shows the functionality that can be controlled from Control Center (CS) depending on whether a local or an external LDAP directory is used:

Function	Local LDAP	External LDAP
Initiate a user	CS	CS
Create, change or remove a user	CS	Via directory
Create/erase a user group	CS	Via directory
Change group membership	CS	Via directory
Allow SMS/Web authentication	CS	CS
Change SMS/Web password	CS	CS or via directory
Change users cell phone number	CS	CS or via directory
Import groups	NA	CS
Choose Inline Navigator	CS	CS
Set <i>SAG Password never expires</i>	CS	CS
Set user e-mail address	CS	CS or via directory
Set <i>Certificate User ID</i>	CS	CS
Set <i>Expires at</i> for SAG account	CS	CS

Every user that shall be administered by Clavister SAG must be included in the Clavister SAG user group (external LDAP directory only). Users not included in this group will not be found by the Clavister SAG control center. Alternatively the Clavister SAG group setting can be left empty to allow admin of all users. To specify a Clavister SAG user group, see the section covering Server Settings and Database.

When selecting the link **Users & Groups** either of the two dialogs below will be shown.

This first dialog is shown if Clavister SAG uses an external LDAP.



List all users...

List initialized users only...

Import groups...

Search for users

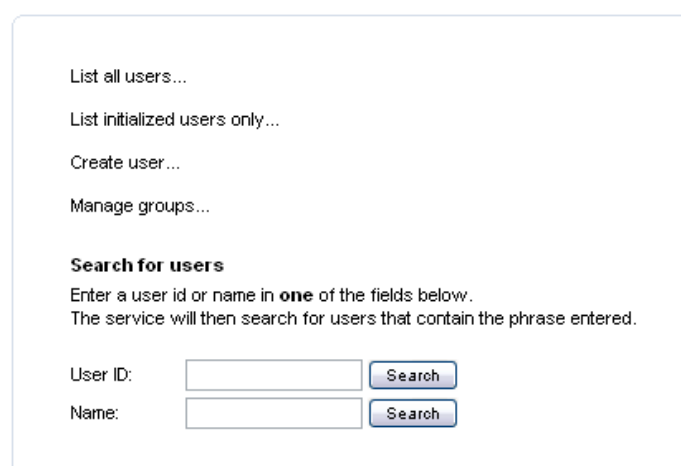
Enter a user id or name in **one** of the fields below.
The service will then search for users that contain the phrase entered.

User ID:

Givenname:

Surname:

The second dialog is shown if Clavister SAG uses the local database:



List all users...

List initialized users only...

Create user...

Manage groups...

Search for users

Enter a user id or name in **one** of the fields below.
The service will then search for users that contain the phrase entered.

User ID:

Name:

These dialogs allow the administrator to manage users and groups.

To search for users, enter a search string in one of the textboxes and press the search button next to it.

List Users

New users in the Clavister SAG user group will be presented as un-initialized if an external LDAP server is used. The administrator can choose to view either all users or only initialized users. Uninitialized users will become initialized when they are viewed and an authentication method is selected. The following image shows an example displaying all users.

4 new and uninitialized user(s) found.
To initialize a new user just click on the username, enable an authentication method and set a password.

Login	Name	Web	SMS
edu2	Education User 2	No	No
edu3	Education User 3	No	No
edu4	Education User 4	No	No
ps		No	No

Filter on: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z All
3 of 3 initialized users listed

Login	Name	Web	SMS
Administrator		Yes	No
demo	Demo User	Yes	No
edu1	Education User 1	Yes	No

[Return](#)

The upper part of the list above shows new users yet to be initialized and the lower part shows initialized users. (Users will be uninitialized if they are imported from Active Directory.)

If the local database is used, there will be no uninitialized users.

The two columns to the right show if the user is allowed to use Web/SMS token as an authentication method. A temporary blocked user is marked as **Locked** and a disabled user is marked **Disabled**. The users are shown in alphabetical order. By pressing one of the letters next to the **Filter on:** text, the users with names beginning with that letter will be displayed.

To change a user's account information, click on the user's login id.

Create New User

Note that this function is only available if Clavister SAG uses the local database. If an external LDAP is used, its administration interface must be used to create users.

When you click on **Create user**, the following dialog is shown:

User Login ID: [Create](#)

Please enter the login id for the new user and click **Create**.



Note

The *UserID* may not contain any characters outside the english alphabet. Examples of letters that are not allowed are: Å, å, Ä, ä, Ö or ö.

Change User Settings

To reach user settings, click on the user's *Login ID*. You can then edit user information, enable/disable login methods, change user passwords, etc. The settings you can change here depends on if Clavister SAG is using the internal database or an external LDAP-directory.

User DN	cn=demo,ou=users,dc=local	
UniqueID (UID)	demo	
Name	<input type="text" value="Demo User"/>	
Certificate User ID	<input type="text"/>	(Format: YYYYMMDDXXXX)
e-Mail Address	<input type="text"/>	
Comment	<input type="text"/>	
Expires at	<input type="text"/>	<input type="button" value="Select"/>
Disabled	<input type="checkbox"/>	
Inline Navigator	<input checked="" type="checkbox"/>	
Web Token / Basic	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Change at next logon <input checked="" type="checkbox"/> Never expires	
Web Password	<input type="text"/>	Retype Password <input type="text"/>
SMS Token	<input type="checkbox"/> Enable <input type="checkbox"/> Change at next logon <input type="checkbox"/> Never expires	
SMS Password	<input type="text"/>	Retype Password <input type="text"/>
SMS Cellphone 1	<input type="text"/>	<input type="checkbox"/> SMS the password to the user.
SMS Cellphone 2	<input type="text"/>	
SMS Cellphone 3	<input type="text"/>	
<input type="button" value="Group Assignment"/> <input type="button" value="Last Activity"/> <input type="button" value="View Allowed Menu Entries"/>		
<input type="button" value="Delete this user"/> <input type="button" value="Apply"/> <input type="button" value="Save"/> <input type="button" value="Return"/>		

Above is an example where the internal database is used. If Clavister SAG uses an external LDAP directory there will be fewer options to set.

- **User DN**
The user's DN (full distinguished name) from the LDAP directory. It will be the same as the UID below if the local database is used.
- **Unique ID (UID)**
The user login ID, which must be unique for every user.
- **GivenName**
The givenname of the user.
- **SurName**
The surname of the user.
- **Certificate User ID**
The attribute of the certificate that holds the unique identifier.
- **Comment**
Can be used to tag the user with some information.
- **Expires at**
The time when this user account expires. Press Select to open a small calendar.

- **Disabled**
The user will not be able to login if this checkbox is checked. In this case, the account is disabled.
- **Inline Navigator**
The user will be using a navigator that is located in a frame within the welcome page if this checkbox is checked. Otherwise the navigator will be located in a separate window. This can also be changed by the user if the access control allows it.

For **Web Token/Basic** the options are:

- **Enable**
Allow the user to log in with the authentication method Web Token or Basic authentication.
- **Change at Next Logon**
If activated the user's password must be change after the next login.
- **Never Expires**
If activated, the Web Token / Basic password will never expire. If not activated the password will expire and the user must change the password. The policies for password changes are handled in the Password Policy settings.
- **Web Password**
Set the password to use when logging in using Web Token or Basic.



Note

Change at Next Logon, Never Expires, and Web Password are not shown if the user password from an external LDAP server is used. See Section 8.2, “Web Authentication” for more information.

For **SMS Token** the options are:

- **Enable**
Allow the user to log in with the authentication method SMS Token.
- **Change at Next Logon**
If activated the user's password must be change after the next login.
- **Never Expires**
If activated, the SMS Token password will never expire. If not activated the password will expire and the user must change the password. The policies for password changes are handled in the Password Policy settings.
- **SMS Password**
Sets the password to use when logging in using SMS Token.
- **SMS Cell Phone Number 1-3**
The one-time passwords will be sent to the user's cell phone number. If more than one is defined, the user can select which one to use.

The format of the phone number must be as follows: +[country code][area code][phone number]. For example: +46733123456, where 46 is country code for Sweden, 733 is the area code and 123456 is the local phone number.

- **SMS The Password to The User**
If activated, the user's new password for SMS Token will be sent to him by SMS. The purpose of this function is to simplify the distribution of new passwords.

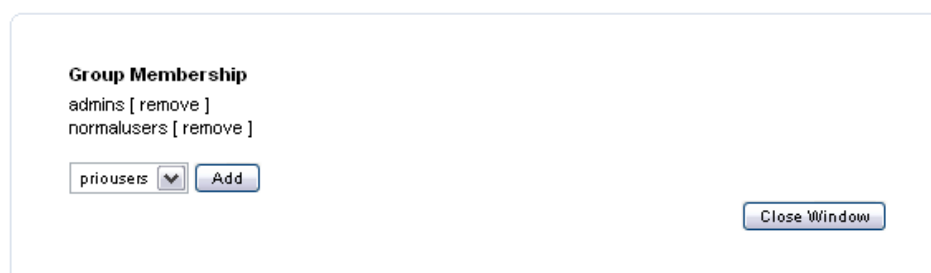


Note

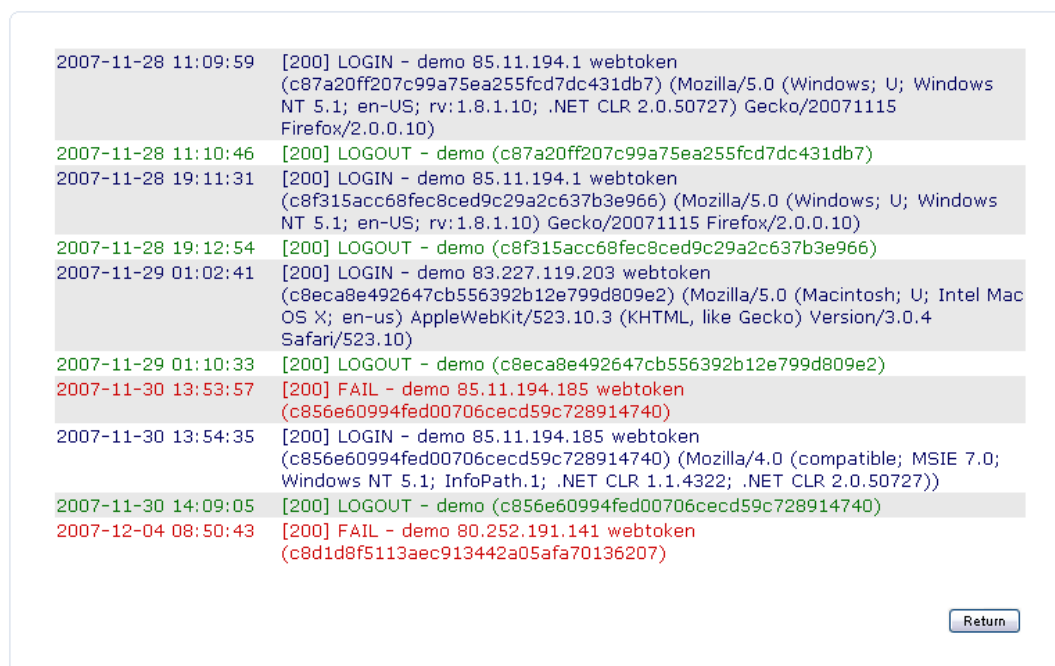
The options **Add a user to a new group** and **Delete this user** are only available if Clavister SAG uses the local database. If an external LDAP server is used, the administration interface for the LDAP server must be used to add and delete users and groups.

Change at Next Logon, Never Expires, and SMS Password is not shown if the user password from an external LDAP server is used. See Section 8.2, “Web Authentication” for more information.

The **Group Assignment** button assigns the user to different groups. A list of the groups the user is a member of are displayed. To include the user in a new user group, select the group from the drop down menu and click **Add**.



The **Last Activity** button displays a list of the user's latest activities.



The **View Allowed Menu Entries** button shows what menu entries this user can access when logging in, with different authentication methods is displayed. First, you have the possibility to fill in from which IP address the menu items should be available.

The Client IP Address can be used to check which menu items are available from a specific IP address. It can also be left blank...

Client IP Address:

If **Check** is pressed the dialog below appears, showing the menu entries the user is able to access.

The following menu entries are available for user **demo** from Any IP Address

Authentication Method - Basic

Control Center

Outlook Web Access

File Share

Remote Desktop

Network Connector

Clavister

Google

SSO Handler

User Settings

Change Password

Authentication Method - Webtoken

Control Center

Outlook Web Access

File Share

Remote Desktop

Demo FTP

SSH Tunnel

Network Connector

Clavister

Google

SSO Handler

User Settings

Change Password

Once the changes have been made to **Change User Settings** the options are:

- **Apply**
Save the settings without leaving the form.
- **Save**
Save the settings and leave the form.
- **Return**
Return to the previous page without saving anything.

Locked Accounts

An account can be locked if the user makes too many failed attempts to login.

This account is temporarily locked

User DN: cn=jasm,ou=users,dc=local
UniqueID (UID): jasm
Name: James Smith
Certificate User ID: (Format: YYYYMMDDXXXX)
e-Mail Address: smith.james@example.com
Comment:
Expires at:
Disabled:
Inline Navigator:

Web Token / Basic Enable
 Change at next logon
 Never expires

Web Password: Retype Password:

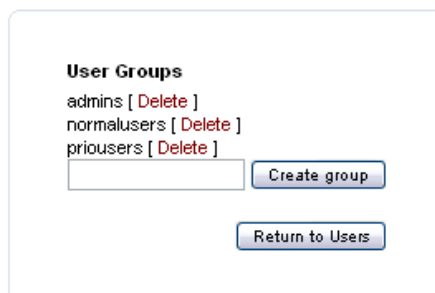
SMS Token Enable
 Change at next logon
 Never expires

SMS Password: Retype Password:
SMS Cellphone 1: SMS the password to the user.
SMS Cellphone 2:
SMS Cellphone 3:

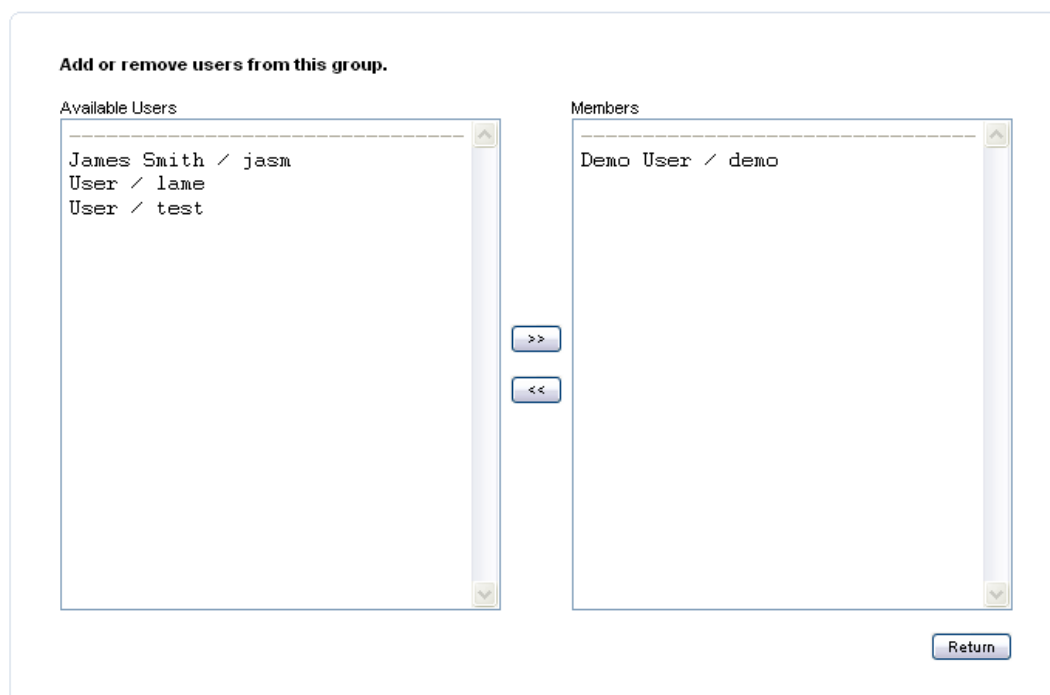
An account can be unlocked with the **Unlock this user** button.

Manage Groups

With this function you can create new groups, delete groups and make users members or non-members of a group. This function is only available if Clavister SAG uses the local database. By default, no groups exist.



To delete a user from a group or assign a user to a group click on the group's name. A dialog similar to the following will be displayed.



Here you can see which members there are in the group and users available to add to the group. If you want to move a user between **Available Users** and **Members**, click on the user and on either >> or <<.

Import Groups

This function is only available if Clavister SAG uses an external LDAP directory. It is used to select which user groups from the external LDAP directory Clavister SAG should use. (See also Section 6.5, "Local Database Settings").



Note

Groups that have been removed from the imported list will NOT be removed from current Access rules etc. This has to be done manually.

4.2. Address Pools

Address pools are groups of addresses used to differentiate between clients connecting from different networks. The pools can for instance be used in the access control and in the individual timeout configuration.

Below is an example with three configured address pools.

These settings are unique for each Virtual Host.

Pool Name
 Secure Administration Network Delete

Add new pool...

To change the settings of an address pool, press its name. To add a new pool, press **Add new pool**.

Figure 4.2. New Address Pool

Pool Name

Single Addresses, Networks & Address Ranges
 It is possible to specify network addresses (eg 192.168.30.0/24),
 as a range of addresses within a C-class network (eg 192.168.10.16-89)
 or as a single IP address (eg 192.168.92.8)

(Network Address)

The settings are:

- **Pool Name**
The name of the address pool.
- **Single Addresses, Networks & Address Ranges**
An address pool consists of lines defining the addresses in the pool. Each line can be either the address of a network (for example *192.168.59.0/24*) a range of addresses in a C-class network (for example *192.168.58.101-250*) or as single addresses (form example *192.168.58.123*). If more fields are needed, press the **More Fields** button.

4.3. Resources

A resource is a service accessible via Clavister SAG. There are four different kinds of resources: Web Server (HTTP and HTTPS), FTP Server, Windows Share and Tunnel.

- **HTTP or HTTPS**
A Web Server may be accessed using HTTP or HTTPS (SSL). Please note that even if the data between Clavister SAG and the internal resource is sent in plaintext (HTTP), the data between Clavister SAG and the client is always encrypted.
- **FTP Server**
The FTP protocol is supported by Clavister SAG. This makes it possible to access a FTP server using Clavister SAG. FTP data will be converted to HTTPS data and then sent to the client.
- **Windows Share**
Clavister SAG can map windows network drives and publish the content on a regular web page. The data is encrypted and sent in the HTTPS protocol to the client.
- **Tunnel**
Clavister SAG supports services using other protocols than HTTP and FTP, e.g. SSH, Terminal Server, Citrix, pcAnywhere, etc. The communication between the client and Clavister SAG is encrypted using AES. Port 443 is used, as for HTTPS/SSL.

The tunnel makes it possible to run locally installed clients such as SSH, Terminal Server, Citrix, etc. Terminal Server, Citrix and VNC are also available as Active-X or Java clients and are bundled with Clavister SAG.

4.3.1. Resource Administration

A list of all available resources is presented in the administration interface:

These settings are unique for each Virtual Host.

Name	URL	ACL
clavistercom	http://www.clavister.com:80	Yes
demo-ftp	ftp://ftp.clavister.com:21	Yes
demo-owa	http://webmail:80	Yes
demo-smb	smb://192.168.101.40/resources	Yes
google	http://images.google.se:80	Yes
localssh	tunnel://127.0.0.1:22	Yes
remote-desktop	tunnel://192.168.101.40:3389	Yes

Add new resource...

To change the settings of a resource, press the name of the resource. The settings are:

- **Name**
The resource name which must be unique and can NOT contain any special characters or white space.
- **URL**
This is information for the administrator to easily get an overview of all resources.
- **ACL**
This is an indication if the access control is specified for the resource or not. It is also possible to click on the text to get directly to the access control for the specified resource.

Adding a New Resource

To add a new resource click on **Add new resource**.

Adding new Resource

Please specify name and type for the new resource. The name is an internal name and is not used by the end user.

Name:

Description:

Type: ▼

Enter a name, description (optional) and select a type for the new resource and click on the **Next>** button.

The **Type** can be one of:

- **HTTP**
Web server without encryption.
- **HTTPS**
Web server with encryption (SSL).
- **Tunnel**
Resource that uses TCP/IP or UDP/IP communication. Multiple ports are supported. To use multiple ports, use comma to separate the ports, for example: *tcp:80,tcp:81,udp:1500*.
- **FTP**
FTP Server.
- **Windows Share**
Windows Network Drive.

The next step will be adapted for the specified resource type selected. The following dialogs are available for the different types:

Configure HTTP Resource "PortalServer" a.k.a "Intranet"

Description:

Type:

The Server Address may be an IP Address or a DNS Name.
It can also be comma separated list of addresses or DNS Names.
This is useful when load balancing between several physical servers.

Example: *mail1.company.com,mail2.company.com,10.104.1.2*

Server Address:

The Port must be a single TCP port number.

Port:

It is possible to specify extra host names.
Separate multiple names with comma.

Example: *mail,mailserver,mail.company.com*

Hostnames:

Reversed Proxy: (Recommended)

Simple SID Proxy: (Use with care)

SSL Tunnel: (Requires Java on the client)

Quick Tunnel: (Requires Java on the client)

The Client Port is only used in the SSL Tunnel and Quick Tunnel modes.
It can be used to force a specific port on the client.
The Client port will be automatically assigned if it is set to 0.

Client Port:

The settings are:

- **Type**
Whether the internal server is a HTTP or HTTPS server.
- **Server Address**
The IP address of the server.
- **Port**
The port to use on the server.
- **Hostnames**
It is possible to specify a DNS or NetBIOS name if the web server requires a specific name in the **Host:** attribute in the HTTP protocol.

This is useful when running *Virtual Hosts* on the web server and the IP address is specified in the **Server Address** field. Multiple names can be specified (comma separated) in order to address translate many different names to a resource. This may be needed when running IIS on a windows system that uses NetBIOS names.

- **Reversed Proxy**
Reversed proxy is the normal mode for HTTP/HTTPS resources.
- **Simple SID Proxy**
The Simple SID mode can be used when third party programs shall access data on a web

resource. The session id will be visible in the URL. Use this option with care!

- **SSL Tunnel**
The data will use a dynamic tunnel to the internal resource and all URLs will be translated to localhost.
- **Quick Tunnel**
The same as the SSL Tunnel mode but without the SSL handshake. The data is still encrypted but the connection phase will be faster. This can be useful for client devices with limited capacity. Note: Some firewalls will not allow communication to Clavister SAG without a correct SSL handshake.
- **Client Port**
If one of the two modes **SSL Tunnel** or **Quick tunnel** is used, this textbox can be used to define a certain client port to use for the tunnel. If it is left blank, Clavister SAG will assign a port automatically.

Advanced Options for HTTP/HTTPS Resources

Advanced Settings

It is possible to specify a special pattern pool.
This is only needed in some special cases when the URL conversion of the web page fails.

Pattern Pool:

Search and Replace:

Content Types: Built in: Custom:

It is possible to specify a special User Agent that will be sent to the Web Server.
Leave this field blank to use the global setting for User Agent.

User Agent: Override:

Miscellaneous Settings

Extended Pipelining: (Gives increased performance on high latency connections)

Force Unique Pipelines: (May give increased performance when handling many small objects)

Disable Nagle's algorithm: (May give increased performance when handling many small objects)

Translate "_top": (This prevents web pages to overwrite the inline navigator)

Translate .ica files: (Communication Tunnels will be setup automatically for .ica files)

Cookie Pass-Through: (Allows this resource to set cookies directly on the client)

Accept Client Cookies: (Allows the client to send cookies to this resource)

Rewrite Request Header: (This rewrites the URI in every request)

URL Convert Posted forms: (Data posted in forms will be URL converted)

Inline URL Converter: (Rewrites URL's in data sent from Client to Server in one batch)

Allow Unknown Headers: (Allow transportation of all headers between client and server)

Send Custom Headers: (Custom Headers always starts with a X)

Authentication Control

SiteVision:

Force Basic:

Form based:

Normal:

The advanced options for HTTP/HTTPS resources are:

- **Pattern Pool**

If there are problems with the URL conversion in a http/https resource, another pattern pool can be selected. Pattern pools are configured in **Server Settings > URL Converter**.

- **Search and Replace**

The Search and Replace settings are used to configure special strings to be translated into other strings before it is sent to the client. Click the text to open the Search and Replace dialog.

Search and Replace
 It is possible to specify search and replace strings. This can be useful when some javascripts shall be disabled or invalid host names are used by the resource.

Parameters can be used in the Replace string. The following extra parameters are available:
 PARM(mgresourceurl) and PARM(mgtunnelport)

Useful normal parameters are: PARM(mgnodeprefix) and PARM(mghostname)

Search for	Replace with
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

- **Content Types**

If the *Built in* option is checked, Clavister SAG uses the Types shown below. The *Custom* option should be checked to add or delete Types.

Advanced Settings

It is possible to specify a special pattern pool.
 This is only needed in some special cases when the URL conversion of the web page fails.

Pattern Pool:

Search and Replace: Configure custom Search and Replace patterns

Content Types: Built in: Custom:

text/html

text/xml

text/css

application/x-javascript

It is possible to specify a special User Agent that will be sent to the Web Server.
 Leave this field blank to use the global setting for User Agent.

User Agent Override:

- **User Agent Override**

This setting can be used to define a special user agent string to send to the web server.

- **Extended Pipelining**

Gives increased performance on high latency connections. If problems with SSO, keep

unchecked.

- **Force Unique Pipelines**
Force unique pipelines, even if the browser doesn't request listitem. This may speed up the transfer of many small objects on a webpage.
- **Disable Nagle's Algorithm**
Immediately send data even if the send buffer isn't full. This may also speed up the transfer of many small objects on a webpage.
- **Translate "_top"**
If this checkbox is checked, Clavister SAG will translate all `target="_top"` within HTML pages, to prevent the page to overwrite the inline navigator.
- **Translate .ica files**
If this checkbox is checked, Clavister SAG will translate all Citrix ICA files from the web server. This means that if Clavister SAG finds a server address that can be matched to a specified resource in Clavister SAG, then the address will be rewritten to `127.0.0.1` in order to tunnel the ICA protocol through Clavister SAG. This is very useful if running a Citrix web interface.

**Note**

All Citrix MetaFrame servers must be specified as tunnel resources and the ICA file can NOT include information about a Browser Server.

- **Cookie Pass-through**
If Cookie Pass-Through is selected, the web resource is allowed to set cookies directly on the client, something that might be necessary for some types of servers. Left unchecked, Clavister SAG handles all resource cookies internally.
- **Rewrite Request Header**
Rewrites URL data in the request URI.
- **URL Convert Posted Forms**
If selected, data posted in forms will be URL converted before it is sent to the server. This is required for some web servers when uploading files.
- **Inline URL Converter**
If the Inline URL Converter is used, data sent from the client will be sent in one batch. This is required for some types of servers that cannot properly handle chunked data.
- **Allow Unknown Headers**
This option allows unknown HTTP headers to be sent between the client and the server. Normally, Clavister SAG only handles known headers. This option is only needed in some rare occasions.

**Note**

Headers starting with X will never be passed from the client.

- **Send Custom Headers**
This option allows custom headers to be sent to a web resource. The web resource must be able to handle X-headers. An example is shown below.

Extended Pipelining:	<input type="checkbox"/>	(Gives increased performance on high latency connections)
Force Unique Pipelines:	<input type="checkbox"/>	(May give increased performance when handling many small objects)
Disable Nagle's algorithm:	<input type="checkbox"/>	(May give increased performance when handling many small objects)
Translate "_top":	<input checked="" type="checkbox"/>	(This prevents web pages to overwrite the inline navigator)
Translate .ica files:	<input type="checkbox"/>	(Communication Tunnels will be setup automatically for .ica files)
Cookie Pass-Through:	<input type="checkbox"/>	(Allows this resource to set cookies directly on the client)
Accept Client Cookies:	<input checked="" type="checkbox"/>	(Allows the client to send cookies to this resource)
Rewrite Request Header:	<input type="checkbox"/>	(This rewrites the URI in every request)
URL Convert Posted forms:	<input type="checkbox"/>	(Data posted in forms will be URL converted)
Inline URL Converter:	<input type="checkbox"/>	(Rewrites URL's in data sent from Client to Server in one batch)
Allow Unknown Headers:	<input type="checkbox"/>	(Allow transportation of all headers between client and server)
Send Custom Headers:	<input checked="" type="checkbox"/>	(Custom Headers always starts with a X)

Header	Value
X	
X	
X	
X	
X	
X	
X	
X	
X	
X	
X	
X	

Authentication Control

SiteVision:

Force Basic:

Form based:

Normal:

- Authentication Control**
 Authentication Control allows the administrator to configure special authentication settings to enable Single Sign-On for a resource.
- SiteVision**
 Enables SSO for SiteVision. Make sure the SiteVision server is configured to use authentication that is set to be **Clavister SAG**.

SiteVision:

Force Basic:

Form based:

Normal:

Username:

Password:

Send Session ID:

- Force Basic**
 If this feature is activated, Clavister SAG automatically authenticates the user to the internal resource using BASIC headers, even if no request for authentication has been sent from the server. This can be used for web servers that accept BASIC authentication headers but do not send any "Authentication Required" replies. Which credentials to use are defined in the controls below (see Appendix B, *Parameters*).
- Form Based**
 If form based authentication is activated, Clavister SAG posts parameters to the internal resource every time the menu entry is clicked. To find out how to configure form based authentication for a particular web server, open the html code of the authentication page and look for the login form. The Post URI is the URI where the data should be posted, look for the **action** tag for the form. The data to post is defined in the **Attribute** and **Value** fields. Look for **input** tags for the form. Add the **name** of the input tags in the **Attribute** fields and whatever information should

be posted in the **Value** fields.

- **Prefetch Data**

The prefetch feature can be used to fetch information from a log in page to be posted together with the other authentication information.

Example 1. Form Based SSO without prefetch: if this is the form part of the web page:

```
<form action="login.php">
<input type="text" name="user_name" value="" />
<input type="password" name="user_password" value="">
</form>
```

This is how the resource could be configured:

SiteVision:	<input type="radio"/>								
Force Basic:	<input type="radio"/>								
Form based:	<input checked="" type="radio"/>								
Normal:	<input type="radio"/>								
<hr/>									
Prefetch Data:	<input type="checkbox"/>								
<hr/>									
Post URI:	<input type="text" value="login.php"/>								
Parameters:	<table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>user_name</td> <td>PARM[gwuid]</td> </tr> <tr> <td>password</td> <td>PARM[gpwprd]</td> </tr> <tr> <td></td> <td></td> </tr> </tbody> </table>	Attribute	Value	user_name	PARM[gwuid]	password	PARM[gpwprd]		
Attribute	Value								
user_name	PARM[gwuid]								
password	PARM[gpwprd]								

See Appendix B, *Parameters* for more information about the parameters that can be used.

Example 2. Form based SSO with prefetch: if this is the form part of the web page:

```
<form action="login.php">
<input type="text" name="user_name" value="" />
<input type="password" name="user_password" value="">
<input type="hidden" name="session_id" value="1213AEF21251BBE1">
<input type="hidden" name="language" value="en">
</form>
```

In this case we need to post the **session_id** and the **language** fields to the POST URI. To configure the prefetch, regular expressions are used. This is an example of how the resource could be configured.

Prefetch Data:	<input checked="" type="checkbox"/>								
Prefetch URI:	<input type="text" value="login.php"/>								
Max Prefetch Size:	<input type="text" value="10240"/> Bytes								
Search Patterns:	Regular Expression								
	<input type="text" value="<input type='hidden' name='session_id' value='(/S+)'/>"/>								
	<input type="text"/>								
	<input type="text"/>								
	<input type="text"/>								
	<input type="text"/>								
<hr/>									
Post URI:	<input type="text" value="login.php"/>								
Parameters:	<table border="1"> <thead> <tr> <th>Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>user_name</td> <td>PARM[gwuid]</td> </tr> <tr> <td>password</td> <td>PARM[gwpwd]</td> </tr> <tr> <td>session_id</td> <td>PARM[gwregexp1]</td> </tr> </tbody> </table>	Attribute	Value	user_name	PARM[gwuid]	password	PARM[gwpwd]	session_id	PARM[gwregexp1]
Attribute	Value								
user_name	PARM[gwuid]								
password	PARM[gwpwd]								
session_id	PARM[gwregexp1]								

**Note**

Only one regular expression can be used on each search pattern line.

Tunnel Resources

Configure Tunnel Resource "server-rdp" a.k.a "RDP"

Description:

The Server Address may be an IP Address or a DNS Name.
It can also be comma separated list of addresses or DNS Names.
This is useful when load balancing between several physical servers.

Example: mail1.company.com,mail2.company.com,10.104.1.2

Server Address:

It is possible to specify multiple TCP and/or UDP ports.
Syntax for TCP Ports: <port number> or tcp:<port number>
Syntax for UDP Ports: udp:<port number>

Example: 1080,tcp:6667,udp:5553

Ports:

Skip SSL handshake: (This can be used to minimize the traffic on GPRS connections)

- **Server Address**

In the case of tunnel resources, the server address might be defined either as a single IP address or as a comma separated list of IP addresses. If more than one address is defined Clavister SAG will spread the load over the servers by assigning the different addresses in a round robin fashion.

**Note**

One user session will always use one IP address.

- **Ports**

The port or ports to enable tunneling for on the server. Which client ports to use are defined in the settings for each menu entry.

Authentication Control

Single Sign On does currently work with the Terminal Server web client (if the server is configured properly) and the Citrix Java client

NOTE: When using Single Sign on for tunnels, the user password will be readable in the HTML source.

Allow Single Sign On:

- **Allow Single Sign On**

This feature enables Single Sign-On for terminal server resources and for resources using the Citrix Java client.

**Note**

The administrator should be aware that since the log on credentials are sent to the client machine, it might theoretically be picked up by malicious software.

Figure 4.3. FTP Resources

Configure FTP Resource "demo-ftp" a.k.a "FTP Server"

Description:

The Server Address may be an IP Address or a DNS Name.
It can also be comma separated list of addresses or DNS Names.
This is useful when load balancing between several physical servers.

Example: mail1.company.com,mail2.company.com,10.104.1.2

Server Address:

The Port must be a single TCP port number.

Port:

Figure 4.4. Windows Share Resources

Configure Windows Share Resource "demo-smb" a.k.a "Fileshare"

Description:

The Server Address may be an IP Address or a DNS Name.
It can also be comma separated list of addresses or DNS Names.
This is useful when load balancing between several physical servers.

Example: mail1.company.com,mail2.company.com,10.104.1.2

Server Address:

Specify the share name to connect to.

Share name:

4.3.2. Access Control

Clavister SAG uses Access Control Lists (ACL) for authorization. Authorization is based on group, encryption grade, IP address, date and time and authentication method. If the resource is a web server the access is also based on path. Each resource has its own ACL.

Figure 4.5. An Access Control List

These settings are unique for each Virtual Host.

Resource	Type
clavistercom	Web Server
demo-ftp	FTP Server
demo-owa	Web Server
demo-smb	Windows Share
google	Web Server
localssh	Tunnel
portalserver	Not Configured
remote-desktop	Tunnel

Local Services

- Control Center
- Message Center
- Network Connector
- About
- Change Web Token Password
- Change SMS Token Password
- Change Internal Password
- Remote Assistance
- User Settings
- SSO Handler

- **Resource**
The figure above shows a list of all resources. A resource without access control rules will be of type **Not Configured**. A not configured resource is not accessible for users.

Click on a resource to change the ACL rules for that resource.

- **Type**
This indicates the type of resource or **Not Configured** if the resource does not have any access rules.

- **Clavister SAG Services**
Here, the access control policies of Clavister SAG's own services can be administered. Click on the service for which you wish to add/change the ACL. Refer to the particular section below for the Control Center ACL.

ACL Rules

The ACL rules for a resource are presented in a list. Please note that rules can only allow access, never deny access.

Figure 4.6. ACL for a Web and FTP Server

Group	Auth.	Enc.	Destination Path	SSO	Restrict	IP Address	Time
Any	Any	None	Any	No	No	Any	
Add new rule...							<input type="button" value="Return"/>

Figure 4.7. ACL for a Tunnel

Group	Auth.	Enc.	IP Address	Time
Any	Webtoken	None	Any	
Add new rule...				<input type="button" value="Return"/>

The settings displayed are:

- **Group**
Sets the group for this rule. Only one group per rule is allowed as well as Any group.
- **Auth**
Sets the authentication method for this rule. The rule will only match users logged in with this method. For example if SMS Token is set, this rule will only authorize users authenticated with SMS Token. **Any** is also allowed in order to accept any authentication method for the specified group. as well as authentication groups. See Section 8.4, "Authentication Groups" for more information.
- **Enc**
Sets the minimum encryption grade. There are five levels of encryption grade:
 - **Very high** - 256 bit AES
 - **High** - 128 bit or longer key length.
 - **Medium** - 56 to 127 bit key length.
 - **Low** - 40 to 43 bit key length.
 - **None** - Clear text.



Note

The weaker encryption grades also include the stronger encryption grades, for example if a rule is set to match the Low encryption grade it will also match the

Medium and High encryption grades.

- **Destination Path**
With the setting Destination Path it is possible to restrict access to a certain directory and its subdirectories. This setting is only valid for Web resources, FTP resources and windows shares.
- **SSO**
If activated, Clavister SAG will store logon information for this resource. A user will only need to authenticate to the resource once. The next time the user access the resource, Clavister SAG will automatically authenticate the user to the resource. SSO using other than NTLM or Basic requires the resource to be configured for that. This can be done in the Advanced Options section for the resource.
- **Restrict**
This makes it possible to restrict the Single Sign On feature. This setting can be any of the following:
 - **No**
The user can enter his or her user name.
 - **SAG UID**
The user can not enter his or her user name. The user's Clavister SAG user name is always used.
 - **First UID**
The user can only enter his or her user name the first time. After a successful login, the user name will be locked to this user name.
- **IP Address**
Specified if the access shall be restricted to any IP Address Pool.
- **Time**
Specifies if the access shall be restricted to specific time or date. Click Time to open the window below.

Day	All	None	Range	From	Until
Monday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Tuesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Wednesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Thursday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Friday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Saturday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Sunday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00

(YYYY-MM-DD)

Valid From: 2007 - 12 - 06 From Any Date

Valid Until: 2007 - 12 - 06 Until Forever

Create a New Access Rule (ACL)

Use the resource list to click on the resource you want to configure, then click on the **Add new Rule**. A new rule field will then be shown at the bottom of the ACL list.

The screenshot shows a configuration form with the following fields and values:

Group	Auth.	Enc.	IP Address	Time
Any	Webtoken	None	Any	

The 'Auth.' dropdown menu is open, showing the following options: Any, Anonymous, Basic, Web Token, SMS Token (highlighted), 1-Way, 2-Way, and Any. There are 'Save' and 'Cancel' buttons at the bottom right of the form.

Edit or Delete an Access Rule

To edit a specific access rule, click on the rule. It is then possible to edit or delete the rule.

The screenshot shows the same configuration form as above, but with the 'Delete' button highlighted and a mouse cursor pointing to it. The 'Auth.' dropdown menu is now closed and shows 'Any'.

Access control for Control Center

With this function the administrator is able to create different settings for different users that must have access to different functions in Control Center.

Examples of different types of settings are.

- One user must be able to list all users but cannot see anything else in Control Center.
- One user must be able to list all users and make changes but cannot see anything else in Control Center.
- The administrator is able to see everything and make changes to everything in Control Center

Click **Control Center** in the ACL.

The menu shown below appears.

The screenshot shows a simple menu with two options:

- Access Control Groups...
- Access Control...

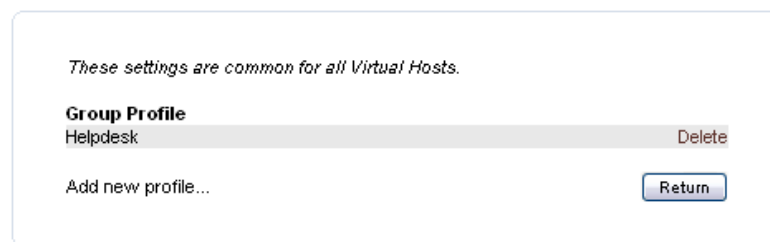
These two options are now discussed.

The *Access Control Groups* option

The option for Access Control Groups are:

- Click the name of a Group Profile to change the settings for that group.
- Click **Add new profile** to create a new access control group.
- Click **Delete** to delete the group.

Figure 4.8. Access Control Groups



In the example below, a group called *Helpdesk* is created. Users using this profile will be able to view and change settings for users as well as view and kill sessions.

The *Access Control* option

Below, the profile *Helpdesk* is being created.

Profile Name
Helpdesk

All
 View All Administrate All

Monitoring
 View Sessions Kill Sessions
 Read SSO Handle SSO
 View Logs Administrate Logs
 View Statistics Handle Remote Assistance

Administration
 View Users and Groups Administrate Users and Groups
 View Imported Groups Administrate Imported Groups
 View Address Pools Administrate Address Pools
 View Resources Administrate Resources
 Administrate Control Center ACL

Authenticator
 View Authenticator Administrate Authenticator

Server Settings
 View Server Settings Administrate Server Settings

Client Settings
 View Client Settings Administrate Client Settings

Authentication
 View Authentication Administrate Authentication

Maintenance
 Install Licence
 Upgrade Product
 Backup Product
 Browse Filesystem

Activate Changes
 Reload Configuration
 Reindex Files
 Restart Service

The control center view for the *Helpdesk* group is shown below.

Group	Auth.	Enc.	IP Address	ACL Group	VHost	Time
admins	Any	None	Any	No Restrictions	Any	
Any	Any	High	Any	Helpdesk	Any	

- Group**
The user group that will use the settings in the profile.
- Auth**
The authentication method the users in the user group must log in with (at least) to be able to use the settings in the profile.
- Enc**
The encryption the users in the user group must use (at least) when they log in.
- IP Address**
Specifies which IP address (from the Address Pools) the user must log in from to be able to use the settings in the profile.
- ACL Group**
The name of the profile the user group should use.
- VHost**
The Virtual Host that the settings in the profile are valid for.



Note

The **Control Center View of Helpdesk** (see above) is always visible for all virtual hosts to users that have any access to the Control Center.

- Time**
Specifies if the access shall be restricted to a specific time or date. See previous chapters for usage.

4.3.3. Cache Control

In the Cache Control it is possible to control the data cached by the clients. The data that can be cached depends on the resource, current directory, and/or file type.



Note

If cache control has been changed for the resource local, the files have to be reindexed. This is done in the **Activate Changes** section.

These settings are unique for each Virtual Host.

Resource	Path	Cache type
gw-local	/drawboard/drawboard.cab	cache
gw-local	/drawboard/drawboard.jar	cache
gw-local	/ica/JICA-cdmM.cab	cache
gw-local	/ica/JICA-cdmN.jar	cache
gw-local	/ica/JICA-clipboardM.cab	cache
gw-local	/ica/JICA-clipboardN.jar	cache
gw-local	/ica/JICA-configM.cab	cache
gw-local	/ica/JICA-configN.jar	cache
gw-local	/ica/JICA-coreM.cab	cache
gw-local	/ica/JICA-coreN.jar	cache
gw-local	/ica/JICA-printerM.cab	cache
gw-local	/ica/JICA-printerN.jar	cache
gw-local	/ica/JICA-seamlessM.cab	cache
gw-local	/ica/JICA-seamlessN.jar	cache
gw-local	/ica/JICA-tw1M.cab	cache
gw-local	/ica/JICA-tw1N.jar	cache
gw-local	/ica/activex/connect.ica	cache
gw-local	/ica/activex/wfica.cab	cache
gw-local	/ica/activex/wficac.cab	cache
gw-local	/mgnc-install.exe	cache
gw-local	/mgnc-osx.tar.gz	cache
gw-local	/softtokens.jar	cache
gw-local	/ssh/fta20.cab	cache
gw-local	/ssh/fta20.jar	cache
gw-local	/ssh/fta25.jar	cache
gw-local	/ssh/putty.exe	cache
gw-local	/startapplication.cab	cache
gw-local	/startapplication.jar	cache
gw-local	/terminalserver/connect.rdp	cache
gw-local	/terminalserver/msrdp.cab	cache
gw-local	/testjava.jar	cache
gw-local	/tunnel.cab	cache
gw-local	/tunnel.jar	cache
gw-local	/vnc.exe	cache
gw-local	/vnc/tightvncviewer.cab	cache
gw-local	/vnc/tightvncviewer.jar	cache
gw-local	/vnc/vncviewer.cab	cache
gw-local	/vnc/vncviewer.jar	cache

Add new rule...

The actions that can be taken are:

- Click on the resource to edit a cache rule.
- Click on **Add new rule** to create a new rule.

The settings in the dialog are:

- **Resource**
The resource the rule is valid for.

- **Path**
The full path to a file or just the type of file the rule is applied on, for example if the path is set to `/softtokens.jar` the specified file on the specified resource will match. If the path is set to `*.jpg` the rule is valid for all files ending with `.jpg`. It is also possible to set the cache type for all files on a resource, using `"*"`.

**Note**

It is not possible to set cache control on a specified directory.

- **Cache Type**
There are three types of cache options:
 1. If the type is *no-store* the data can only be cached in the web browsers memory.
 2. If the type is *cache*, data can also be stored on the disc.
 3. If the type is *private*, the browser may use the file (Internet Explorer can open it) but can not save it in the cache.

**Note**

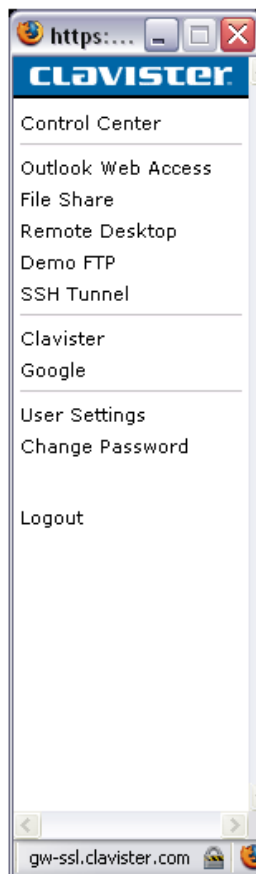
If no rule exists for a specific resource and path, then no files are allowed to be cached from that resource.

Cache Control Should be Enabled with Passive FTP

In order for "passive" FTP to function correctly through Clavister SAG, cache control should be enabled for FTP resources.

4.4. The Navigator

Shown below are the resources presented to the users after logon to Clavister SAG. This is opened in a separate window called the *navigator*.



The navigator display is adjusted for the specific user, so that only resources accessible to the user are included.

It is possible to let the user choose an "inline" navigator with the menu integrated into the browser window instead of appearing in a separate window.

Settings for user: jasm

Use inline navigator:



Note

The menu is not generated when resources are created. The administrator must specify each one of the menu entries.

Users that have installed pop-up blocking software may not be able to see the navigator menu if not using inline navigator without unblocking the navigator window.

Autostart and Autostart Navigator

It is possible to have a resource start automatically when a user logs on. This is useful since many users will often use a certain resource every time they log on, for example their web mail.

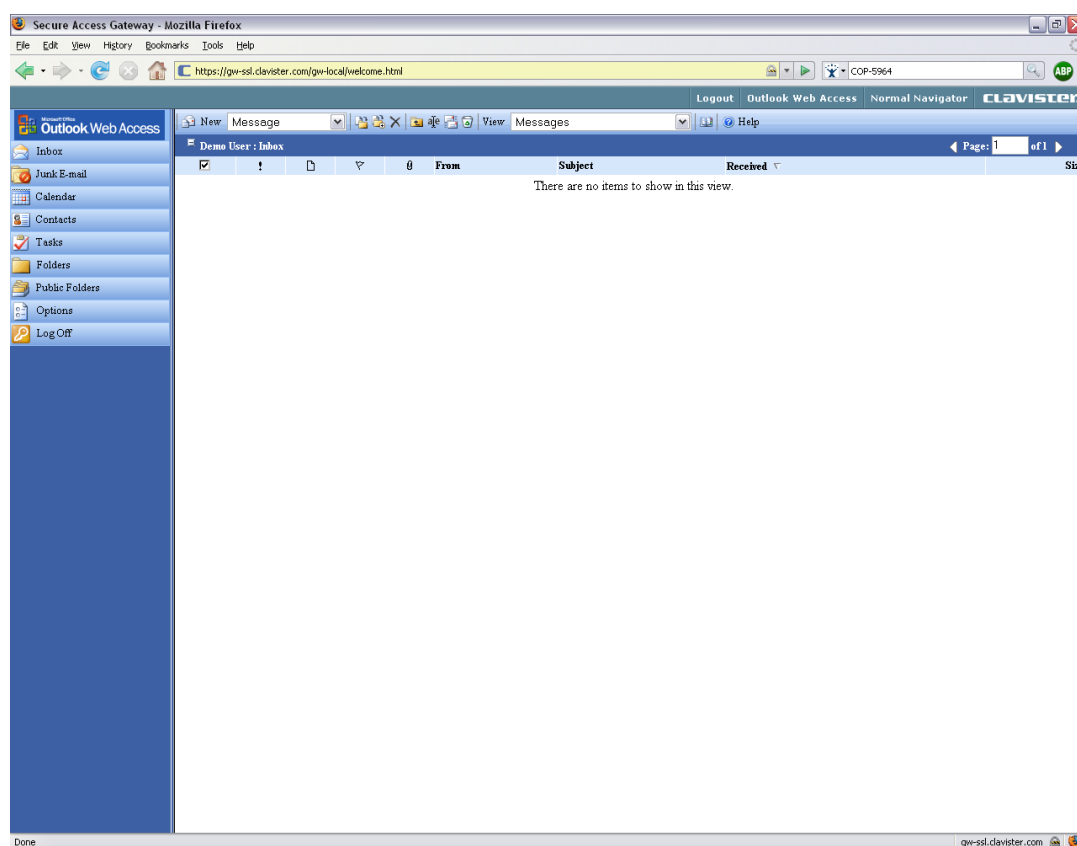
It is possible to have a smaller menu appear in the top of the browser when using autostart. This smaller menu is called the *autostart navigator*. It can contain a few of the most frequently used menu items. Setup of the autostart feature and defining the autostart navigator is done when specifying the menu items.

Since the autostart navigator is only one line high, the user might need the normal navigator also. To get a normal navigator, the user can press the **Normal Navigator** in the autostart menu.



Note

It is not possible to choose the inline navigator when using the autostart navigator.



Dynamic Autostart

It is possible to autostart an internal resource, for example a webpage, from an external webpage. The link to the internal resource on the external webpage looks like:

```
http://sag.server.name.com/sag-local/autostart?
  resource=<resourcename> &uri=<the uri>&formfill=<true|false>
```

An example might be:

```
http://login.foretaget.se/sag-local/autostart?resource
  =intranet&uri=/&formfill=false
```


When the link is clicked on the external webpage, the web browser redirects to the Clavister SAG login page.

The user logs in to Clavister SAG and if the user is authenticated the browser will directly show the internal resource.

It is also possible to specify the authentication method in the link. For example:

```
http://demo.mobilityguard.se/mg-local/autostart?
resource=webmail&uri=/exchange/&logintype=webtoken,smstoken
```

```
http://demo.mobilityguard.se/mg-local/autostart?
resource=webmail&uri=/exchange/&logintype=webtoken
```



Note

If dynamic autostart is used there will be no menu (navigator) available to the user. This means that no log out button will be available. This could be handled using search/replace for the auto-started resource.

4.4.1. Creating New Menu Entries

Click on **Add new entry** to start a guide to create menu entries.

Figure 4.9. Creating New Menu Entries

These settings are unique for each Virtual Host.

Menu entry	Resource	Move
Control Center		Move
Message Center		Move
-----		Move
Outlook Web Access	demo-owa	Move
File Share	demo-smb	Move
Remote Desktop	remote-desktop	Move
Demo FTP	demo-ftp	Move
SSH Tunnel	localssh	Move
Network Connector		Move
-----		Move
Clavister	clavistercom	Move
Google	google	Move
-----		Move
SSO Handler		Move
User Settings		Move
Change Password		Move
Add new entry...		



Note

There are special resources created by Clavister SAG. Access rules and menu entries should be added for some of these resources.

The following special resources can be found in the menu guide:

- Control Center
- Message Center

- Change SMS Token Password
- Change Web Token Password
- Change Internal Password
- User Settings
- SSO Handler
- About Clavister SAG
- Remote Assistance
- Menu Separator

The menu guide is different for each resource type. The following sections contain step by step guides to create menu entries for different resource types.

A. Create a Menu Entry for a Web or FTP Resource

For this example, a resource called Web mail is used. It runs on the internal server `webmail.company.com` and will be made accessible via Clavister SAG. The start page for Web mail is `http://webmail.company.com/webmail/index.html`.

We assume that the ACL rules are set correctly. This example only shows how to set up a menu entry.

Step 1.

Choose the resource to which you want to add a menu entry. The resource mail is chosen for this example.



Select the resource to add a menu entry for:

clavistercom

Cancel Next >

Step 2.

Now specify if the menu entry should link to a subdirectory or a specific file. In the example, the path is set to: `webmail/index.html`.



Adding Web Server Resource for host 'clavistercom'.

If you wish to link to a special path or page on the web server you can enter it below. This is optional, and if left blank the servers root path will be used.

`http://www.clavister.com` products/

< Back Cancel Next >

Step 3.

Type the name of the menu entry. This name will be presented to the users. Keep the name short to

avoid unnecessary line feeds in the navigator. It is also possible to specify a group for application autostart and if this menu entry shall be visible in the autostart navigator. You can also specify to which OS the menu entry should be visible for, and if you want the menu entry to open a new window.

Enter a description for this menu entry.

This text will be displayed in the navigation window, so it's recommended to keep it short.

Description

If you specify a group below, then this menu entry will be selected instead of the welcome page for every users that is a member of the specified group.

Autostart Group

It is also possible to select that this menu entry shall be visible in the special Autostart Navigator.

Hide Navigator

Autostart Navigator

You can choose to hide this menu entry for all operating systems except the one specified here if you specify Windows, then this menu entry will only be shown to client running windows. The operating system name is the same as shown in the session list for a user.

Leave the field blank to allow this entry on all operating systems

Only for OS

You can choose to open this menu entry in a new window. Even if the inline navigator or the autostart navigator are active

Open in new window

Click **Next**. The menu entry is now created and can be found at the bottom of the menu entry list. The position of the menu entry can be changed, see **Move** in the section **Change view order**.

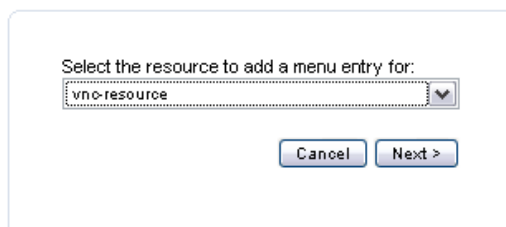
The new entry '**Clavister**' has been successfully added to the menu.

B. Create a Menu Entry for a Communication Tunnel

In this example a resource called *vnc* is used. It runs on the internal server *server.company.com*. The resource is made accessible via Clavister SAG. The remote access service Virtual Network Computing (VNC) must use port 5900.

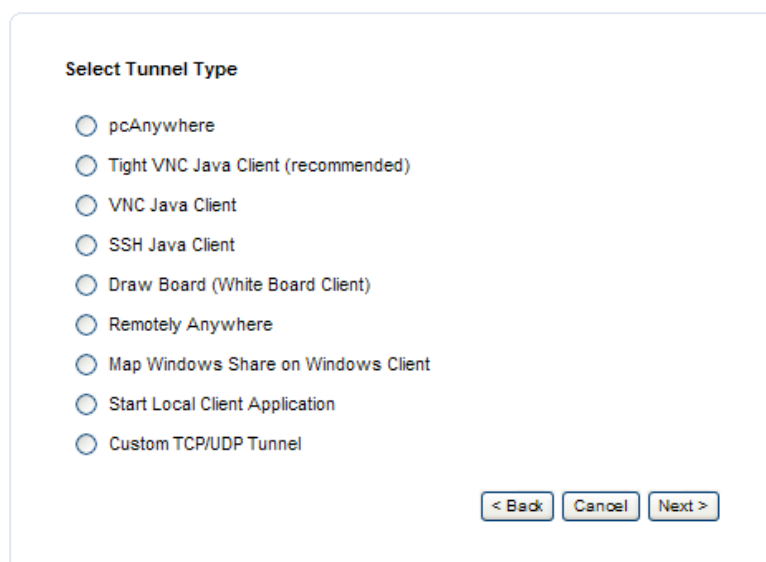
Step 1.

Choose the resource to which you want to add a menu entry. In this example *vnc* is chosen.

**Step 2.**

Clavister SAG provides templates for standard application and protocols, for example Citrix ICA, Terminal Services, pcAnywhere, VNC, SSH and others. If there is no template for a certain service, **Custom TCP/UDP Tunnel** can be used. In the example it is suggested to use **Tight VNC Java Client (recommended)**. This template provides a Java applet, which requires no installation of a client on the user's machines.

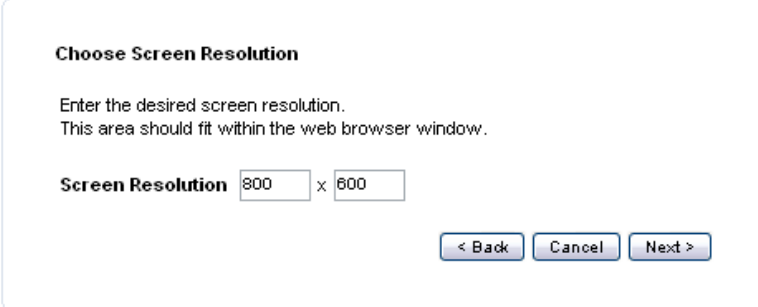
It is suggested to use a template based on the port specified for the resource.

**Step 3.**

The **Tight VNC Java Client** allows extra parameters to set the window size. Please use small or normal resolutions, otherwise users with normal resolutions will not be able to see the whole window. A good choice is 800x624 pixels. The reason to increase the height with 24 pixels is that the Java Applet has a tool bar which is 24 pixels high.

**Note**

The resolution should be the same as the console resolution on the server (plus an additional 24 pixels in the height).



Choose Screen Resolution

Enter the desired screen resolution.
This area should fit within the web browser window.

Screen Resolution x

Step 4.

Type the name of the menu entry. This name will be presented to the users. Keep the name short to avoid unnecessary line feeds in the navigator. Also choose that the user must accept all incoming connections to the tunnel. This is used to prevent access by malicious programs to the tunnel since the user has to accept all connections. Then select autostart options described in a previous example. Finally configure options **Only for OS** and **Open in new windows** as described above.

The name for the menu entry is set to *VNC* and the dialog is set to *Yes* which means that the user must accept every incoming connection to the tunnel.

Enter a description for this menu entry.

This text will be displayed in the navigation window, so it's recommended to try keeping it short.

Description

Also choose if the user should be asked to accept or deny every connection made to the tunnel.

Dialog

If you specify a group below, then this menu entry will be selected instead of the welcome page for every users that is a member of the specified group.

Autostart Group

It is also possible to select that this menu entry shall be visible in the special Autostart Navigator.

Hide Navigator

Autostart Navigator

You can choose to hide this menu entry for all operating systems except the one specified here if you specify Windows, then this menu entry will only be shown to client running windows. The operating system name is the same as shown in the session list for a user.

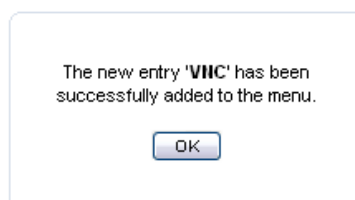
Leave the field blank to allow this entry on all operating systems

Only for OS

You can choose to open this menu entry in a new window. Even if the inline navigator or the autostart navigator are active

Open in new window

The menu entry is now created and can be found at the bottom of the menu entry list. The position of the menu entry can be changed using **Move** option as described later.



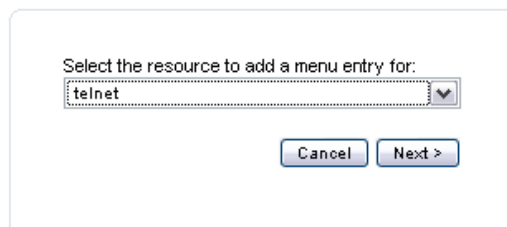
C. Create a Menu Entry for a Custom Tunnel Resource

In this example a resource called *telnet* running on the internal server *telnet.company.com* is used. The resource should be made accessible via Clavister SAG. The Telnet protocol uses port 23.

It is assumed that the ACL rules are already set. This example shows only how to create a menu entry.

Step 1.

Choose the resource to which you want to add a menu entry. For this example telnet is chosen.



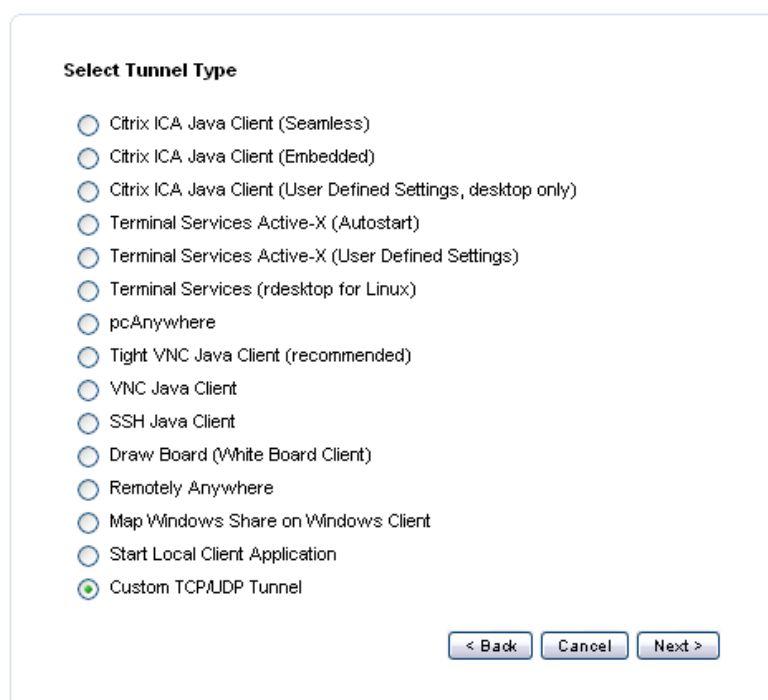
Select the resource to add a menu entry for:

telnet

Cancel Next >

Step 2.

As there is no template for Telnet, Clavister SAG suggests **Custom TCP/UDP Tunnel**.



Select Tunnel Type

- Citrix ICA Java Client (Seamless)
- Citrix ICA Java Client (Embedded)
- Citrix ICA Java Client (User Defined Settings, desktop only)
- Terminal Services Active-X (Autostart)
- Terminal Services Active-X (User Defined Settings)
- Terminal Services (rdesktop for Linux)
- pcAnywhere
- Tight VNC Java Client (recommended)
- VNC Java Client
- SSH Java Client
- Draw Board (White Board Client)
- Remotely Anywhere
- Map Windows Share on Windows Client
- Start Local Client Application
- Custom TCP/UDP Tunnel

< Back Cancel Next >

Step 3.

The local Clavister SAG Tunnel client will open a port on the local computer to which the local telnet client can connect. Please note that ports under 1024 can cause problems in a UNIX / Linux environment due to access restrictions.

In this example the client port 2300 is used.



Choose Client Port(s)

Enter the local client port to listen to.
Ports below 1024 might cause problems with client side security restrictions.

Syntax: *tcp:3000* or *udp:3001* use comma to separate multiple entries.

Client Port(s) 1494

< Back Cancel Next >

Step 4.

Type the name of the menu entry. This name will be presented to the users. Keep the name short to avoid unnecessary line feeds. Also choose that the user must accept all incoming connections to the tunnel. This is used to prevent malicious programs to access the Tunnel since the user has to accept all connections. Then select autostart options described in a previous example.

Finally configure options **Only for OS** and **Open in new windows** as described above.

The name for the menu entry is set to *Telnet* and the dialog is set to *Yes* which means that the user must accept every incoming connection to the tunnel.

The menu entry is now created and can be found at the bottom of the menu entry list. The position of the menu entry can be changed, see **Move** in the *Change view order* section.



When a user wants to use the tunnel, they only need to start the Telnet client and then connect to 127.0.0.1 on port 2300. It is possible to use a special HTML page that describes how to start the Telnet client and also how to connect to the tunnel.

4.4.2. Edit a Menu Entry

Click on the menu entry you wish to edit and an edit view is shown. The edit view will look different depending on the resource type. An example of the edit view for the resource types HTTP and HTTPS is shown below:

Resource type	HTTP Resource
Description	<input type="text" value="Clavister"/>
URI	<input type="text" value="/gw-resource/clavistercom/"/>
Only For OS	<input type="text"/>
Autostart Group	No Autostart <input type="button" value="v"/>
Hide Navigator	<input type="checkbox"/>
Autostart Navigator	<input type="checkbox"/>
Open in a new window	<input type="checkbox"/>
<input type="button" value="Save/Update"/> <input type="button" value="Delete"/> <input type="button" value="Back"/>	

An example of the edit view for the resource type Tunnel (VNC) is shown below:

Resource type	VNC
Description	VNC
Client port(s)	5910
Connect page URI	/gw-local/vnc/vncviewer.html
Only For OS	
Connection Dialog	No <input type="button" value="v"/>
Autostart Group	No Autostart <input type="button" value="v"/>
Hide Navigator	<input type="checkbox"/>
Autostart Navigator	<input type="checkbox"/>
Open in a new window	<input type="checkbox"/>
Extra parameters (optional)	
Screen X Resolution	800
Screen Y Resolution	800
Parameter 3 (p3)	
Parameter 4 (p4)	
Parameter 5 (p5)	
Parameter 6 (p6)	
Parameter 7 (p7)	
Parameter 8 (p8)	
Parameter 9 (p9)	
Parameter 10 (p10)	
<input type="button" value="Save/Update"/> <input type="button" value="Delete"/> <input type="button" value="Back"/>	

The **Connect page URI** contains the path to the client that is started below the communication tunnel applet in the web browser. This page can be changed to a customized page if desired.



Note

The parameter names can differ depending on which template is used for the specific menu entry.

4.4.3. Change View Order

A new menu entry will always be positioned at the bottom of the menu entry list. It is often desirable to change its position, which can be done with the **Move** function. Below is a menu entry list.

These settings are unique for each Virtual Host.

Menu entry	Resource	Move
Control Center		Move
Message Center		Move
-----		Move
Outlook Web Access	demo-owa	Move
File Share	demo-smb	Move
Remote Desktop	remote-desktop	Move
Demo FTP	demo-ftp	Move
SSH Tunnel	localssh	Move
Network Connector		Move
-----		Move
Clavister	clavistercom	Move
Google	google	Move
-----		Move
SSO Handler		Move
User Settings		Move
Change Password		Move
VNC	vnc-resource	Move
Change SMS Token Password		Move
Change SMS Token Password		Move
Telnet	telnet	Move

Add new entry...

To edit a menu entry position click on **Move**. Arrows will appear to indicate where it is possible to insert the entry.

For example, if you like to move the menu entry *Telnet*, click on the link **Move** on the row where the entry *Telnet* is located.

These settings are unique for each Virtual Host.

Menu entry	Resource	Destination
Control Center		↕
Message Center		↕
-----		↕
Outlook Web Access	demo-owa	↕
File Share	demo-smb	↕
Remote Desktop	remote-desktop	↕
Demo FTP	demo-ftp	↕
SSH Tunnel	localssh	↕
Network Connector		↕
-----		↕
Clavister	clavistercom	↕
Google	google	↕
-----		↕
SSO Handler		↕
User Settings		↕
Change Password		↕
VNC	vnc-resource	↕
Change SMS Token Password		↕
Change SMS Token Password		↕
Telnet	telnet	↕

Click on an arrow to place the entry in another position in the list. The entry will be inserted above the selected line.

Change Web Token Password is changed to *Change Web Password* so that the text fits on one line without wrapping.

This is done by clicking on the **Change Web Token Password** text.

The screenshot shows a configuration dialog box titled "Change WebToken Password". It contains the following fields and controls:

- Resource type: Change WebToken Password
- Description: Change Web Password
- Only For OS: (empty text box)
- Autostart Group: No Autostart (dropdown menu)
- Hide Navigator:
- Autostart Navigator:
- Open in a new window:

At the bottom of the dialog are three buttons: "Save/Update", "Delete", and "Back".

Finally, a separator is inserted between *Your IMP Mailbox* and *PC-Anywhere test* by adding a new separator entry and then moving the new separator to the right location.

The screenshot shows a dialog box titled "Select the resource to add a menu entry for:". It contains a dropdown menu with the selected option "# Menu Separator". Below the dropdown are two buttons: "Cancel" and "Next >".

Select *# Menu Separator* and click **Next**.

The screenshot shows a confirmation dialog box with the text: "The new separator has been successfully added to the menu." Below the text is an "OK" button.

Chapter 5. The Authenticator

The authenticator sub-menu is only available if an authenticator license has been installed. The authenticator module turns the Clavister SAG server into a RADIUS capable authentication server.

Figure 5.1. The Authenticator Menu



RADIUS Settings



These settings are common for all Virtual Hosts.

Global Settings


Listen Port

Challenge Text

Invalid Login Text

- **Listen Port**
The UDP port which Clavister SAG will listen for RADIUS request on.
- **Challenge Text**
The challenge text that are sent to the RADIUS Client when an authentication request has succeeded.
- **Invalid Login Text**
The text that are sent to the RADIUS Client when an authentication request is invalid (If the user name or password are incorrect).

Authenticator Clients



These settings are common for all Virtual Hosts.

Name	IP Address	Shared Secret
server	10.4.0.123	---- Secret ----

Add new server...

- **Name**
The client's name, this can be any name.
- **Shared Secret** A shared secret that the client and Clavister SAG share to hide user passwords in the RADIUS requests etc.

- **Add new server** This text is clickable, and is used to add new RADIUS clients. To Edit a RADIUS Client, the administrator can click on the client name.

To edit a RADIUS Client, the administrator can click on the client name.

Chapter 6. Server Settings

- ▼ **Server Settings**
 - Appliance Settings
 - General Settings
 - Supervision Settings
 - Node Settings
 - Network Connector
 - LDAP Settings
 - URL Converter
 - Virtual Hosts

6.1. General Settings

Some general settings for Clavister SAG's basic functions are to be found here. Note that the information about virtual hosts will only be visible if virtual hosts are configured.

The settings below are common for all Virtual Hosts.

Certificate Settings

Default Hostname

Certificate File

Certificate Password

Log Settings

Log All Requests

Compress Log Files

Remove Old Log Files

Remove Log Files Older Than days

Miscellaneous Settings

Session Independent Resource Handling (Requires wildcard certificate)

Use Multiple Browser Windows

The following settings are unique for each Virtual Host.

SMTP Server

SMTP From Address

Language ▼

Group for Prioritized Users ▼

Preferred Internal Authentication ▼

Public Remote Assistance

Bind Session to Client IP Address

Forward client user-agent

Persistent Single-Sign-On

Javascript to open new windows

Certificate Settings

Information on the certificate Clavister SAG should use.

- **Default Hostname**
The DNS name Clavister SAG should use. For example: *webaccess.company.com*.
- **Certificate File**
Name and path to the SSL certificate file. The certificate must be in PKCS-12 format. We recommend that the certificate file is stored in the root directory. For example: *webaccess.company.com.p12*.
- **Certificate Password**
The certificate password, which is necessary in order for Clavister SAG to read the private key from the certificate. For example: *SeCrEt*.

Log Settings

It is possible to decide if everything should be written to log, and if log files should automatically be compressed or deleted after a certain time.

- **Log All Requests**
If not activated, only requests of type *text/html* will be written to the log. If activated every HTTP and HTTPS request will be written to log. The recommended option is deactivated.
- **Compress Log Files**
If activated, the log files will be compressed using *gzip*.
- **Remove Old Log Files**
If activated, the log files will be removed after *xx* days, see below.
- **Remove Log Files Older Than**
If the **Remove Old Log Files** option is activated, Clavister SAG will remove all log files older than the time specified here.

Miscellaneous Settings

- **Session Independent Resource Handling (SIRH)**
This option makes it possible to access several internal web resources simultaneously without any loss of performance or functionality. This option is required when running a Clavister SAG cluster.

An extra DNS record has to be assigned to the DNS server in order to setup SIRH. For example if the Clavister SAG server is named *login.company.com* there has to be two DNS records. The first will handle *login.company.com* and the second will handle **.login.company.com*. The DNS records shall point to the Clavister SAG servers.



Note

This is only valid in NONE cluster configurations. In a cluster a subzone must be created that uses Clavister SAG as DNS servers.

An example of a BIND v9 configuration:

```
$TTL 86400
@           IN      SOA     ns1.company.com. domains.company.com. (
                2004010101 ; serial
                86400 ; refresh
                3600 ; retry
                1814400 ; expire
                86400 ; default_ttl
```


)		
@	IN	NS	ns1.company.com.
login	IN	A	10.24.19.2
*.login	IN	A	10.24.19.2

A wild card certificate must be installed in order to use SIRH securely. Contact Clavister support to get more information about wild card certificates support@clavister.com.

- **Use Multiple Browser Windows**
This option allows each resource to be opened in a separate web browser window. It is recommended to use *Multiple Browser Windows* only if SIRH is activated.
- **SMTP Server**
The IP-address to the SMTP server that will be used to send emails.
- **SMTP From Address**
This is the address from which Clavister SAG will send email messages.
- **Language**
Choose which language Clavister SAG should use. If set to Auto the language depends on which language the web browser supports. You can choose between English and Swedish support to force a specific language. The Control Center language is always English. For further details, see Chapter 11, *Modification of Pages*.
- **Group for Prioritized Users**
Licenses are normally allocated per logged-in user. This may cause the system to run out of licenses at certain periods when many users are logged on to the system simultaneously. To solve the problem with accessibility that may occur when many users are logged on, you can add administrators and other important personnel to the Prioritized Users group.

All users that are members of the group specified here, will be allocated a license for 30 days. This will guarantee access even if there are many users using Clavister SAG.
- **Preferred Internal Authentication**
Selects which authentication method should be used against an internal resource if multiple authentication methods are available. The recommended method is *Basic*.
- **Public Remote Assistance**
If checked, **Request Remote Assistance** will show up on the login page.

Figure 6.1. Request Remote Assistance

- **Bind Session to Client IP Address**
If activated, each session will be bound to the IP address that the user logged in from. If a user's IP address is changed during a session, this session becomes invalid.
- **Forward client user-agent**
If activated, Clavister SAG will forward the web browser in use to the internal resources. If not activated, Clavister SAG will instead indicate that the users are using *Clavister SAG* as web browser.
- **Persistent Single-Sign-On**
If activated, Clavister SAG will store the Single-Sign-On database in encrypted form to the hard drive. This is useful since the database will not be cleared when Clavister SAG is restarted.
- **JavaScript to open new windows**
If checked Clavister SAG uses JavaScript to open new windows instead of *target=* in the HTML code. This is default. If JavaScript is not used, Clavister SAG is not able to close the windows.

6.2. Supervision Settings

It is possible to let Clavister SAG send SMS messages to system administrators to let them know that something has happened. Messages can be sent if the number of free licenses is less than some number, if a user account is locked or if some rare system error has occurred.

The settings below are common for all Virtual Hosts.

Activate SMS Types

Nearly or completely out of licenses

User account temporarily locked

System errors

Thresholds

Limit that Alarms can only be sent once every given minute. A value of 0 minutes means that an alarm will be sent immediately regardless of when the last alarm was sent.

Nearly or completely out of licenses minutes

User account temporarily locked minutes

System errors minutes

Send warning when only the specified amount of licenses or less are available.

Nearly out of licenses licenses

Specify the cell phone numbers that alarms shall be sent to below. Separate numbers with commas.

Example: +46733123456,+358476123456

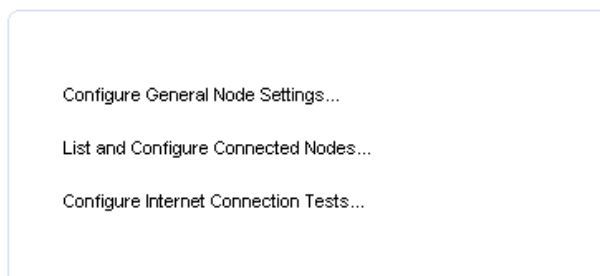
Numbers

- **Activate SMS Types**
Each checkbox is used to activate or deactivate a supervision SMS type.
- **Thresholds**
The threshold text boxes are used to define the minimum number of minutes between supervision SMS's. For example, if the number of minutes is set to 0 for **Nearly or completely out of licenses**, a new SMS is sent directly every time a user is logged in and the number of free licenses is low. If it is set to 60 minutes, the time between SMS's is at least 60 minutes.

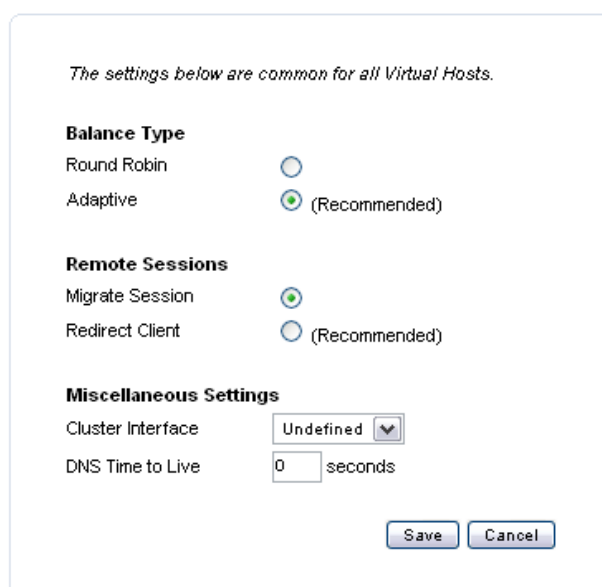
The **Nearly out of licenses** box is used to define the number of free licenses that is needed before the server sends warnings about it.

6.3. Node Settings

The node settings are only visible if *Load Balancing* is active in the Clavister SAG license. The Clavister SAG cluster function is configured here.



General Node Settings



- **Balance Type**
The load balancing type determines the strategy for the load balancing. The choices are:
 - *Round Robin* - the cluster nodes will be selected in a round robin style.
 - *Adaptive* - the node with the least load at that particular time will be selected.
- **Remote Sessions**
 - *Migrate Session* - Clavister SAG migrates the session to the other node so it can use both nodes with the same session.
 - *Migrate Session* - The node where the session is not active redirects requests from the session to the other node where the session was created.
- **Cluster Interface**
The network interface that will be used for cluster traffic.
- **DNS Time To Live**
Sets the number of seconds that the DNS entry is allowed to be cached. The default is 1 second.

Node Information

Node	Type	Status	CPU Usage	Memory Usage	Version	Sessions
200	Primary	Active	0.0%	26.3%	6.1.3 TR36 (12938)	1

[Return](#)

The node information display contains information about configured nodes

- **Node**
This column contains the node IDs. The node ID is equivalent to the last 8 bits in the IPv4 IP address. It is possible to click on the node ID to configure the specified node.
- **Type**
The Type column indicates if the node is the primary node or a slave node.
- **Status**
This column contains the status of the node. See the explanation for Status below for information about the different states.
- **CPU**
This column indicates the CPU usage for each node.
- **Memory**
This column indicates the amount of memory consumed for each node.
- **Disk**
This column indicates the amount of disk space used for each node.
- **Version**
This column indicates the version for each node.
- **Sessions**
This column displays the number of session registered in each node.

The administrator must configure all new nodes in the Clavister SAG cluster. This is done by clicking on the node number in the node list.

Node Settings Fields

Network

This Node's Cluster IP 192.168.101.200

DNS Settings

It is possible to reply with different IP addresses depending on who is requesting an IP address

This is useful when several Network Interfaces are used.

Note: *Only the address pools from the default Virtual Host will be used.*

Address Pool	IP Address
Default / External	85.11.194.34
Disabled <input type="button" value="v"/>	<input type="text"/>
Disabled <input type="button" value="v"/>	<input type="text"/>
Disabled <input type="button" value="v"/>	<input type="text"/>

Status Information

Status	Active
Type	Primary
Version	6.1.3 TR32 (12929)
CPU Usage	1.0%
Memory Usage	27.0%
Number of Sessions	1

Control Settings

Preferred as Primary

Avoidance Factor

- **This Node's Cluster IP**
This field shows the cluster address of this node. It is the first address of the defined cluster interface of this node.
- **DNS Settings**
The DNS Settings are used to define what IP should be used to connect to the Clavister SAG server. Users might refer to the Clavister SAG server using different IP addresses if they are connecting from different networks. Clavister SAG looks at the IP of the requestor and tries to map it against an address pool to figure out which address to return. See Section 4.2, “Address Pools”



Note

*The administrator must always activate the node by pressing the **Save/Update** button before the node can become active.*

The **Status** information is:

- **Status**
This field displays the present node status. The following status information is available:

- *Not Configured* - The node has not yet been configured.
- *Initializing* - Used in the startup phase.
- *Negotiating* - Used during the negotiation phase between the nodes.
- *Not Responding* - When the server is not responding.
- *Offline* - When the server is offline.
- *Active* - The node is in normal operation.
- **Type**
This field indicates if the node is in primary or slave mode.
- **Version**
This field indicates the Clavister SAG version.
- **CPU Usage**
This field indicates the CPU usage for the node.
- **Memory Usage**
This field indicates the amount of memory consumed by the node.
- **Disk Usage**
This field indicates the amount of disk space consumed by the node.
- **Active Message Threads**
Number of cluster messages that are currently being processed by the node.
- **Number of Sessions**
This column displays the number of session registered in the node.

The **Control Settings** are:

- **Preferred as Primary**
If this parameter is set the node will be forced to be the primary node.
- **Avoidance Factor**
An integer value with a default value of 0. Increasing the value increases the probability the cluster does not choose this node. Decreasing the value increase the probability the cluster does choose this node

The buttons in this dialog are:

- **Restart Service**
This button will restart the node.
- **Save**
This button will activate every change made to the node settings. This button is also used when the node is in the state *Not Configured* to configure the node.
- **Cancel**
This button will cancel any changes made in this dialog.

Internet Connection Tests

When running Clavister SAG as a cluster, different nodes can use different Internet connections to ensure that the cluster always can be reached. When a node has lost its Internet connectivity, it lets the other nodes know that is no longer available. The Internet connection is monitored by checking the connection to up to five different hosts using ICMP Ping.

The settings below are common for all Virtual Hosts.

Hosts to send ICMP echo requests to (ping)

Enter one or more servers that echo requests will be sent to, in order to check if the Internet connection is up or down.

If the connection is considered down, the node that detects this will be marked as Offline. This is very useful when multiple Internet providers are used in a cluster.

Leave the fields below blank to **disable** this feature!

Host 1	<input type="text"/>
Host 2	<input type="text"/>
Host 3	<input type="text"/>
Host 4	<input type="text"/>
Host 5	<input type="text"/>

Enter how many hosts that are allowed to be down before the connection is considered down (Host Threshold).

***Example:** if set to 0 the connection will be considered down if any host does not respond to ping. If set to 3 the connection will be considered down when 4 hosts does not respond to ping.*

Host Threshold

- **Host 1-5**
Each line can hold the IP of a host to ping
- **Host Threshold**
The number of hosts that is allowed to fail the ping before setting the node offline.

6.4. Network Connector

The network connector is used to get traditional VPN functionality through Clavister SAG. The network connector requires client software that is distributed from the network connector web page in Clavister SAG. There are three different parts to configure for the Network Connector:

Configure Client DNS, WINS and Routing Tables

Configure Client Networks

Configure Access Control

DNS, WINS and Routing

It is possible to specify different routing tables for different user groups. This can be useful if it is desired to set different DNS and routing settings for consultants and employees for example.

These settings are unique for each Virtual Host.

Table Name
Default Settings

Add new table... Return

When the link **Add new table** is clicked, the configuration page for the new table is displayed. If tables are already defined, clicking on their name in the list displays their configuration.

Name

IP Address

Primary DNS

Secondary DNS

Primary WINS

Secondary WINS

	IP Address	Mask
Route 1	<input type="text" value="10.4.0.0"/>	<input type="text" value="/ 16"/>
Route 2	<input type="text"/>	<input type="text" value="/"/>
Route 3	<input type="text"/>	<input type="text" value="/"/>
Route 4	<input type="text"/>	<input type="text" value="/"/>
Route 5	<input type="text"/>	<input type="text" value="/"/>

- **Name**
The table name.

- **Primary and Secondary DNS.**
IP addresses to the primary and secondary DNS servers that shall be used by the connecting clients.
- **Primary and Secondary WINS**
IP addresses to the primary and secondary WINS servers that shall be used by the connecting clients.
- **Route 1, 2, 3 ... 32**
This is the client routing entries. It is possible to specify up to 32 networks or hosts that shall be routed. It is also possible to specify that all networks should be routed to Clavister SAG. The best way to do this is to specify two routes; the first *0.0.0.0/1* and the second *128.0.0.0/1*. This is done to allow windows clients to get a better default route with a lower metric.

Network Configuration

It is possible to configure different network connector settings for different user groups. By default, the network configuration has only one row, which applies to all groups.

These settings are unique for each Virtual Host.

Warning: *The Network Address must NOT be the same as in any other Virtual Host. It will result in a conflict and the same client IP address can be used by several clients, which will result in communication failure.*

Group	Node	Address / Mask	DNS, WINS & Routing
Any	200	192.168.0.0 / 24	Default Settings

Add a new network configuration...

To add a new rule in the network configuration, press the **Add a new network configuration** link. A new row is displayed.

- **Group**
The user group that this row should apply to.
- **Node**
The Clavister SAG node that this row should apply to. This option is only displayed if Clavister SAG is configured to run load balancing.
- **Address/Mask**
The connecting clients that match this rule should be assigned an IP address from this network.
- **DNS, WINS & Routing**
The name of the routing table to be used.

Access Control for the Network Connector

This is used to set up the access control for the network connector. This is done by adding rules to the list which tell the system when to allow the network connector to run. Each line defines the rules for one group of users.

Group	Auth.	Enc.	IP Address	Time
admins	Any	Medium	Any	Time
Add new rule...				<input type="button" value="Return"/>

- **Group**
The group of users that this rule applies to.
- **Authentication (Auth.)**
Which level of authentication to be required for using the network connector.
- **Encryption (Enc.)**
The level of encryption that must be met to use the network connector.
- **IP Address**
The address pool a user must belong to in order to use the network connector.
- **Time**
When a new row is added and the authentication, encryption and IP address fields are completed, a link with the word *Time* appears next to the other fields. When pressed, the time control for the network connector is displayed. It is used to set up the timing properties for the network connector. It works in the same way as it does for the general Access Control.

Day	All	None	Range	From	Until
Monday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Tuesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Wednesday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Thursday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Friday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Saturday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00
Sunday	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	00:00	24:00

(YYYY-MM-DD)

Valid From: 2007-12-06 From Any Date

Valid Until: 2007-12-06 Until Forever

The topmost part of the time control is used to define what time of week the network connector should be available for the selected user group. Each day of the week has three radio buttons:

- *All* - Makes the network connector available for that entire day.
- *None* - Disables the network connector that day.
- *Range* - Enables the network connector between the times defined in the drop-down boxes **From** and **Until**.

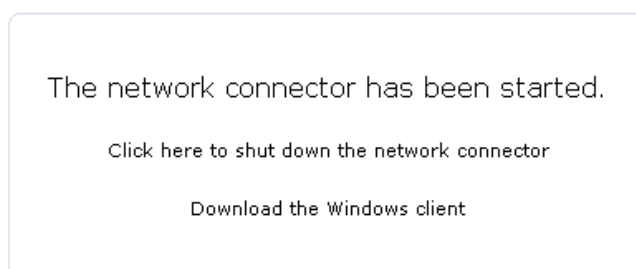
The **Valid From** line is used to define a first date at which the network connector is available. Checking the **From Any Date** box makes the network connector available immediately. The **Valid Until** line is used to define the last date at which the network connector is available. Checking the **Until Forever** box makes the network connector available indefinitely.

The Network Connector Client

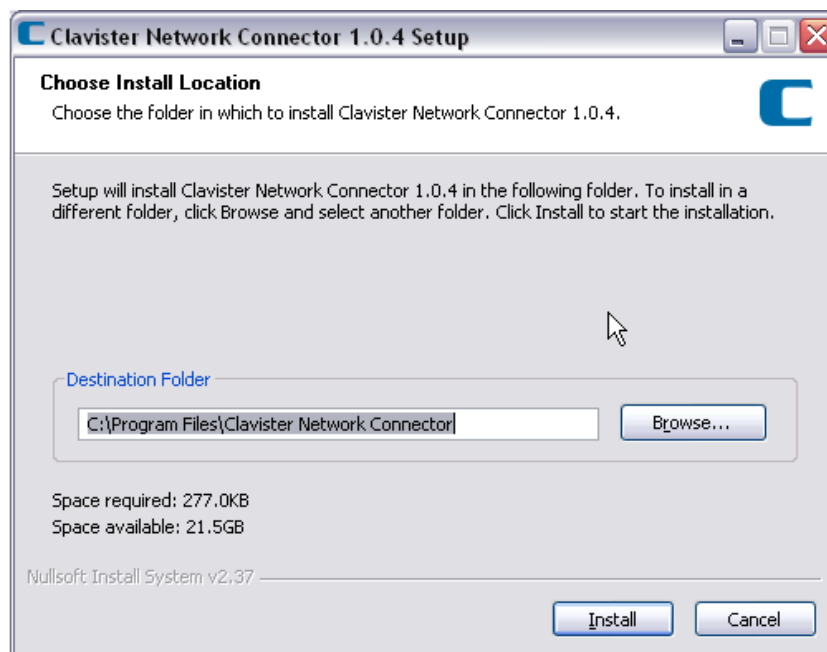
The *Network Connector Client* is a piece of software that is installed separately on a Windows based workstation connecting to the Clavister SAG hardware.

When the network connector is initially accessed, the screen will ask if the network connector client is to be installed as shown below.

Network connector established



If the install option is chosen then an install wizard launches to install the client.



Once installed, the presence and mode of the client is shown by an icon in the windows toolbar.



The client operates by creating a secure tunnel between the Network Connector Java applet running in the browser and the Clavister SAG and then routing all Internet traffic through this tunnel. The client creates a route on the Windows PC to perform this routing. The browser has to be open with the Java applet running for the tunnel to operate.

More Client Details

The client functions by listening on a local TCP socket to get information from the Clavister SAG Java applet that runs in the user's web browser. It operates like a VPN client but instead of replacing

the Window's IP stack, it makes use of the transmissions sent by the Java applet. This means that all traffic goes via TCP port 443.

With the network connector, the client gets an extra IP address from the server and the choice can be made to have a "split tunnel" or if all traffic goes through the tunnel.

Configuring a Security Gateway with the Network Connector

It is important to configure a security gateway in a particular way for the network connector to function correctly. One of the reasons for this is that when the network connector is used, no NAT is performed on the Clavister SAG. The steps for configuration are as follows:

- Create a route on the security gateway to say on which interface the network connector range is found.
- For example, the network connector IP range may be found on *if1* of the security gateway and to reach that IP range it may be required to go through the Clavister SAG's interface IP address that's connected to the *if1* interface. Therefore, on the same route you must configure the external IP address of the CSAG as the route's gateway.

The need for this configuration is also because of the MAC and IP addresses issues involved but this section will expand not further on this point.

6.5. Local Database Settings

Clavister SAG can be used with an internal database or an external LDAP, for example, eDirectory, Active Directory or OpenLDAP. The LDAP attributes that Clavister SAG uses with the external LDAP are explained here.

If you want to use the local database keep the settings shown below.

Database Settings

These settings are unique for each Virtual Host.

Server Type	(requires restart)
Built in	<input checked="" type="radio"/>
External	<input type="radio"/>
External using encryption	<input type="radio"/>
Cache Settings	
Max Cache Age	<input type="text" value="120"/> seconds

[Save / Update](#)

An external LDAP example is shown below which illustrates ActiveDirectory usage.

Server Type	(requires restart)	
Built in	<input type="radio"/>	eDirectory <input type="radio"/>
External	<input checked="" type="radio"/>	Active Directory <input checked="" type="radio"/>
External using encryption	<input type="radio"/>	Other LDAP Service <input type="radio"/>
User Password Handling		
Allow Password Change	<input checked="" type="checkbox"/>	
Warn time	14 Days	
Cache Settings		
Max Cache Age	120 seconds	
Connection Settings		
	(requires restart)	
LDAP Server and port	10.8.1.40 389	
User (dn)	CN=Education User 1,CN=Users,DC=demo,DC=clavister,DC=com	
Password	••••••••	
Search Settings		
Use nested groups	<input checked="" type="checkbox"/>	
User search base	CN=Users,DC=demo,DC=clavister,DC=com	
Group search base	DC=demo,DC=clavister,DC=com	
Clavister SAG Group	CN=SAG-Access,OU=SAG,DC=demo,DC=clavister,DC=com	
Use user location in ACL	<input checked="" type="checkbox"/>	
Container objectClasses	organizationalUnit (Separate with comma)	
Object Classes		
Product objectClass	sag	
User objectClass	person	
Group objectClass	group	
Attributes		
Load default settings for:	Keep Current Settings ▼	
User Login ID	samacountname	
Group ID	cn	
Surname	sn	
Given name	givenname	
Group membership	memberOf	
Distinguished name	distinguishedName	
Web Password	sagWebPassword	
Web Timestamp	sagWebPasswordTimestamp	
Web Old password list	sagWebOldPasswordList	
SMS Number	mobile	
SMS Password	sagSMSPassword	
SMS Timestamp	sagSMSPasswordTimestamp	
SMS Old password list	sagSMSOldPasswordList	
Status	sagStatus	
Login fail	sagLoginFail	
Login fail timestamp	sagLoginFailTimestamp	
e-Mail address	mail	
Comment	sagComment	
Expires	SagExpires	
Custom Fields		
<i>The custom fields can be used as parameters for dynamic content e.g. in the menu. They are accessed with PARM{ldap1}, PARM{ldap2} etc.</i>		
Custom Field 1		
Custom Field 2		
Custom Field 3		
Custom Field 4		

The **Server Type** specifies if the database is external or local and if the connection should be encrypted. The settings are:

- **Built in**
A local database is used to store users and groups. The users and groups can be fully administered from Control Center.
- **External**
If external is chosen, Clavister SAG will get user and group information from an external LDAP. The administrator can not create, edit or delete users and groups from Control Center.
- **External using encryption**
The connection between Clavister SAG and the external LDAP is encrypted. Otherwise the same as **External**.

The **Password Handling** section is only visible if an external directory is used. The settings for this are:

- **Allow Password Change**
This feature works only if the connection between the Clavister SAG and the LDAP server is encrypted.
- **Warn Time**
See **Force Password Change** above.

The **Cache Setting** setting is:

- **Max Cache Age**
The maximum time that Clavister SAG is allowed to cache user information from the local database or external LDAP server.

Connection Settings specifies IP address, port and account information for the LDAP server. The settings are:

- **LDAP Server and Port**
The IP address and port number of the LDAP server. If the LDAP server uses encryption, *stunnel* must be installed on the server. *stunnel* is included with Clavister SAG.
- **User (dn)**
The Full *distinguished name* (DN) for the user account used for login on the LDAP server. For example: *cn=LDAPuser,ou=users,o=company*.
- **Password**
The user account's password.

The **Search Settings** settings are:

- **Use nested groups**
If checked, Clavister SAG is able to use nested groups from the external directory.
- **User search base**
Sets from where in the LDAP tree the search for users should start. Usually from the tree's root level but can be changed when needed.
- **Group search base**

Sets from where in the LDAP tree the search for user groups should start. Usually it is from the tree's root level but this can be changed when needed.

- **Clavister SAG Group**
Full DN for the Clavister SAG's general user group, users must be members of this group for Clavister SAG to find them. Example: `cn=SAGUsers,ou=groups,o=company`
- **Use user location in ACL**
If checked Clavister SAG can use the container of a user in the access control. When activated, containers will also be listed in the *Import groups* section of *Users and groups*. If a container is checked, it is included in the list of available groups to select from in the access control.
- **Container objectClasses**
What object classes to regard as containers are defined here. Example: `organizationalUnit`.

**Note**

Clavister SAG must be restarted if the Search Settings are modified, in order for the change to take effect.

The **Object Classes** settings are:

- **Clavister SAG objectClass**
The name of Clavister SAG's object class.
- **User objectClass**
The name of the LDAP object class to identify users, in most cases *person* is used.
- **Group objectClass**
The name of the LDAP object class to identify user groups, in most cases *groups* is used.

These values will be changed when you choose a value below in *Load default settings for*.

The **LDAP Attributes** settings are:

- **Load default settings for**
If this selection is set to any other value than *Keep Current Settings*, the proper attribute settings for the selected directory server will be stored when the *Save/Update* button is clicked.

The following presets are available:

- *Active Directory*
- *eDirectory/NDS*
- *Built in*
- **User Login ID**
Attribute for user's login id. This attribute must be unique.
- **Group ID**
Attribute used by groups.
- **Surname**
Attribute for user's surname.
- **Given name**
Attribute for user's given name.
- **Group membership**

Attribute for the group memberships of the user.

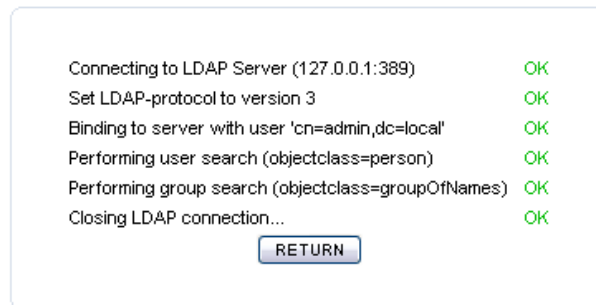
- **Distinguished name**
Attribute for the distinguished name of the object.
- **Web password**
This attribute contains a hash of the user's password for Web Token. Clavister SAG must be able to change this attribute.
- **Web timestamp**
This attribute contains the time of the last change of the user's Web Token password. Clavister SAG must be able to change this attribute.
- **Web old password list**
This attribute contains hashes of the user's previous passwords for Web Token. Clavister SAG must be able to change this attribute.
- **SMS number**
This attribute contains the user's cell phone number. Clavister SAG must be able to change this attribute.
- **SMS password**
This attribute contains a hash of the user's password for SMS Token. Clavister SAG must be able to change this attribute.
- **SMS timestamp**
This attribute contains the time of the last change of the user's SMS Token password. Clavister SAG must be able to change this attribute.
- **SMS old password list**
This attribute contains hashes of the user's previous passwords for SMS Token. Clavister SAG must be able to change this attribute.
- **Status**
This attribute contains the status value for Clavister SAG. Clavister SAG must be able to change this attribute.
- **Login fail**
This attribute counts the number of failed logins made by the user. Clavister SAG must be able to change this attribute.
- **Login fail timestamp**
This attribute contains the time of the latest failed login for the user. Clavister SAG must be able to change this attribute.
- **e-Mail address**
The email address for the user. This attribute is used by Message Center.
- **Comment**
When this attribute is configured, a comment field will be displayed for each user in the user administration.
- **Expires**
If this setting is used then the expiration date of a user can be set using Control Center. An expired user can no longer log in.

Custom fields are used to get custom dynamic information in menu entries and in the access control. It is very useful if the user id is set to the users email address but the home account is a regular user name. For instance if the user Bob logs on to Clavister SAG with the email address *bob@company.com* and the aim is to restrict Bob to only be able to see files in Bob's home folder which is named *bob*, then the administrator can map the LDAP attribute for the user name (bob) to customize parameter 1 and then use `PARM{ldap1}` in the menu and access control.

LDAP Connectivity Test

This tool can be used to check if the connection between the LDAP server and Clavister SAG is good. It can also be used to test if the LDAP user name and password are correct. This test will not modify any attributes in the LDAP directory.

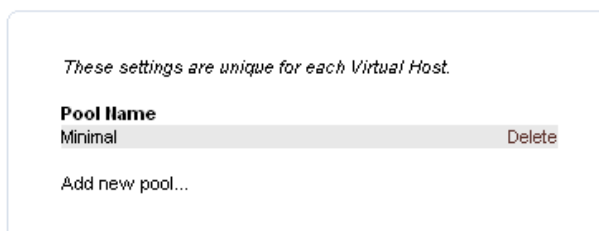
To start the test, click on **LDAP connectivity test**.



6.6. URL Converter

The URL Converter is used when Clavister SAG communicates with a resource of the types HTTP or HTTPS. The URL Converter scans all web pages for certain patterns in order to find absolute links. These links are translated to the DNS name of Clavister SAG.

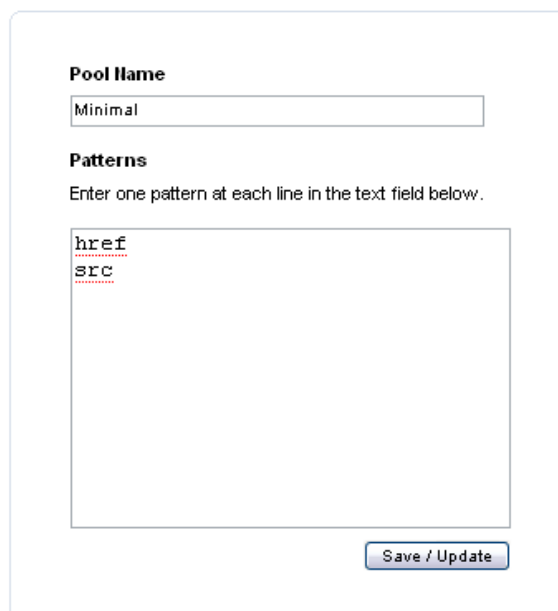
There are two pattern pools available by default in Clavister SAG. The first is named *Normal* and cannot be edited by the administrator. The second one is named *Minimal* which only contain a few search patterns. The latter is, for instance, used for Lotus Notes.



- **Pool Name**
This is the name of the pattern pool.
- **Delete** Click on the delete link to delete the pattern pool. All resources assigned to a deleted pattern pool, will automatically be assigned with the *Normal* pattern pool.

Adding and Editing a Pattern Pool

To add a new pattern pool, click on the **Add new pool...** link. To edit a pattern pool, click on the pool name.



- **Pool Name**
This is the name of the pattern pool.
- **Patterns** A search pattern is entered on each line in the Pattern field.

6.7. Virtual Hosts

The concept of virtual hosts enables a Clavister SAG server (or a cluster of servers) to act as two or more separate servers, with separate URLs, user databases and configurations, but with one certificate.

If one or more virtual hosts are defined, a dropdown box appears in the top left of the control center. This box allows the administrator to select which configuration to edit, either the default configuration or the configuration for one of the virtual hosts. Some of the configuration is common to all virtual hosts and some are defined separately. If virtual hosts are configured on the server, a text appears on each configuration page in the control center, telling the administrator if that part of the configuration is common for all or is specifically for the selected virtual host.

Multiple host names can be specified separated by comma.

Id	Host Name(s)	Description
1	education.example.com	Education

- **Id**
The virtual host id is automatically generated and is used internally in Clavister SAG.
- **Host name**
The host name is the URL to which clients connect to log in to a virtual host. Multiple host names can be specified delimited by commas. NOTE that the user must connect to the host name using HTTP.
- **Description**
The description is the name of the virtual host that is used in control center.

To add a new virtual host, press Add new server. When a virtual host is created, the Clavister SAG server generates configuration files and folders for that host. When a virtual host is deleted, these files are removed.

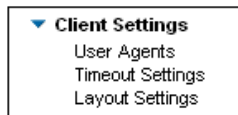


Note

If a virtual host is deleted, so are the configuration and all other files for that virtual host. This will cause problems for all users connected to the virtual host at that time

Chapter 7. Client Settings

Figure 7.1. The Client Settings Menu



7.1. User Agents

Clavister SAG can be configured to function differently depending of which web browser is used. The functionality of the different web browsers can be set here.

These settings are common for all Virtual Hosts.

User Agents	Comment	Move
mozilla/4.0 \(\compatible; \(smisie \(S+; \(S+) \(s* s*; \(sms search \(S+) robot	Microsoft Search Robot	Move
mozilla/4.0 \(\compatible; \(smisie \(S+; \(smac. *)\)\$	Internet Explorer on Mac	Move
mozilla/4.0 \(\compatible; \(smisie \(S+; \(s(\w+). *)\)\$	Internet Explorer	Move
mozilla/5.0 \(\w+; \(s(\w+); \(s(\w+).+rv.(.*)\) gecko/d+\$	Mozilla	Move
mozilla/5.0 \(\macintosh; \(s(\w+); \(s(\w+).*)\) gecko/d+ (\w+)/(\(S+)\$	Gecko based eg. Firefox and Netscape >= version 6 on Mac	Move
mozilla/5.0 \(.+; \(s(\w+); \(s(\w+).*)\) gecko/d+(\(s+ S+)* (\(S+) \((S+)	Gecko based eg. Firefox and Netscape >= version 6	Move
mozilla/4.0 \(\compatible; \(msie .+; \(s(\w+).*)\) \(opera \(1.0-9.*\) s+\(Opera	Move
java plugin	Java VM	Move
mozilla/4.0 \(\(.*) \(s. *)\) Java(\. *)	Java VM	Move
mozilla/4.[0-9]+ \(\compatible; \(MSIE [0-9]\.+; \(symbian os\) \(opera ([0-9]\.+) \(s	Opera on Symbian	Move
mozilla/2.0 \(\compatible; \(msie \(.*\); \(s(\w+); \(s240x320)\)\$	Internet Explorer on PocketPC	Move
mozilla/4.0[0-9]? \(\w+; \(s(\w+); \(s(\w+).*)\) \(snetfront (\. *)	Netfront on PocketPC	Move
\(SonyEricsson[\w\d]+)\((\w\d)+\)	Sony Ericsson P800 & P900	Move
mozilla/5.0 \(\compatible; \(konqueror (\. *)\) \(s(\w+)	Konqueror	Move
mozilla/5.0 \(galeon (\. *)\) \(s(\w+); \(1,1\) \(s(\w+)	Galeon	Move
mozilla/5.0 \(.+; \(s(\w+); \(s(\w+).*)\) \(s(\w+) (\w\d+)	Safari	Move
opera(\. *) \(s(\w+); \(s(\w+).*)\)	Opera	Move
mozilla/4.[1-9][0-9]? \(s(\w+); \(s(\w+); \(s(\w+) (\w\d+)	Netscape 4.x	Move
Microsoft Data Access Internet Publishing Provider Cache Manager	Microsoft Cache Manager	Move
MSFrontPage/(\(S+)	Microsoft FrontPage	Move
Microsoft Office Protocol Discovery	Microsoft Office Protocol Discovery	Move
mozilla/5.0 \(\compatible; \(googlebot \(S+; \(http://www.google.com/bot.html\)		Move
Secure Connector \(\(Version \(S+ \) (\. *)\)\$	Universal Client	Move
Add new agent...		
Test agent...		

The components of this display are:

- User Agents**
 This column contains regular expressions that will match the User Agent. The User Agent is sent in the HTTP protocol from the client to the Clavister SAG server.
- Comment**
 A comment only used by the Administrator for a better overview of the specified agents.
- Move**
 Used to move an entry up or down in the list. User Agents that are more common should be placed first in the list for performance reasons.
- Add new agent...**
 This link is used to add new regular expressions.
- Test agent...**
 This link is used to test which regular expression matches a specific User Agent.

**Note**

If changes has been made, they will not take effect in the tests until the Clavister SAG configuration has been reloaded.

Add New User Agent

Regular Expression	<input type="text"/>	
	Index	Static String
Browser Name	<input type="text"/>	<input type="text"/>
Browser Version	<input type="text"/>	<input type="text"/>
Operating System	<input type="text"/>	<input type="text"/>
Comment	<input type="text"/>	
Handles Error Body	<input checked="" type="checkbox"/>	The browser can handle custom error messages (most browsers can)
Handles Javascript	<input checked="" type="checkbox"/>	If not checked, a simple version of Web and SMS Token can be used
Handles Java	<input checked="" type="checkbox"/>	If not checked, Java will not be used for Web and SMS Token
Small Screen	<input type="checkbox"/>	Many pages will be optimized for a small screen
Local Tunnel	<input type="checkbox"/>	Locally installed Communication Tunnel (typically a handheld device)
No Browser	<input type="checkbox"/>	Login procedure is not performed by a web browser.
<input type="button" value="Save / Update"/> <input type="button" value="Delete"/> <input type="button" value="Back"/>		

- **Regular Expression**

Regular expressions are used to parse User Agent strings sent from the web browser to the Clavister SAG server. A regular expression can match strings that are almost the same all the time. The string may contain version information that may differ from one User Agent to another depending on the version of the web browser.

The version information can also be used later to indicate which browser version a specific user uses.

- **Index/Static String**

It is possible to hard-code the browser name and version as well as the operating system name in the *Static String* field. It is also possible to collect that information from the regular expression. This is done by grouping matches between parentheses. In this case the group number is specified in the *Index* field. The first group has the number 1, the second group has the number 2 and so on.

- **Browser Name**

These settings are used to set the browser name or the group index to use as browser name if this regular expression matches the User Agent.

- **Browser Version**

These settings are used to set the browser version or the group index to use as browser version if this regular expression matches the User Agent.

- **Operating System**

These settings are used to set the name of the operating system or the group index to use as operating system name if this regular expression matches the User Agent.

- **Comment**

This is a comment that is used by the administrator to get an easy overview of all regular expressions.

- **Handles Error Body**
If set, the web browser can handle customized error messages. Except for Microsoft Java VM most browsers handle this properly.
- **Handles JavaScript**
Indicates that the web browser has JavaScripting capabilities.
- **Handles Java**
Indicates that the web browser has Java capabilities.
- **Small Screen**
Indicates that the web browser is run on a device with a small screen, typically a pocket device such as a PDA.
- **Local tunnel**
This checkbox is reserved for future functionality.
- **No browser**
Login procedure is not performed by a web browser.

Testing User Agents

Note that you have to reload the configuration file before any new or changed Regular Expressions will take affect.

User Agent

- **User Agent**
The User Agent, which must be tested for a match.

User Agent: Microsoft Office Protocol Discovery

Browser: Protocol Discovery
Version:
OS: Windows

Error Body: true
Javascript: false
Java: false
Small Display: false
Local Tunnel: false
Custom Login: false

All data specified for the matched regular expression will be displayed as well as the dynamic values such as browser version etc. If no regular expression matches a message will be presented indicating that nothing matched the tested User Agent.

7.2. Timeout Settings

The time limits in Clavister SAG can be set here.

Global Session Timeouts

Max idle time minutes

Warn before timeout seconds

Max unused age seconds

Configure Individual Timeouts

Global Session Timeouts

Global Session Timeouts are time limits for user sessions. It is also possible to set up individual timeout settings by clicking on the **Configure Individual Timeouts** link.

- **Max idle time**
The maximum time a user can be idle before she is automatically logged out from Clavister SAG.
- **Warn before timeout**
A warning is sent to the user before she is automatically logged out from Clavister SAG. The warning is sent xx seconds before automatic logout.
- **Max unused age**
How long a session is valid before the user must authenticate.

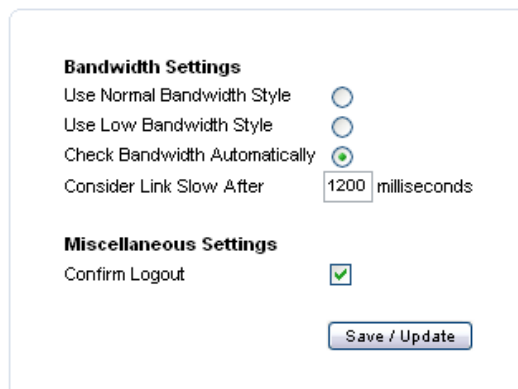
Individual Timeout Settings

Group	Address Pool	Max Idle Time	Warning Time
<input type="text" value="admins"/>	<input type="text" value="Secure Administration Network"/>	<input type="text" value="10"/> minutes	<input type="text" value="60"/> seconds

- **Group**
The group that a user must be a member of, in order to get the specified timeout settings.
- **Address Pool**
A warning is sent to the user before she is automatically logged out from Clavister SAG. The warning is sent xx seconds before automatic logout.
- **Max Idle Time**
The maximum time in minutes that the users can idle before a timeout.
- **Warning Time**
Indicated when a warning shall be displayed for the user.
- **Move**

This is used to move the rule up or down. It is useful if a user is a member of many groups. The matching will parse each line from top to bottom of the list and will stop on the first match.

7.3. Layout Settings



The screenshot shows a settings panel with two sections: **Bandwidth Settings** and **Miscellaneous Settings**. In the Bandwidth section, 'Use Normal Bandwidth Style' and 'Use Low Bandwidth Style' are both unselected (radio buttons), while 'Check Bandwidth Automatically' is selected (radio button). The 'Consider Link Slow After' field is set to '1200' milliseconds. In the Miscellaneous section, 'Confirm Logout' is checked (checkbox). A 'Save / Update' button is located at the bottom right of the panel.

Bandwidth Settings

Clavister SAG uses two different user interfaces depending on the latency and bandwidth between the user and the Clavister SAG server. The two user interfaces are *Low* (also known as light) and *Normal*. *Low* is for slow connections for example modems, ISDN, GSM/GPRS, and also 3G networks (due to high latency in the mobile networks). Normal is for connections such as xDSL or other high bandwidth connections with low latency. The difference between *Low* and *Normal* is that many pictures are removed and replaced by simple HTML in the low bandwidth mode.

Clavister SAG can dynamically choose which user interface to use; the decision is based on a fast latency/bandwidth test. It is also possible for the user to choose user interface.

- **Use Normal Bandwidth Style**
The normal user interface is used.
- **Use Low Bandwidth Style**
The optimized user interface is used.
- Clavister SAG will dynamically choose the interface depending on latency and bandwidth.
- **Consider link slow after**
The time limit for the automatic bandwidth test, if the test takes more time then given here, the bandwidth will be considered as slow.

Miscellaneous Settings

If **Confirm Logout** is activated, the user will have to acknowledge the logout request from Clavister SAG. If this option is deactivated, then the user will be logged out directly when clicking on the logout link. This option protects users from accidental logouts.

Chapter 8. Authentication

Figure 8.1. The Authentication Menu



8.1. RADIUS Servers

Clavister SAG can be used with external authentication servers. The authentication servers must support the RADIUS protocol to be configured in this section.

The configured RADIUS servers are displayed in a list as shown in the example below:

Address	Shared Secret	Authentication Port	Accounting Port	Description
192.168.0.10	---- Secret ----	1645	1646	Digipass
Add new server...				

The settings are:

- **Description**
A unique descriptive name for the RADIUS server. This name will be shown for the users at login.
- **Address**
The RADIUS server's IP address.
- **Shared Secret**
The password or the shared secret used for communicating with the RADIUS server.
- **Authentication Port**
The RADIUS server's port number used for authentication.
- **Accounting Port**
The RADIUS server's port number used for accounting. Not yet used by Clavister SAG but reserved for the future.
- **Auth Through User Database**
Will use custom parameters for authenticating the RADIUS server. This requires the user to enter a valid UserID and password when logging in.
- **User Parameter**
The parameter whose value will be sent as the username to the RADIUS server.
- **User Password**
The parameter whose value will be sent as the user's password to the RADIUS server.

8.2. Web Authentication

All the settings concerning the module Clavister SAG Web Authentication (Web and SMS token) are found here.

Web Authentication Settings

These settings are unique for each Virtual Host.

Account Locking Policy

Time to sleep after failed login seconds

Max attempts before temporary lock times

Temporary lock time seconds

Anonymous

Anonymous username

Basic

Always show login dialog

Use random realm

Web Token

Allow bypass of the keypad

Random button placement

SMS Token

Random button placement

SMS Token Dialog Type

Keypad with Java

Keypad without Java

Simple input without Java

The **Account Locking Policy** settings are:

- **Time to sleep after failed login**
The time in seconds that Clavister SAG will pause before an error message is sent to the user after an incorrect login attempt. The recommended value is 3 seconds.
- **Max attempts before temporary lock**
The number of failed login attempts a user can make before the account is locked. The recommended number of times is 3.
- **Temporary lock time**
Sets how long a user will be locked out from Clavister SAG after a temporary locking of the account. The recommended value is between 600 and 1800 seconds (10 and 30 minutes).

The **Anonymous username** allows the setting of the username for anonymous users. The default value is *anonymous*.

The **Basic** settings are:

- **Always show login dialog**
Force the browser to always display the login prompt.
- **use random realm**
Make sure that a password saved by the browser cannot be used automatically.

The **Web Token** settings are:

- **Allow bypass of the keypad**
If the browser cannot handle javascript, allow a version without the keypad.
- **Random button placement**
If activated, Clavister SAG will randomize the placement of the Web Token login dialog buttons. This makes it more difficult for a Trojan horse to read passwords. If the number panel is not used at login this option has no real function. It is recommended that this option is activated for Web Token.

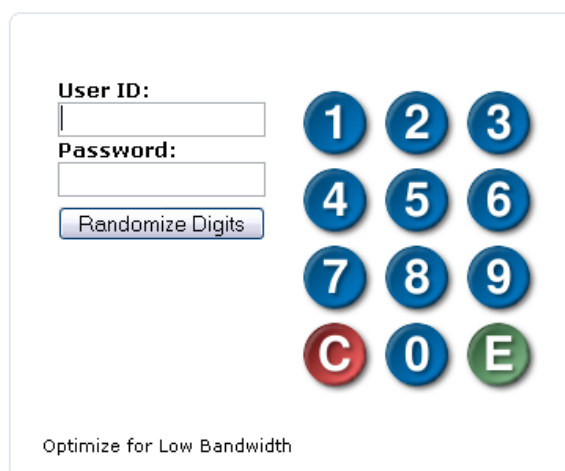
The **SMS Token** field is:

- **Random button placement**
If activated, Clavister SAG will randomize the placement of the SMS Token login dialog buttons. This makes it more difficult for a Trojan horse to read passwords. If the number panel is not used at login this option has no real function.

The **SMS Token Dialog Type** allows one of three different user login interfaces to be used.

1. **Keypad with Java**
If activated, the users must use the number pad to enter any numbers in the password. This is the same as for *Web Token* and is also the recommended option.

Figure 8.2. The Java Keypad



The image shows a login interface with the following elements:

- User ID:** A text input field.
- Password:** A text input field.
- Randomize Digits:** A button located below the password field.
- Keypad:** A grid of buttons on the right side:
 - Row 1: 1, 2, 3
 - Row 2: 4, 5, 6
 - Row 3: 7, 8, 9
 - Row 4: C (red), 0, E (green)
- Optimize for Low Bandwidth:** Text at the bottom of the interface.

Figure 8.3. A Randomized Javascript Keypad

Enter your User ID and Password

The form contains the following elements:

- User ID:** A text input field.
- Password:** A text input field.
- Randomize Digits:** A button.
- Keypad:** A grid of buttons including digits 0-9 and letters C, E, 1.
- Optimize for Low Bandwidth:** A link at the bottom.

2. **Keypad without Javascript**
If activated, the user will be shown a dialog similar to the *Keypad with Javascript* but Javascript will not be used.
3. **Simple input without Javascript**
If activated, the user will be shown a very simple input dialog without the number pad for SMS Token login. The user can only use the keyboard to enter the password. This option does not require Javascript support.

Password Policy

The configuration page includes the following sections and settings:

- Password Source**
 - Separate Passwords: (This is Recommended)
 - Internal Directory Password: (Requires External LDAP Server)
- Common**
 - Force password change every: days
 - Passwords to remember: (0 - 7)
- Web Token**
 - Minimum password length:
 - Minimum letters:
 - Minimum figures:
 - Minimum special characters:
- SMS Token**
 - Minimum password length:
 - Minimum letters:
 - Minimum figures:
 - Minimum special characters:

Save / Update

The **Password Source** settings are:

- **Separate Passwords**
If this option is selected, then the users will be assigned different passwords for Web and SMS Token, as well as for the internal passwords for, as an example, Active Directory.
- **Internal Directory Password**
If this option is selected, Clavister SAG will use the users internal password used to logon to the internal network.

**Note**

Enabling this option requires that Clavister SAG is connected to an external LDAP service.

The **Common** settings are:

- **Force password change every**
The user's password will expire after the specified number of days. A user with an expired password must change the password. If zero days are set, the password will never expire.
- **Passwords to remember**
Clavister SAG can remember a maximum of seven old passwords for each user. When a user is forced to change the password, they can not change to any of the old passwords previously used.

The **Web Token** settings are:

- **Minimum password length**
The minimum number of characters in the password. A minimum of six characters is recommended.
- **Minimum letters**
The minimum number of letters in the password. A minimum of two letters is recommended.
- **Minimum figures**
The minimum numbers of figures in the password. A minimum of two figures is recommended.
- **Minimum special characters**
The minimum number of special characters in the password.
The valid special characters are: `!"#$%&'()*+,-./[^_`{|}~:;<>=@`

The **SMS Token** settings are:

- **Minimum password length**
The minimum number of characters in the password. A minimum of six characters is recommended.
- **Minimum letters**
The minimum number of letters in the password. A minimum of two letters is recommended.
- **Minimum figures**
The minimum number of figures in the password. A minimum of two figures is recommended.
- **Minimum special characters**
The minimum number of special characters See Web Token above for more information on the valid characters.

SMS Settings

The settings for the SMS servers and one-time passwords.

SMS Settings

SMS Credits can be purchased through the Clavister Client Web at <https://clientweb.clavister.com>

Server Controls

Use flash SMS

One Time Password

Max valid time seconds

Message prefix:

Valid characters

Password length characters

Insert separator after characters

Use separator

Server Controls relates to the functioning of the SMS server. The single setting is:

- **Use Flash SMS**

If *Use Flash SMS* is checked, SMSs will only be shown on the screen and not stored in the cell phone, thus avoiding filling the memory of the cell phone unnecessarily. Flash SMS is included in the original GSM SMS standard and should be supported by all GSM phones that have SMS support.

The **One Time Password** settings control how the one-time password sent to the user is handled and formatted.

- **Max valid time**

Sets the number of seconds a one-time password is valid. Recommended value is 180 seconds (3 minutes).

- **Message prefix**

Sets a message prefix to be sent with the one-time password. For example: "*Password is:*"

- **Valid characters**

Specifies the valid characters to generate the one-time password. It is recommended not to include similar characters and letters such as *0* and *O*, *1* and *I* and so on.

- **Password length**

Sets the length of the one-time password.

- **Insert separator after**

A separator can be added to the one-time password to make it easier to read. The position of the separator is set here, e.g. if the one-time password is of length six the separator should probably be placed at position three. An example of a one-time password with separator is: *RE3-4XW*.

- **Use separator**

Sets whether or not to use a separator.

Obtaining SMS Credits

SMS credits are available for purchase through the Clavister Client Web internet site which is located at: <https://clientweb.clavister.com>.

The online payment system accepts credit cards only (VISA or Mastercard at the time of writing although this will be extended later).

8.3. Authentication Methods

Clavister SAG supports many different methods for user authentication, for example Web Token, SMS Token, Vasco Digipass and SecurID. The authentication methods are configured here.

Method	Enabled	Rank	Ileg.	IP Address
Anonymous	<input type="checkbox"/>		<input type="checkbox"/>	Any
Basic	<input checked="" type="checkbox"/>		<input type="checkbox"/>	Any
Web Token	<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Any
SMS Token	<input checked="" type="checkbox"/>	2	<input type="checkbox"/>	Any
Enable Ranking	<input type="checkbox"/>			
Test Logon	<input type="checkbox"/>			
Testlogon from	<input type="text" value="192.168.101.1"/>			
Testlogon should <i>never</i> be used in a production environment!				
<input type="button" value="Save / Update"/>				

If an authentication method is not activated, users will not be able to login with this method. Nor will the authentication method be shown among the login options on the first page. Please note that every defined RADIUS server is also shown here.

The settings are:

- **Method**

The authentication methods are:

- *Basic* - This method uses the HTTP authentication headers to send the authentication information.



Note

Most web browsers have the possibility to store the password for Basic authentication servers. This method is only recommended for internal networks.

- *Web Token* - A one factor authentication method. Users are authenticated with their user name and password. This method is not as secure as SMS Token and access should therefore be more restricted.
- *SMS Token* - A two factor authentication method. Authentication is based on user name, password and a one-time password. First the user enters the user name and password. If the user name and password are correct, a one-time password will be sent to the user's cell phone. If s he also enters the one-time password she will be authenticated. This method is seen as more secure than Web Token as a user must also have the correct cell phone to login.
- *Digipass* - This is a RADIUS server defined in the previous chapter.
- **Neg**
If selected, users connecting from the address pool specified in the IP address field cannot use this authentication method.
- **IP-addresses**
This field specifies from which address pool this authentication method can be used.

- **Enable Ranking**
With authentication ranking turned on, each user will get a navigator containing menu entries for all resources that user has access to, no matter which authentication method she used to log on. When the user selects a resource in the list that requires another authentication method, Clavister SAG will automatically try to authenticate the user using that authentication method. If access to the resource is allowed using more than one authentication, Clavister SAG will select the authentication method with the lowest rank that the user has access to.
- **Test Logon**
Test logon allows the administrator to get full access to Control Center and resources that access localhost from one or more IP addresses. Test logon is used to install Clavister SAG before any user account is created.
- **Test logon from**
The IP addresses from where Test Logon is allowed.

**Note**

Test Logon must never be used in a production environment.

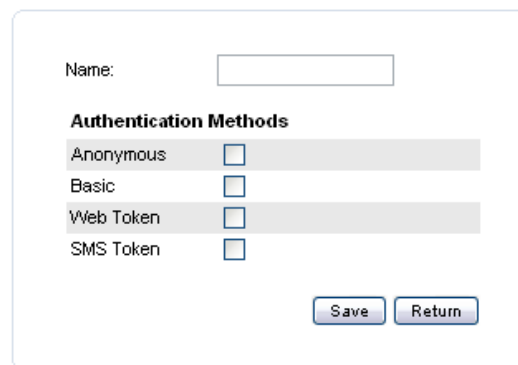
8.4. Authentication Groups

Authentication groups can be used to logically group two or more authentication methods. These groups can be used in the access control in the same way normal authentication methods are used.



A screenshot of a web interface showing a list of authentication groups. The list is titled "Group Name" and contains two entries: "1-Way" and "2-Way". To the right of each entry is a "Delete" button. Below the list is a link that says "Add new group..."

To create a new group, click **Add new group**.
To delete a group, click **Delete** to the right of the group's name.



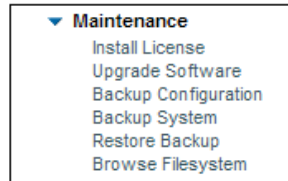
A screenshot of a web interface for creating a new authentication group. It features a "Name:" label followed by an empty text input field. Below this is a section titled "Authentication Methods" which contains four rows, each with a method name and a checkbox: "Anonymous", "Basic", "Web Token", and "SMS Token". At the bottom right of the form are two buttons: "Save" and "Return".

The settings for group creation are:

- **Name**
Your description of the group.
- **Authentication Methods**
The methods for the group.

Chapter 9. Maintenance

Figure 9.1. The Maintenance Menu



Install License

This button is used to install a new license file.

The license file will be checked before it is installed. Please note that only the integrity of the file is checked, Clavister SAG will not check if the license file contains the correct number of licenses, nor will it check the host name of the Clavister SAG server.

The first step is to choose a file by typing in the full path or click on **Browse**. Click on **Upload** once the correct file is chosen.

A screenshot of a web form for uploading a license file. The form contains the following text: "Please choose a license file to upload." and "The integrity of the file will be checked to avoid activation of a corrupt license." Below the text is a text input field, a "Browse..." button, and an "Upload" button.

Then click on **Activate license** to activate the new license.

A screenshot of a confirmation dialog box. The text inside reads: "The license file is valid and ready for activation." followed by "Please note that only the integrity of the license file has been checked. There is no guarantee that the right number of licenses is correct, nor that the right host names are specified in the license file." At the bottom, there are two buttons: "Activate License" and "Cancel".

The upgrade will be rejected if the license file is corrupt or damaged. If accepted the following will appear.

A screenshot of a success message box. The text inside reads: "The new license has been activated." followed by "Click Here to return to the status page." with a link.

Upgrading Clavister SAG

Clavister SAG can easily be upgraded to a new version from Control Center. To do this click on **Upgrade Clavister SAG**. The integrity of the new program package will be checked before it is installed. Please contact Clavister SAG support for more information and to obtain packages.

The first step is to choose the new program packet file and upload it to Clavister SAG.

Please choose the software package file to upload.
The integrity of the file will be checked to avoid installation of a corrupt package.

The packet will be decompressed.

Now the packet is verified and ready for installation. Next click on **Install**.

The new software package has been verified and is ready for installation.

Please note that only the integrity of the package has been checked.
It may still be rejected during the installation.

However, the package will not be installed if
any incompatibilities are found during the installation process.

Clavister SAG must now be restarted after a successful upgrade. to do this click on **Restart service** to restart.

The software package is now being installed on all nodes.

Do NOT interrupt this process!

The following text will be shown until the service has been restarted. The login page will be displayed automatically when Clavister SAG has restarted successfully.

Clavister Secure Access Gateway is restarting, Please wait...

Backup Configuration

This function is used to download the configuration files to your local computer.



Note

Only the configuration files are handled. The built-in user database, SSO-database and customized pages will NOT be backed up. For a complete backup use the Backup

Installation feature described below.

Backup System

This function is used to backup the Clavister SAG system. All user data and customized HTML pages as well as the network configuration will be backed up to a single backup file when this function is used.

The backup file created is encrypted and can be opened only by the restore function described next.

Restore Backup

This option is used to restore a previously created backup. Only backups from the 6.20 product version or later can be restored with this function.

Browse File System

The Control Center File Browser is a powerful tool to administer files on the Clavister SAG server.

The fields in this dialog are.

- **Index of**
The title contains the current directory listed in the file dialog.
- **Enter a directory name below and press the "Create Directory" button...**
A directory name can be entered in this field and the directory will be created when the **Create Directory** button is pressed.
- **Enter the full path to a local file below and press the "Upload" button...**
It is possible to manually enter a filename in this field or to select a file by pressing the **Browse...** button. The specified file will be uploaded to the current directory on the Clavister SAG server when the Upload button is pressed.

Installation Root Directory Structure

All Clavister SAG files are stored in the Clavister SAG root directory on the server. The different directories in the root directory are:

- *logfiles* - Every log file is stored here.
- *stunnel* - This directory is used to store LDAP certificates for LDAPS functionality.
- *server* - This directory contains every web page and related files. The subdirectories are:
 - *custom_data-public* - This directory contains every file that is accessible to everyone, for example login pages and the Clavister SAG logo.
 - *custom_data-private* - This directory contains the files that only are accessible to users that have been authenticated, for example the welcome page.











Note

Each virtual host has its own custom_data-public and custom_data-private directory. To browse to a specific virtual host's custom directory, use the drop-down box in the upper left corner in the control center to choose host.

Browsing the /server Directory

The browser has some extra functionality when browsing the directories in */server*.

Parent Directory	
 jta20.cab	Copy
 jta20.jar	Copy
 jta25.jar	Copy
 putty.exe	Copy
 ssh.conf	Copy
 ssh.html	Copy
 ssh.html-light	Copy
 ssh.html-pda	Copy

Files with this color and size are a part of the installation and has NOT been modified by the administrator.

Files with this color and size are a part of the installation and has been modified by the administrator.

Files with this color and size are not a part of the installation.

Enter a directory name below and press the "Create Directory" button to create a new directory.

Enter the full path to a local file below and press the "Upload" button to upload a file to the current directory.

The extra browser options are:

- Clavister SAG allows the administrator to customize pages and files without destroying the default files.
- Files that are not modified are displayed in a blue font and have a **Coy** button next to them.
- Files that are modified are displayed using a bold blue font and have a **Delete** button next to them.
- Files that are not a part of a default Clavister SAG installation are displayed in a bold green font and have a **Delete** button next to them.
- Modified pages are reloaded when the **Activate Changes => Reindex Files** is pressed.

Chapter 10. Activate Changes

Figure 10.1. The Activate Changes Option

Activate Changes

Any changes to Clavister SAG's configuration must be activated to work, click on the option **Activate Changes** and the following dialog will appear.

Reload configuration

All changes made will remain inactive until a reload of the configuration is made.

This will not terminate the active sessions unless the new settings directly affects the logged in users.

Reload configuration

Reindex files

If files are changed or added to the public or private file structure you must force the service to reindex all files.

Reindex files

Restart the service

In some rare maintenance cases the service has to be restarted. All active sessions will be disconnected including your session. This means that you have to relogin after a restart.

Use with care!

Restart Service

Shut down the server

Use this function to power off the Appliance. This shall **always** be done **before the power cable is disconnected!**

Shut Down

The options are:

- **Reload configuration**
Clavister SAG will reload the configuration file and activate any configuration changes. Users currently logged in will remain logged in.
- **Reindex files**
Clavister SAG stores information on every file the users have access to, for example login pages.

Clavister SAG must reindex files if they have been added to or changed in the directories *custom_data-public* or *custom_data-private*.

Files must also be reindexed if the Cache Control has been changed for the resource sag-local.

See Section 4.3.3, “Cache Control” for more information on caching.

- **Restart service**

For certain changes to take place, Clavister SAG must be restarted. One example is changes in the LDAP configuration. This restart of Clavister SAG should normally not be done in a production environment.



Important

All users will be disconnected and logged out from Clavister SAG. This includes the administrator!

Chapter 11. Modification of Pages

To make changes to a webpage:

1. Browse to the directory where the file is located.
2. Click on the file name and choose to save the file to the local computer.
3. Make the changes and save the file.
4. To upload the file to Clavister SAG follow the steps described for file system browsing in Chapter 9, *Maintenance*.

When the file is uploaded it will look similar to the following example where the file *commonfooter.html* has been changed:

Parent Directory

commonfooter.html	Copy
commonfooter.html-light	Copy
commonfooter.html-pda	Copy
errorheader.html	Copy
errorheader.html-light	Copy
errorheader.html-pda	Copy
head.html	Copy
head.html-pda	Copy
normalheader.html	Copy
normalheader.html-light	Copy
normalheader.html-pda	Copy
numpad.html	Copy
numpad.html-light	Copy
requestraheader.html	Copy
requestraheader.html-light	Copy

Files with this color and size are a part of the installation and has NOT been modified by the administrator.

Files with this color and size are a part of the installation and has been modified by the administrator.

Files with this color and size are not a part of the installation.

Enter a directory name below and press the "Create Directory" button to create a new directory.

Enter the full path to a local file below and press the "Upload" button to upload a file to the current directory.

To remove the modified file, click **Delete** to the right of the filename.



Note

If changes are made to a file in the virtual host *Default*, these changes affect all virtual hosts. This behavior is chosen because most organizations use the same customizations throughout all virtual hosts.

To use the default page in a virtual host use the **Copy** button next to the file in the custom directory of that virtual host. This will create a custom page that overrides the custom page from the default host.

Include Files

The parts of the HTML code that are common to many pages are put in separate files that are merged into the final pages during start-up or when re-indexing files. The files can be found in the directory `/server/custom_data-public/include`.

An example is:

```
<html>
  <body>
    PARM{include:commonfooter.html}
  </body>
</html>
```

The parameter `PARM{include:<fileName>}` is replaced by the content of the file with name `<fileName>`.

Language Support

During the merge the files are translated into separate files for each language using special translation files for the configured languages.

The parameter `PARM{text-<tagString>}` is replaced by the translation of the string `<tagString>` for each language. The language files can be found in the directory `/lang` underneath the root directory.

The language files contain lines that look like:

```
<tagString> {space} <translation>
```

For example the English is:

```
pleasechooseauthmethod Please+choose+authentication+method
```

The Swedish is:

```
pleasechooseauthmethod
V&auml;l;lj+den+inloggningsmetod+du+vill+anv&auml;nda
```

Appendix A. Load Balancing

Two or more Clavister SAG servers can be run as a cluster to achieve load balancing and high availability. The servers (called *nodes* in the cluster) are connected with each other and exchange information about sessions, configuration and current load.

If the Clavister SAG cluster shares the DMZ with any other hosts, it is important to use a separate interface for the cluster traffic. This is to make sure that no other server interferes with the cluster.

There are some requirements for using a cluster:

- **Session Independent Resource Handling**

SIRH must be enabled in order to use Load Balancing. See section *General Settings* in the Clavister SAG Administration Guide.

- **License**

The license file must include a license for load balancing.

- **DNS**

The DNS Servers must be updated to forward all DNS requests to Clavister SAG.

Below is an example of a BIND v9 zone file, where two Clavister SAG servers are used in a cluster.

```
$TTL 86400
@           IN           SOA      ns1.company.com. domains.company.com. (
                2004010101 ; serial
                86400 ; refresh
                3600 ; retry
                1814400 ; expire
                86400 ; default_ttl
                )
@           IN           NS       ns1.company.com.
csns1.company.com. IN     A       10.24.19.2
csns2.company.com. IN     A       10.24.19.5
login      IN           NS       csns1.company.com.
login      IN           NS       csns2.company.com.
```

Appendix B. Parameters

Clavister SAG can handle different types of parameters to get dynamic data in web pages and paths. They can also be used to tell Clavister SAG what values to use for some Single Sign-On procedures. A parameter consist of a tag and a name. For example: *PARAM{description}*.

Parameters in destination paths and Access Control

Parameters can be used in search paths and in authentication control. For example: To make a menu entry for a user's home directory in a file share, the administrator can enter */home/PARAM{gwuid}/* in the path of the menu entry.

Special parameters used only for Single Sign-on

An administrator can use parameters to tell Clavister SAG which values to send to an internal resource on behalf of the user. This is done in *Authentication Control* in the *Advanced Options* for the resource. For example, if the credentials to login to an internal resource are the same as the credentials used to log on to Clavister SAG, the administrator can enter the parameters *PARAM{gwuid}* and *PARAM{gwpwd}*.

There are also special parameters that can ONLY be used for Single Sign-On (SSO). If information is missing in the SSO database, Clavister SAG will ask for it when the user first tries to use the resource and then add it to the SSO database.

Parameter Name	SSO	Custom Headers, Menu paths, ACL	Search & Replace	Description
PARAM{gwuid}	x	x	x	Current user's ID.
PARAM{gwuidlow}	x	x	x	Current user's ID in lower case.
PARAM{certuserid}	x	x	x	Same as LDAP attr. "Cert User ID".
PARAM{gwfdn}	x	x	x	Current user's distinguished name.
PARAM{gwpwd}	x	x	x	Current user's password (Basic/WebToken/SMSToken only).
PARAM{givenname}	x	x	x	The logged in user's given name (Basic/WebToken/SMSToken only).
PARAM{surname}	x	x	x	The logged in user's surname (Basic/WebToken/SMSToken only).
PARAM{gwssso-uid}	x			Current user's SSO entry (user id).
PARAM{gwssso-pwd}	x			Current user's SSO entry (password).
PARAM{gwssso-dom}	x			Current user's SSO entry (domain).
PARAM{gwregexpN}	x			Used in conjunction with prefetch function in form filler.
PARAM{ldap1..4}	x	x	x	Custom LDAP attribute #1 - #4.
PARAM{vhostname}	x	x	x	The first virtual host name of the current session.
PARAM{gwnodeprefix}	x	x	x	The cluster node prefix, eg. m01.
PARAM{gwhostname}	x	x	x	The default host name eg. login.gw.se.
PARAM{gwsid}	x	x	x	The user's session ID.
PARAM{gwcip}	x	x	x	The user's client IP address.
PARAM{addresspool}	x	x	x	Name of the address pool of the client. Empty if no match.
PARAM{groups64}	x	x	x	Base64-encoded list of user groups for current user. Separated with ";".
PARAM{gwresourceurl}			x	The Clavister SAG URL to access the current resource.
PARAM{gwtunnelport}			x	Client port when using Quick- or SSL tunnel mode.
PARAM{gwauthmethod}	x	x	x	Authentication method (name or CC-ID).
PARAM{function:name()}	x	x	x	Various functions described above.

Parameters in Clavister SAG web pages

Special parameters are used in the Clavister SAG web pages to get dynamic error messages or other dynamic information. The value of the parameters is set in the URL for the web page.

An example would be:

```
https://login.Clavister.se/sag-local/errormessage.html?
description=Error+Code+113
```

In this case the file *errormessage.html* will be requested with the parameter *description* set to *Error Code 113*.

The parameter *PARM{include:<fileName>}* is replaced by the content of the file with name *<fileName>*.

The parameter *PARM{text-<tagStrings>}* is replaced by the translation of the string *<tagString>* for each language. The language files can be found in the directory */lang*. The files contain lines that look like: *<tagString> {space} <translation>*. For example: *pleasechooseauthmethod Please+choose+authentication+method*

The code in the web page is: *PARM{text-pleasechooseauthmethod}*

The result in the web browser is: *Please choose authentication method.*

Sometimes you need to url encode what is sent to a web server (form based login). This done with: *PARM{function:urlencode(/PARM[gwregexp1])}*

An example use of PARM{gwuid}: Map Network drive on Windows Client

Step 1 - A tunnel resource is added to the file server at port 139.

Configure Tunnel Resource "test" a.k.a "test"

Description:

The Server Address may be an IP Address or a DNS Name.
It can also be comma separated list of addresses or DNS Names.
This is useful when load balancing between several physical servers.

Example: *mail1.company.com,mail2.company.com,10.104.1.2*

Server Address:

It is possible to specify multiple TCP and/or UDP ports.
Syntax for TCP Ports: *<port number> or tcp:<port number>*
Syntax for UDP Ports: *udp:<port number>*

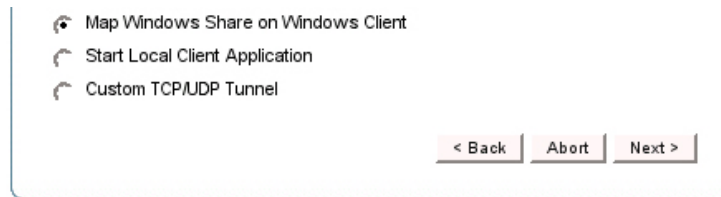
Example: *1080,tcp:6667,udp:5553*

Ports:

Skip SSL handshake: (This can be used to minimize the traffic on GPRS connections)

Step 2 - A menu entry is created for the resource using *Add new entry*. Clavister SAG lets the

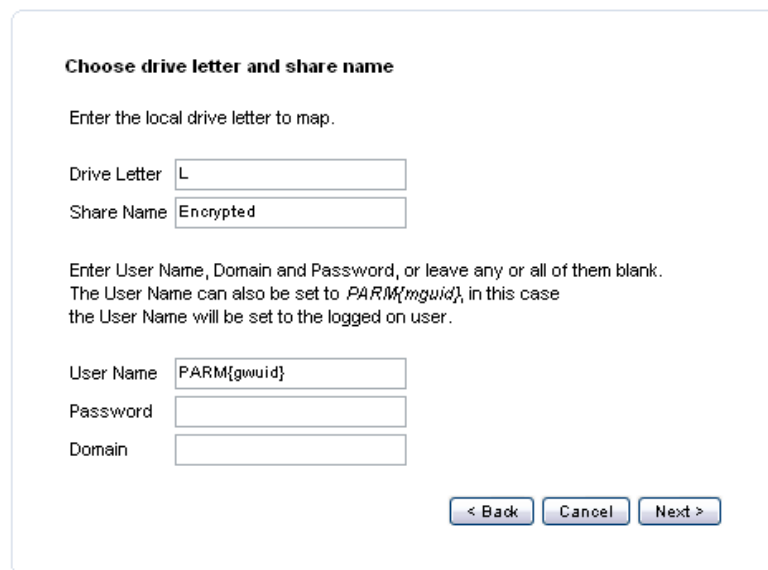
administrator select tunnel type.



A dialog box with a light blue border. It contains three radio button options: "Map Windows Share on Windows Client" (which is selected), "Start Local Client Application", and "Custom TCP/UDP Tunnel". At the bottom right, there are three buttons: "< Back", "Abort", and "Next >".

Clavister SAG suggests using *Map Windows Share on Windows Client*. Click **Next**.

Step 3.



A dialog box titled "Choose drive letter and share name". It contains the following fields and text:

- Text: "Enter the local drive letter to map."
- Field: "Drive Letter" with value "L".
- Field: "Share Name" with value "Encrypted".
- Text: "Enter User Name, Domain and Password, or leave any or all of them blank. The User Name can also be set to *PARM{gwuid}*, in this case the User Name will be set to the logged on user."
- Field: "User Name" with value "PARM{gwuid}".
- Field: "Password" (empty).
- Field: "Domain" (empty).
- Buttons: "< Back", "Cancel", and "Next >".

Enter the drive letter for the share on the client. Also enter the share name on the server, in this case the share name is *Encrypted*. The user name could be a static user name on the server. However, it is also possible to use the Clavister SAG user id by entering *PARM{gwuid}* in the User Name field. If the password field is left empty, the Windows client will ask for the password upon connection. The *Domain* field is optional.

Step 4.

Enter a description for this menu entry.

This text will be displayed in the navigation window, so it's recommended to try keeping it short.

Description

Also choose if the user should be asked to accept or deny every connection made to the tunnel.

Dialog

If you specify a group below, then this menu entry will be selected instead of the welcome page for every users that is a member of the specified group.

Autostart Group

It is also possible to select that this menu entry shall be visible in the special Autostart Navigator.

Hide Navigator

Autostart Navigator

The menu entry is named in the usual way. Here it is called *Map Drive Encrypted*. When **Next** is pressed, the menu entry is created with the correct parameters. When the menu item is selected in the navigator, Windows maps the disk.

Appendix C. External LDAP Attributes and Objects

For Clavister SAG to be able to store Clavister SAG specific information in an external LDAP, some extra attributes and an object class is needed in the LDAP server.

Attributes

These attributes have unique Object IDs. Clavister SAG's OID number is: "1.3.6.1.4.1.5089.101".

The individual attributes have the Object ID: 1.3.6.1.4.1.5089.101.* where the * is one of the values from the *Last Digit(s)* column in the table below.

Assigned LDAP attribute	Type (Syntax)	Last Digit(s) in OID	Remark
sagLoginFail	int	.1	
sagLoginFailTimestamp	int	.2	
sagStatus	int	.3	
sagMemberOf	int	.4	
sagExpires	int	.5	
sagSMSPassword	string	.10	
sagSMSPasswordTimestamp	string	.11	
sagSMSOldPasswordList	string	.12	
sagSMSCellphone	string	.13	
sagWebPassword	string	.20	
sagWebPasswordTimestamp	string	.21	
sagWebOldPasswordList	string	.22	
sagEmailAddress	string	.23	Optional
sagComment	string	.24	Optional
sagCertUserID	string	.25	Optional

For example, the attribute *sagLoginFail* has the complete object id: 1.3.6.1.4.1.5089.101.1.

The attributes should all be single value attributes that are case insensitive.

Type with Active Directory

When specifying the *Type* with Microsoft Active Directory, a type of *int* in the above table is equivalent to *Integer* in AD. A type of *string* in the above table is equivalent to *IA5-String* in AD.

Type with Novell

A type of *int* in the above table is equivalent to *Integer* with Novell. A type of *string* in the above table is equivalent to *Octet String* with Novell.

Object Classes

Only one (auxiliary) object class is needed for Clavister SAG. (This is not needed for Microsoft Active Directory Servers).

Object class name	Complete OID
sag	1.3.6.1.4.1.5089.102.1

Appendix D. Microsoft Active Directory Integration

This section contains information about how to set up Clavister SAG to use Microsoft Active Directory as an external user database.



Caution

Changes made to the active directory schema are permanent. Therefore, make sure the necessary backups exist for the server before continuing.

Schema Snap-in for Management Console

Clavister SAG needs some attributes to be added to the Active Directory Schema. To add attributes the administrator can use the Active Directory Schema snap-in for management console. Start the management console by typing *mmc* in **Start => Run** and pressing **Enter**.

For domain servers running Windows 2000:

The snap-in is not installed by default in the Windows 2000 installation, but the *Adminpak.exe* program on the Windows 2000 Server CD-ROM will install it.

Add the snap-in to the management console (see below).

Once the snap-in is added, the top-level entry **Active Directory Schema** is added to the navigation pane. Right-click it and choose **Operations Master**. In the resulting dialog box, make sure that the checkbox labeled **The Schema May Be Modified On This Domain Controller** is checked.

For domain servers running Windows 2003:

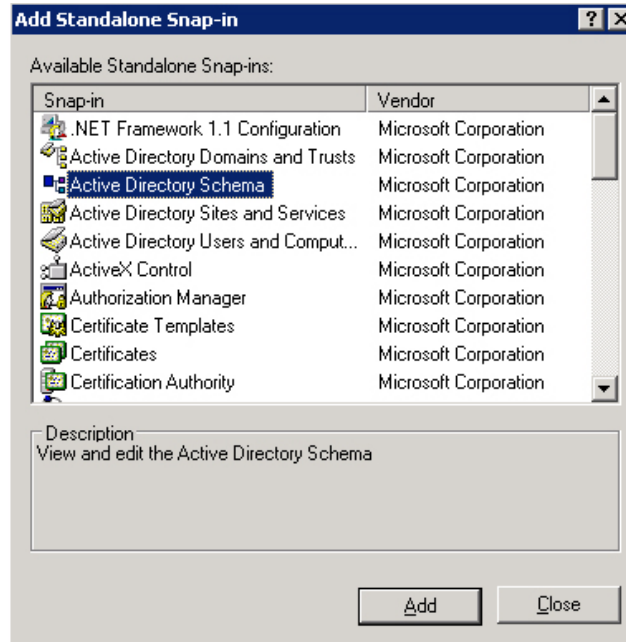
The snap-in is installed by default but must be enabled. This can be done by entering the following command in a console:

```
> regsvr32 schmmgmt.dll
```

This will enable the snap-in which then can be added in management console.

Add the Snap-in

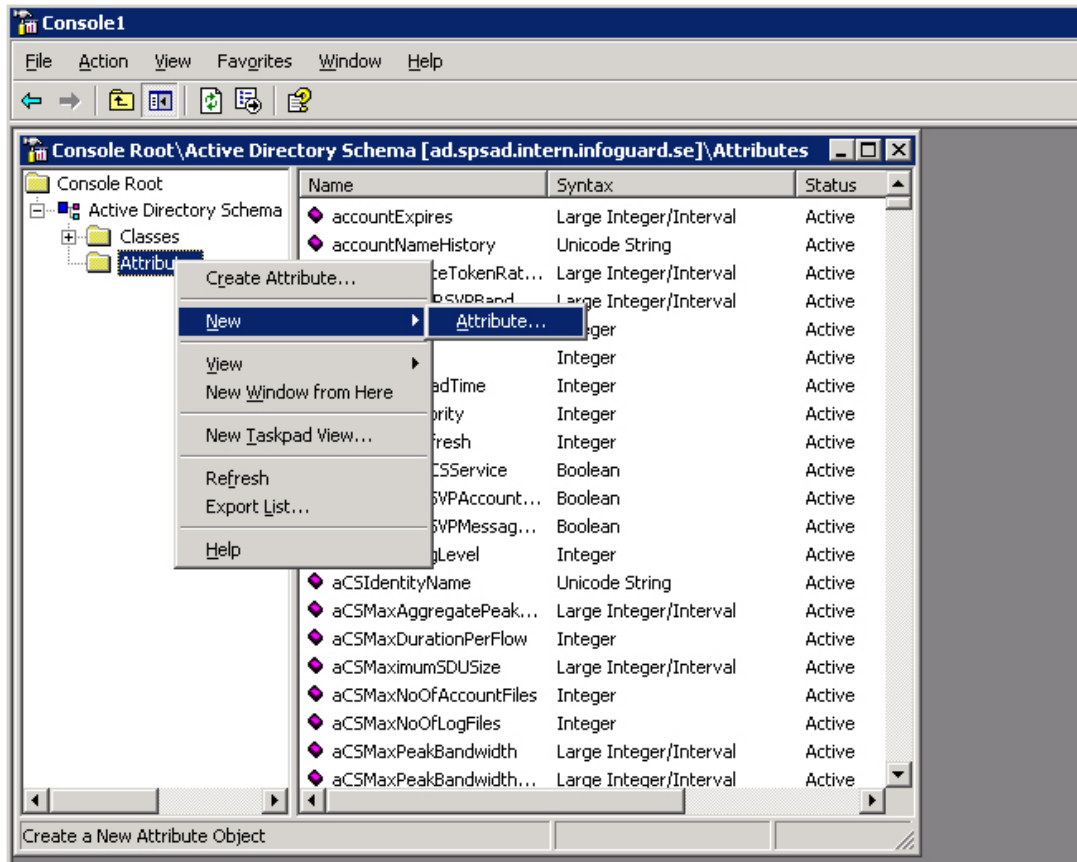
Add the snap-in by selecting **Add/Delete Snap-ins** under the File menu. Select the **Active Directory Schema** snap-in from the list of snap-ins.



Press Add and press OK in the next dialog to return to the console root tree.

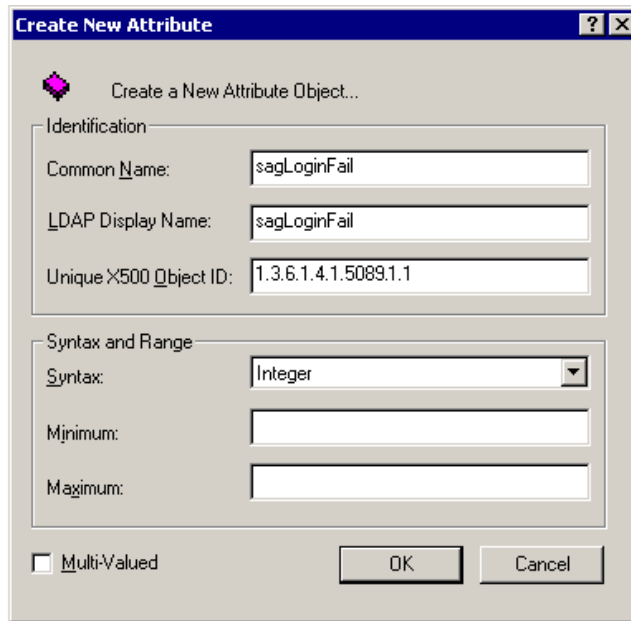
Add Attributes

By right-clicking the **Active Directory Schema => Attributes** select **New Attribute**.



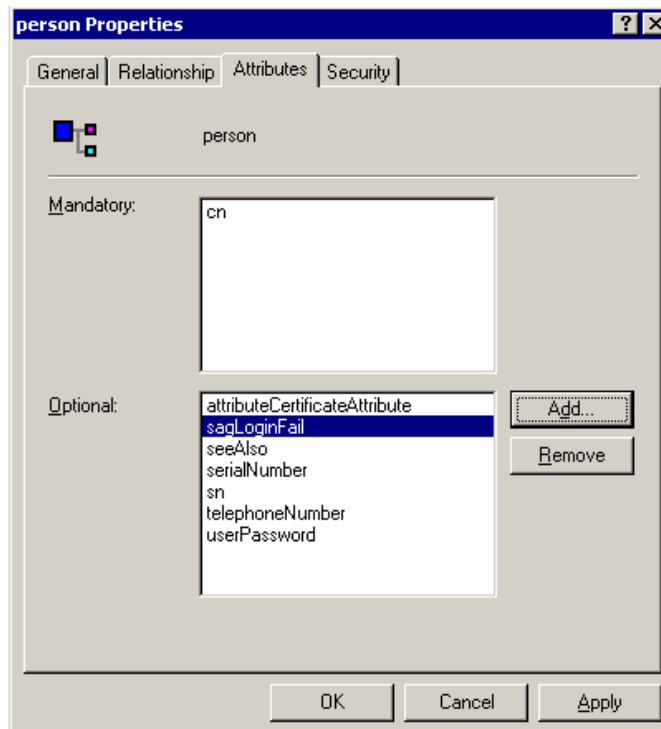
The system will display a warning, telling you that adding attributes to the schema is a permanent operation. Press **Continue**.

The new attributes and their respective OID and syntax can be found in Appendix C, *External LDAP Attributes and Objects*. Make absolutely sure that the information is correct before adding each attribute. Changes made are permanent. Below is an example of how the information should be added.



Adding attributes to the object class *person*

The attributes must then be added to the object class *person*. This is done by viewing the properties for the class *person* under the Classes item in the tree.



Add all of the sag-attributes as optional attributes to the object class *person*.

Configuring Clavister SAG to use an Active Directory Server



Tip

Make sure that the administrator can log on to Clavister SAG even if the configuration for the active directory fails. This can be done by either configuring another virtual host to use an internal LDAP, or by temporarily allowing test logon from the IP of the administrator's computer during configuration of the LDAP service.

LDAP Settings

In Control Center, configuration for the user database can be found under the **LDAP Settings** tab. Below is an example of how the settings might look for Active Directory.

LDAP Settings

Server Type		(requires restart)	
Built in	<input type="radio"/>	eDirectory	<input type="radio"/>
External	<input checked="" type="radio"/>	Active Directory	<input checked="" type="radio"/>
External using encryption	<input type="radio"/>	Other	<input type="radio"/>
User Password Handling			
Allow Password Change	<input checked="" type="checkbox"/>		
Warn time	14	Days	
Cache Settings			
Max Cache Age	60	seconds	
Connection Settings		(requires restart)	
LDAP Server and port	10.103.10.19	389	
User (dn)	cn=admin,dc=local		
Password	*****		
Search Settings			
Use nested groups	<input checked="" type="checkbox"/>		
User search base	ou=users,dc=local		
Group search base	ou=groups,dc=local		
Product Group	cn=users,ou=groups,dc=local		
Use user location in ACL	<input checked="" type="checkbox"/>		
Container objectClasses	organizationalUnit,container (Separate with comma)		
Object Classes			
Product objectClass	sag		
User objectClass	person		
Group objectClass	memberOf		

LDAP Attributes

The Control Center features the option to load default attribute settings for the most commonly used LDAP servers. To load the default settings for Microsoft Active Directory, select **Active Directory** in the drop down box and press **Save/Update**. The default attribute settings are now loaded.

For information about the fields, please see Section 6.5, "Local Database Settings".

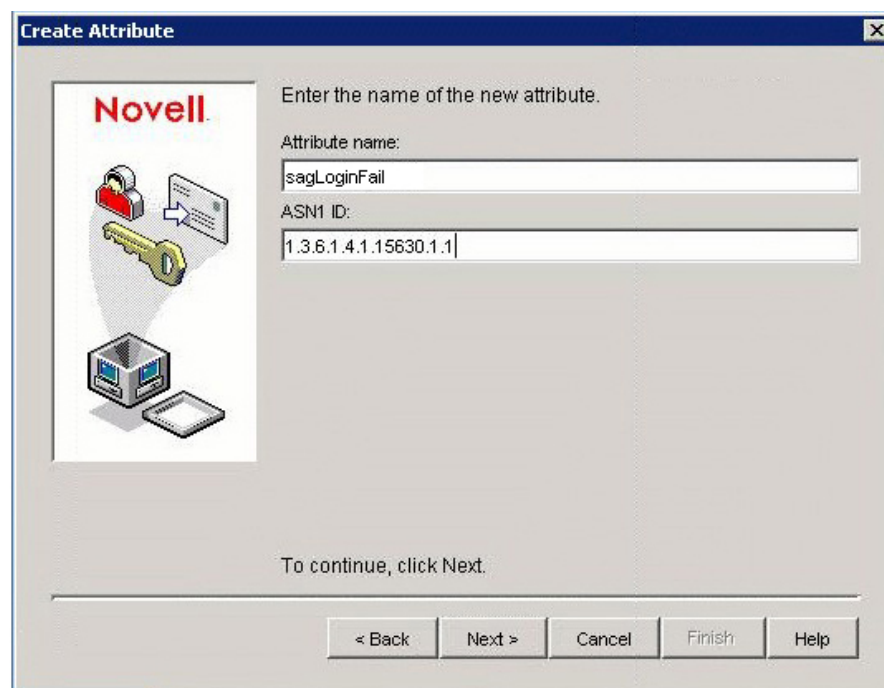
Appendix E. Novell eDirectory Integration

This section contains information about how to set up Clavister SAG to use Novell eDirectory/NDS as an external user database.

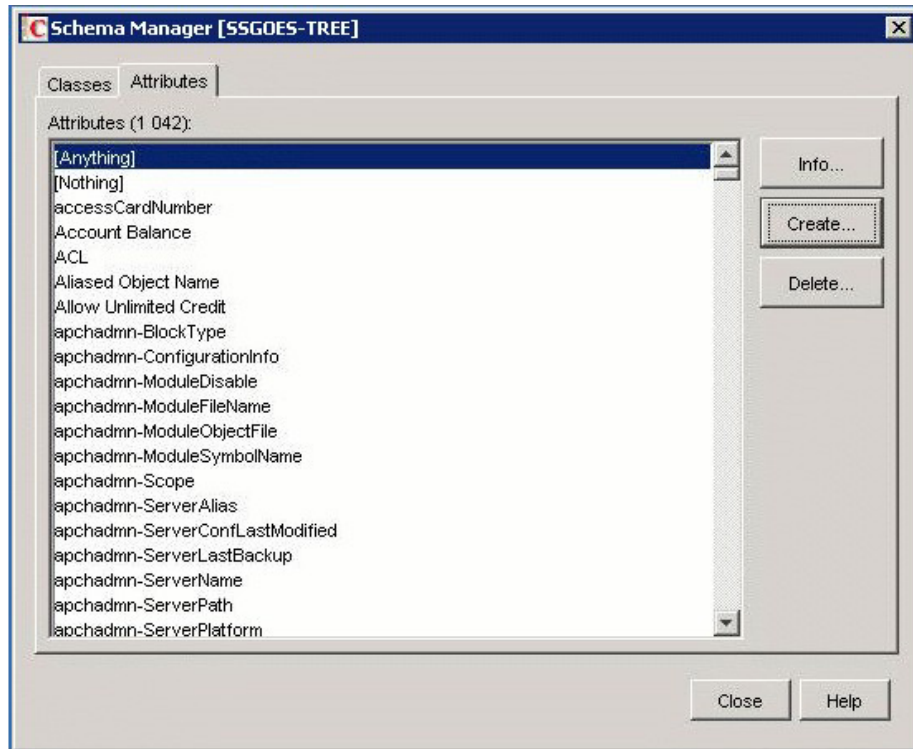
Clavister SAG needs some attributes to be added to the schema. To add attributes the administrator can use the **Novell ConsoleOne** application. Open **Schema Manager**.

Create Attributes

First create the new attributes. The attributes to create can be found in Appendix C, *External LDAP Attributes and Objects*.



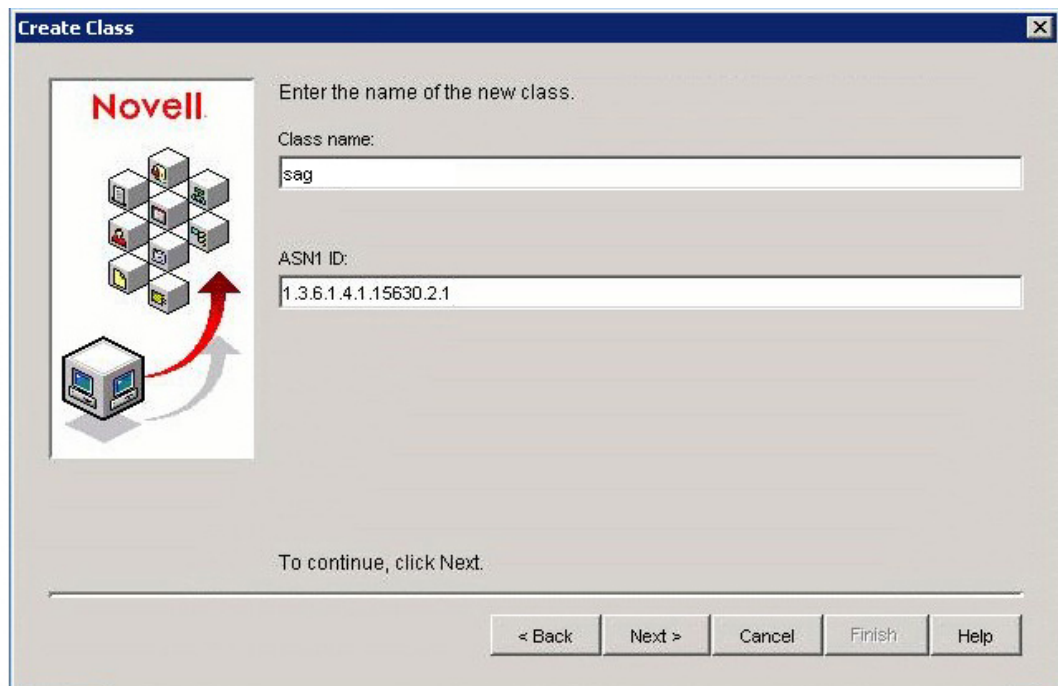
To add a new attribute, press **Create** under the **Attributes** tab.



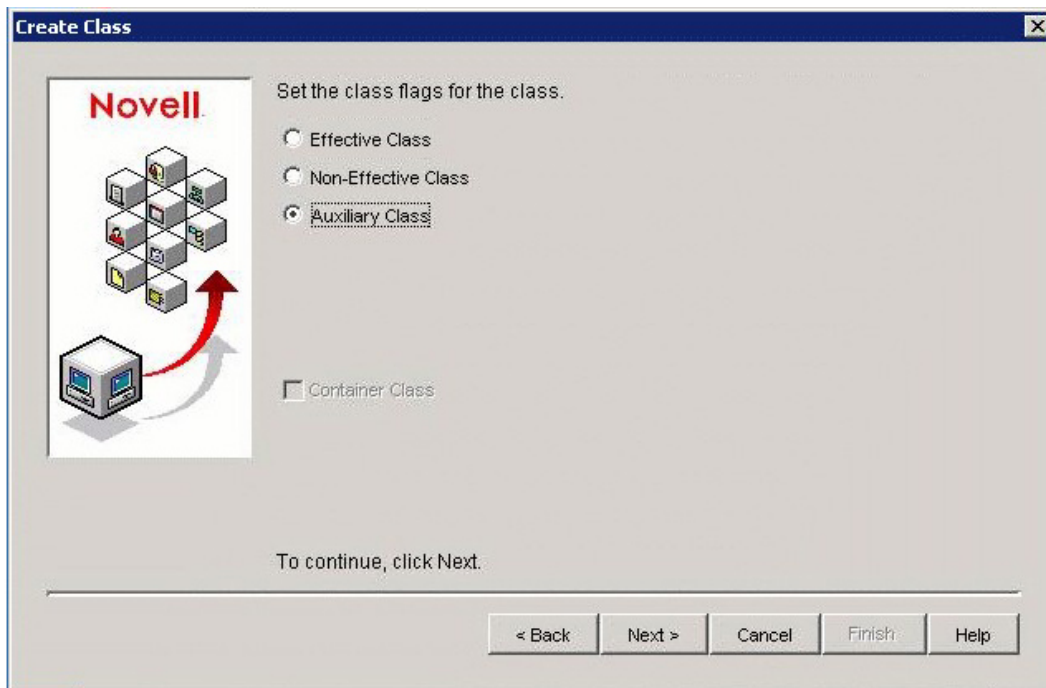
Select the correct syntax for each attribute, *Integer* or *Octet String*, depending on which attribute. All attributes should be *Single valued*.

Add Object Class

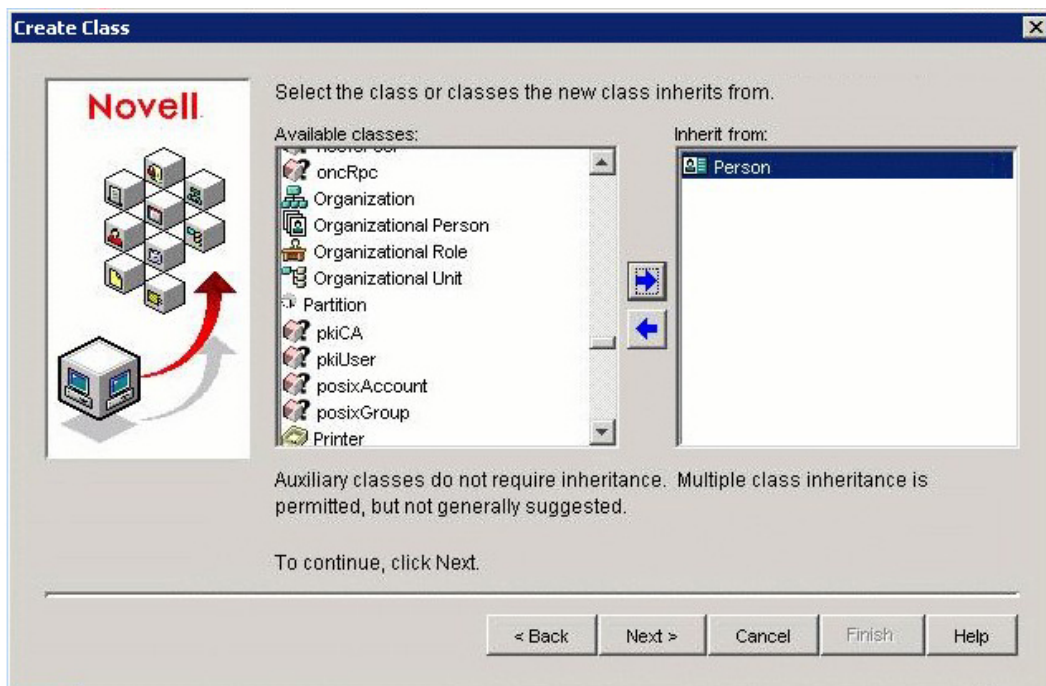
Under the **Classes** tab, select **Create** to create the class.



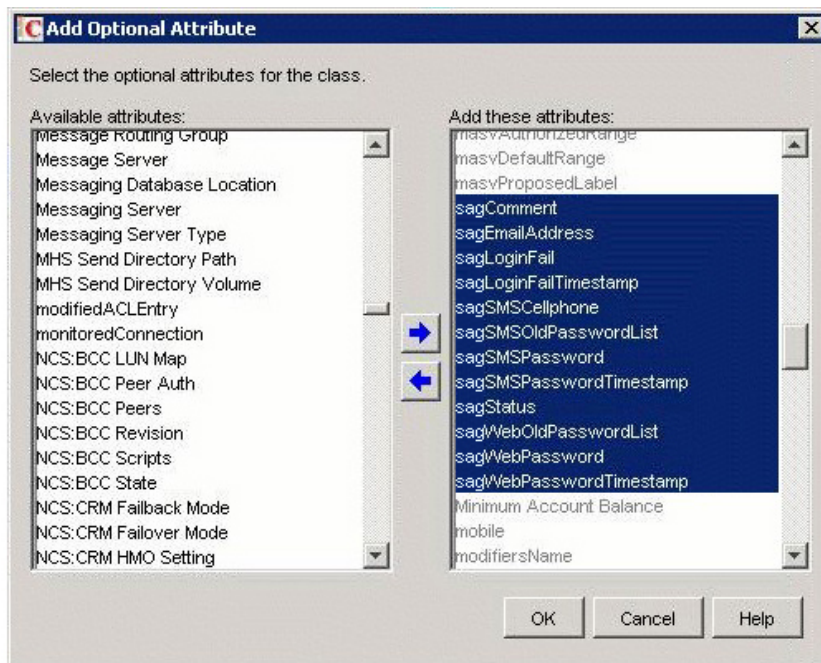
The new class should be an auxiliary class.



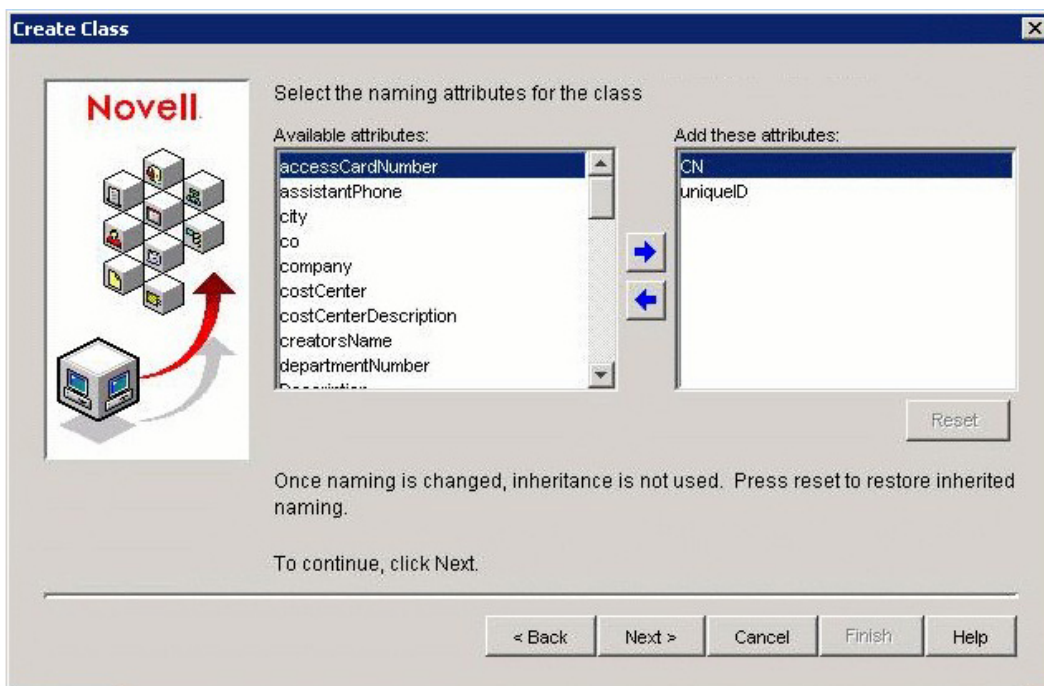
Let the new class inherit the object class *person*. Leave the **Mandatory Attributes** as they are.



Add the *sag** attributes you just added to the list of optional attributes.



Use the default naming attributes. We are now ready to configure Clavister SAG to use this eDirectory.



Appendix F. Message Center

This appendix covers usage of the *Message Center* module in Clavister SAG. The purpose of Message Center is to allow the administrator or dedicated users to send SMS and email messages to users registered in Clavister SAG. The Message Center is ideal to use for sending status messages about resources within Clavister SAG to affected users.

Message Center is accessed through the navigator in Clavister SAG.

General Buttons

There are three general buttons that are common in Message Center.



- **< Back**
Cancel the current stage and go back to the previous stage.
- **Abort**
Cancel the current stage and go back to the beginning.
- **Next >**
Accept the settings and continue to the next stage.

Message Center use is divided into 6 stages which are described below

Step 1 - Enter a message.

Enter Message

This is a wizard used to send messages to users with SMS and/or e-Mail.

Choose preferred delivery method

Send both SMS and e-Mail
 Send only as SMS
 Send only as e-Mail

Enter SMS message (MAX 160 characters)

This is a text message sent as an SMS

123 Characters left.

Enter e-Mail message

Check if same as SMS message.

Subject: Message from SAG

This is a test message sent as an e-mail
//Your SAG Administrator|

Next >

- **Choose preferred delivery method**
Select if the message shall be sent as both as SMS and email or only as SMS or email.
- **Enter SMS message**
Enter a message that will be sent as a SMS message. The message can only contain 160 characters.
- **Enter e-Mail message**
Enter a message that will be sent as an email message.
- **Check if same as SMS message**
Check this check box if the same message shall be sent both as SMS and as an email message. This is the default behavior.
- **Subject**
The subject of the email message.

Stage 2 - Select virtual hosts.

This stage is only available if there are any virtual hosts configured in Clavister SAG.

Select one or more Virtual Host and click **Next >**.

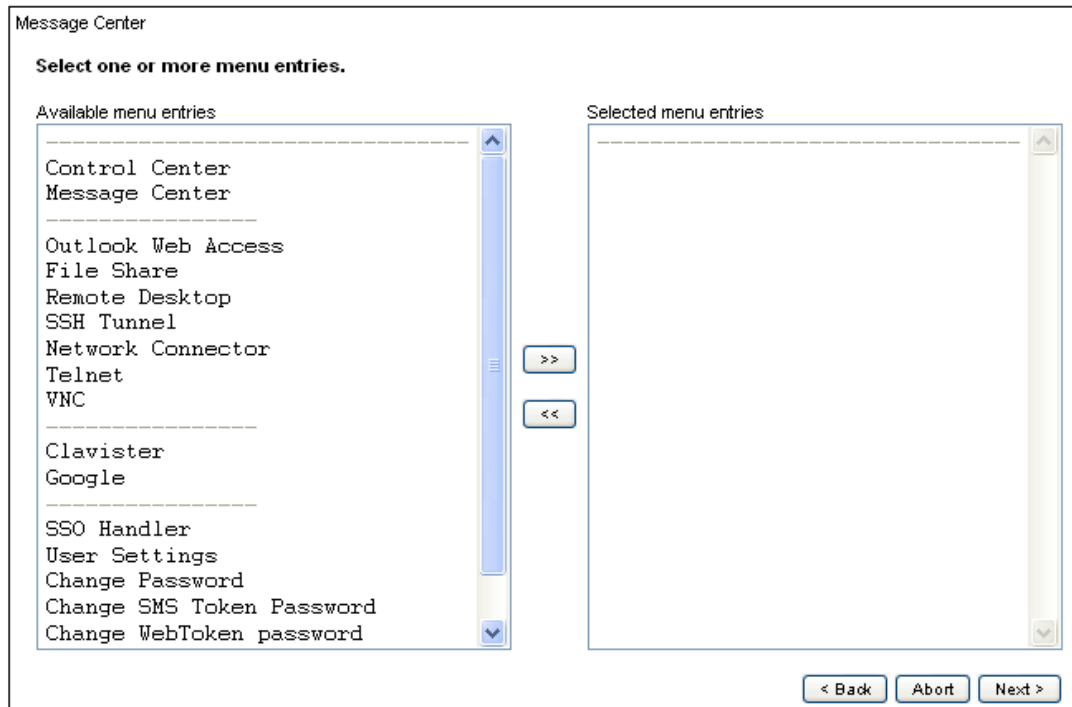
Step 3 - Choose selection method.

There are 5 different ways to select users that shall receive the message.

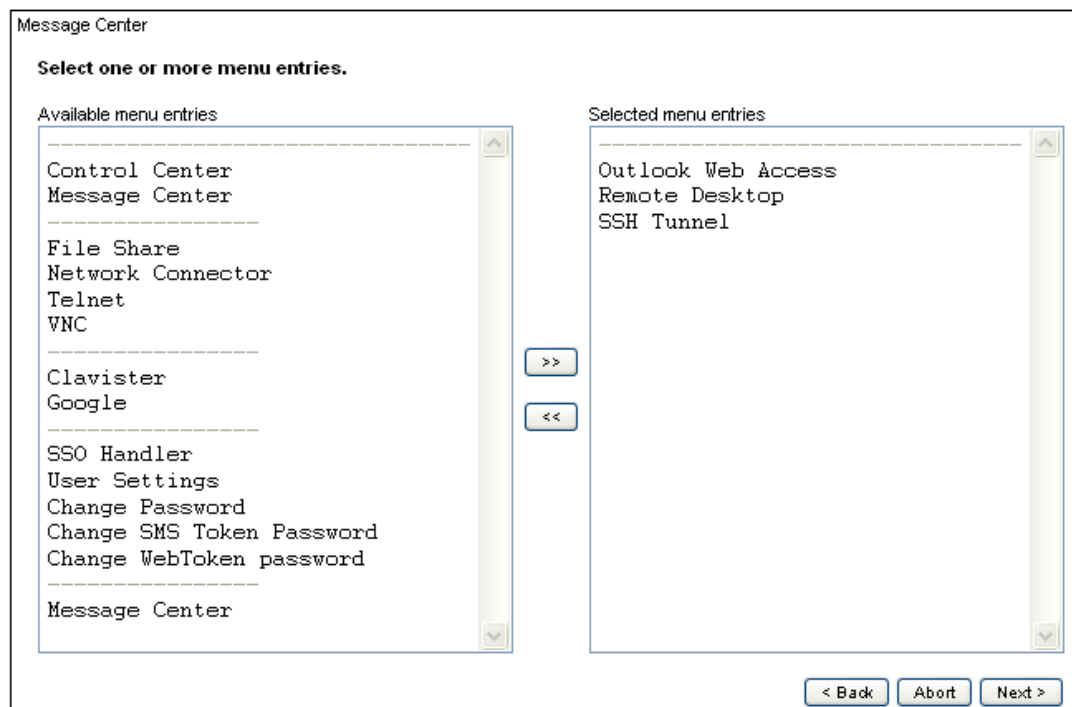
- **Select all users**
This will select all users, however it is possible to remove users from the selection in the next stage.
- **Select users by selecting one or more groups**
This will select users that are members of the groups that can be selected in the next stage.
- **Select users by selecting one or more menu entries**
This will select users that have access to the menu entries that can be selected in the next stage.
- **Select users by selecting one or more resources**
This will select users that have access to the resources that can be selected in the next stage.
- **Select users individually**
This is the opposite of **Select all users**.

Step 4 - Selecting menu entries, resources or groups.

Depending on which selection method was chosen in the previous stage, this stage will be used to select menu entries, resources or groups.



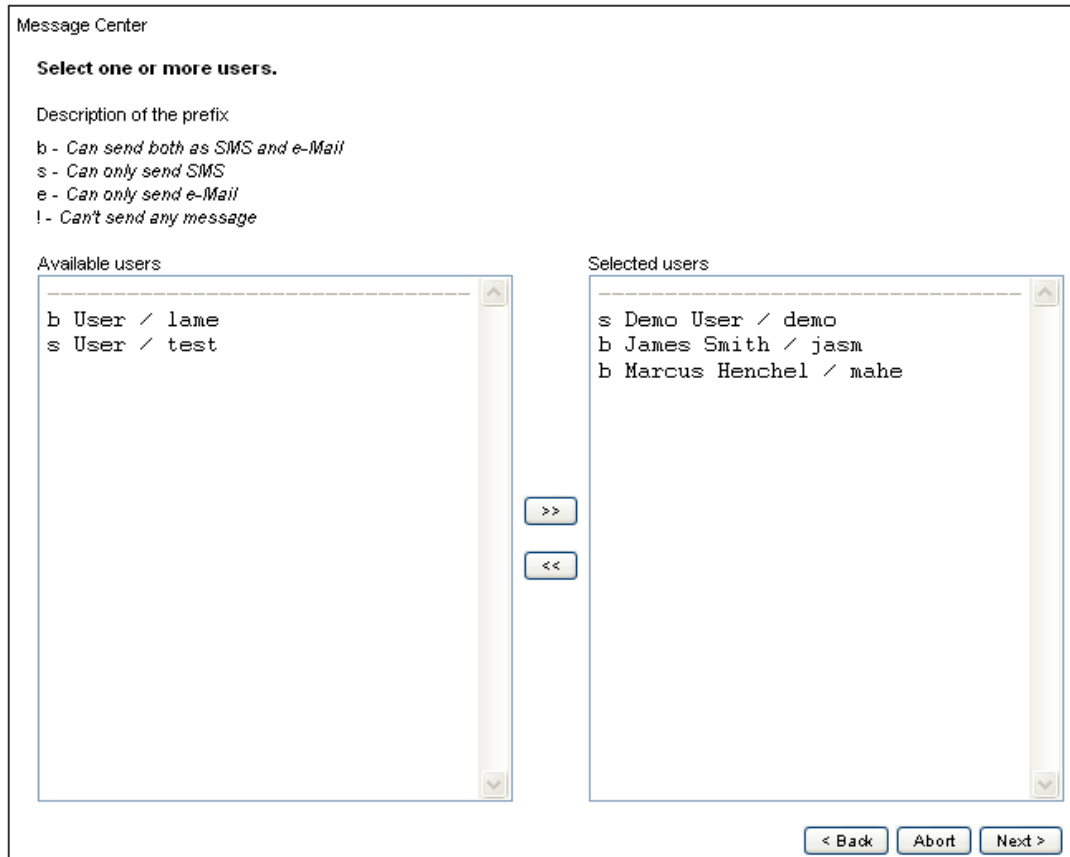
Select the menu entries and click on the >> button to add them to the list of menu entries that will be used to select users in the next stage.



When done selecting menu entries, click **Next >** to continue to the next stage. Note: To remove selected entries, select them in the right selection box and click on the << button.

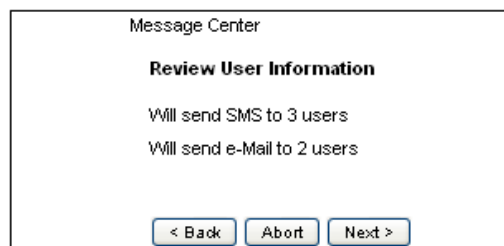
Step 5 - Selecting or removing users.

If menu entries or groups has been selected in the previous stage, then the users that have access or are members of the selected groups will be preselected in this stage.



It is now possible to select more users or remove users by using the << and >> buttons. When done, click on the **Next >** button.

Step 6 - Summarize before sending.



- **Will send SMS to X users**
This indicates how many SMS that will be sent.
- **Will not send any email**
This indicated how mail emails that will be sent.

When the **Next >** button is clicked, the message will be sent to the selected users. A status page will be shown where real time information about the sending progress and status of each message is displayed.

Alphabetical Index

A

- access control, 38
- address pools, 27
- authentication, 93
 - groups, 102
 - methods, 100
 - RADIUS, 93
 - web, 94
- authenticator, 61

B

- backup, 105

C

- cache control, 45
- client settings, 86
- configuration & administration, 8
- control center, 8
- creating menu entries, 49

F

- file system browsing, 106

I

- include files, 112

L

- language support, 112
- layout settings, 91
- ldap settings, 77
- license installation, 104
- log viewing, 15

M

- maintenance, 104
- modifying pages, 111
- monitoring, 10

N

- network connector, 72
 - client, 74
- node settings, 67

R

- RADIUS servers, 93
- resources, 28
- root directory structure, 106

S

- server settings, 63
- statistics, 16
- supervision settings, 66

T

- timeout settings, 89

U

- upgrading Clavister SAG, 104
- URL converter, 83
- user agents, 86
 - adding, 87
 - testing, 88

W

- web authentication, 94

V

- view order, 57
- virtual host, 84
 - selector, 9