GateManager Administrator's Guide

This document is intended for all GateManager administrators. It includes information about the complete documentation package.

Version: 4.0, 2009-04-21

Table of Contents

1. About documentation for GateManager

Standard GateManager documentation includes the following:

- *Installation and Operations Guide*. This guide covers how to install the Linux operating system and GateManager Server and Proxy; how to upgrade; how to manage backups). This guide includes sensitive information intended only for the Owner (that is the person or authority with the highest legal responsibility for a GateManager installation.
- *Server Setup and Management Guide*. This guide shows how to set up domains, roles, accounts and product support using the GateManager Console; and how to carry out a few additional tasks using other tools). This guide includes sensitive information intended only for the Owner.
- Documentation for every day use of the GateManager Console. This is where you will find information on enrolling Appliances, creating alerts, managing your own account, and so on. There are also glossaries.
    - *Administrator's Guide*. This includes most of the information in the *Online help* along with quite a lot more.
    - *Online help* for the Console. This puts selected information at your fingertips. The online help is available to you as soon as you download and launch the Console. You do not need to be logged on to the GateManager to use the help system.
- *Developer's Guide* to integration with a backend application via Web Services.
- *Release Notes*

When you participate in a pilot project or roll out your own solution, you will be provided with additional information specific to your setup.

1.1. About this document

The GateManager and the products supported by it have all evolved quite a lot over time, and so has this Administrator's Guide.

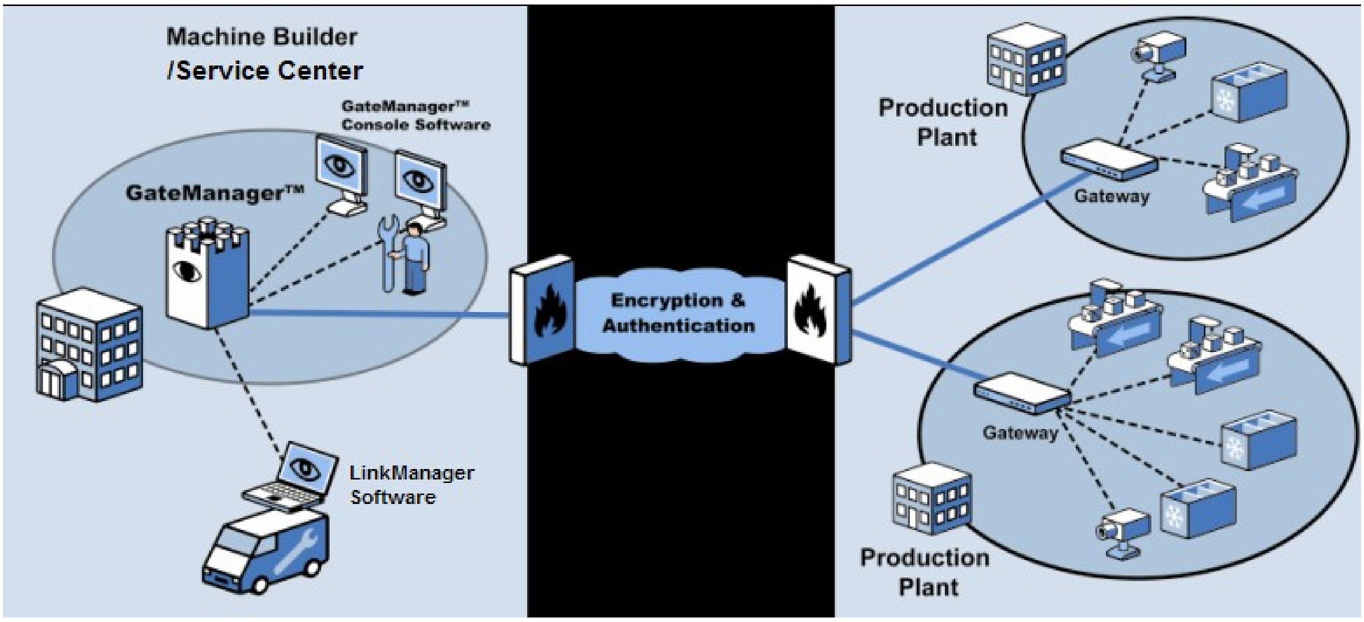
As a consequence, the illustrations and screen shots in this guide have been added and replaced gradually over time – possibly leaving some minor inconsistencies between the illustrations and the actual screen contents you will see in the latest version of the GateManager Console.

We hope that you still find the information in this guide useful, despite those minor inconsistencies.

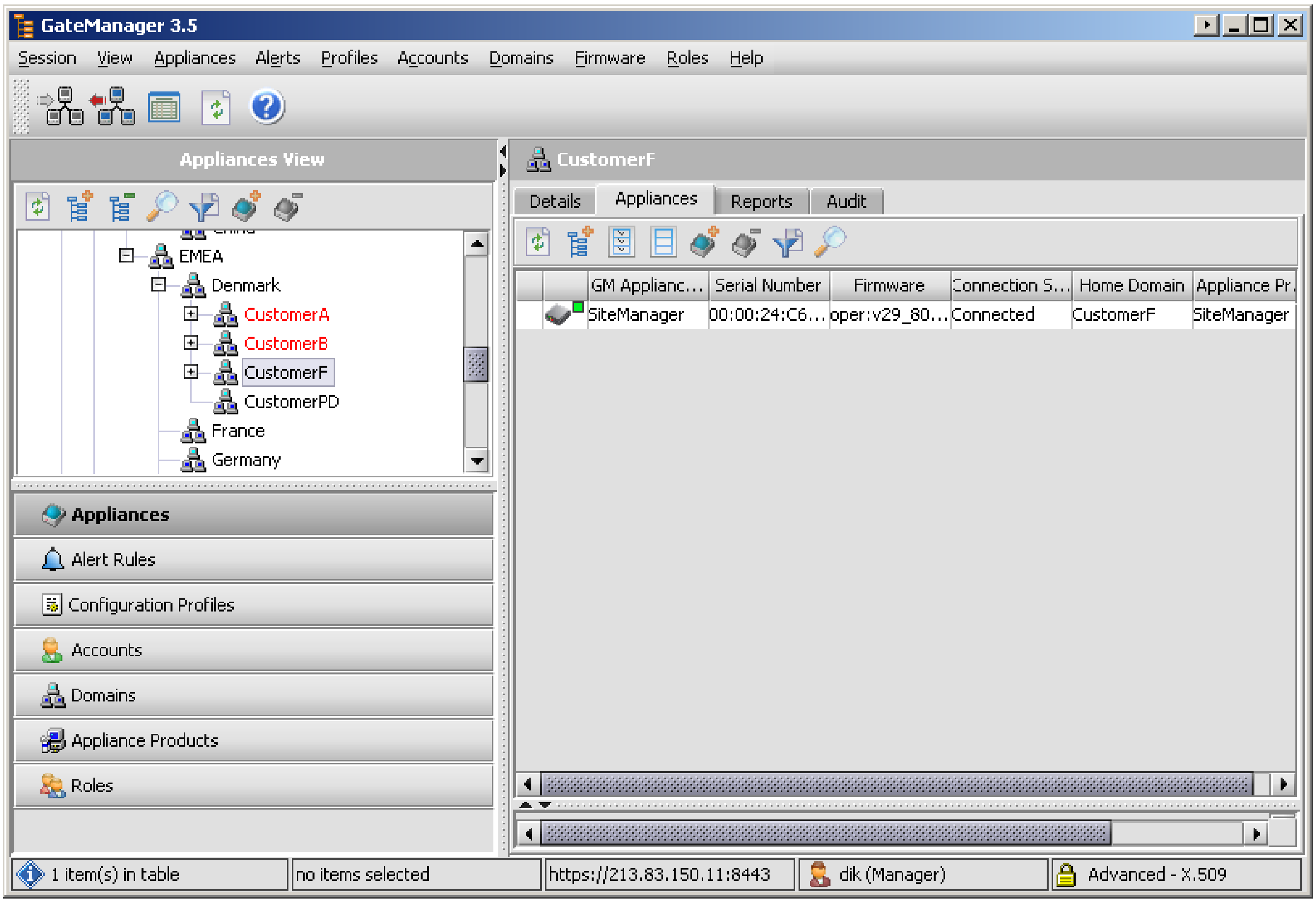
The Secomea documentation team

2. The GateManager Console

The GateManager Console is the administrative interface to the GateManager and all the equipment (Appliances) monitored by it.



2.1. Console functions



GM Applianc…	Serial Number	Firmware	Connection S…	Home Domain	Appliance Pr…
SiteManager	00:00:24:C6…	oper:v29_80…	Connected	CustomerF	SiteManager

1 item(s) in table | no items selected | https://213.83.150.11:8443 | dik (Manager) | Advanced - X.509

The GateManager Console is primarily used for administration and maintenance of the solution infrastructure - for example, attaching appliances to domains, managing and tracking users, backing up configurations, updating software, defining and assigning alerts.

It also gives a user several different views of all the Appliances he or she has the right to work with - and supports working with individual Appliances, for example by displaying an Appliance's own device logs and providing the Go-to-Appliance function.

Field Engineers will very rarely, if ever, use the Console. Thwy will use th LinkManager to access remote Appliances.

There are several different kinds of users: GateManager Console users, LinkManager users, backend application integrators. All kinds of users are created and managed via the GateManager Console.

2.2. Network and firewall configurations for Console use

If the Console is not in the same local network as the GateManager, the Internet firewall through which the Console connects to the Intermet may have restrictions on traffic going from the local to the public network which may be blocking access to the GateManager. If this is the case, you may need to give the following information to your systems or security administrator:

The following openings must be configured.

To be able to use the GateManager Console at all:

Allow TCP outgoing to the GateManager Server address(es) on port 443 (https) - or other port (e.g. 8443) assigned by GateManager installation and operations personnel. The firewall must accept encrypted traffic on the selected port.

To be able to use the option "Go to Appliance" (GTA):

Allow TCP outgoing to the GateManager Proxy address(es) on port range 55000-59999 - or other port range assigned by GateManager installation and operations personnel.

2.3. System requirements for the GateManager Console

You must have a PC suitable for running the GateManager Console, which is your interface to the GateManager Server. The PC must run minimum Windows 2000 Service Pack 4, Windows XP Service Pack 2, or Windows Vista.

Minimum system requirements for running the GateManager Console:

- RAM: 256MB
- CPU: PIII or AMD 1.00GHz processor
- Hard Disk Space: 100 MB free space

The GateManager Console includes a dedicated copy of the Java™ 2 Runtime Environment (J2RE) software. This J2RE installation will not interfere with any other copies of Java or Java Runtime that might be installed on the computer.

2.4. Becoming a Console user

- **IMPORTANT**: The following steps are to be used by all GateManager administrators *except* the Owner, i.e. the primary responsible party for a GateManager installation. The Owner should use the instructions provided in the *Server Setup Guide*.

1. Before you begin, you must have received a user name, password, and (in most cases) X.509 certificate. The e-mail with the certificate has instructions about what to do with it.
2. Install and launch the console on your PC (see "Install and launch the Console" page 9).
3. The first time you start the console, you must set up a connection (see "Connection Setup" page 10). The connection must be defined before you can log in.

2.5. Install and launch the Console

Following are the instructions for first-time installation.

1. Copy or download the GateManager Console installation program to your PC.
2. Double click the installer program, and follow the instructions to install it on your PC.
3. Start the Console from the Start menu, All Programs, Secomea GateManager Console item.
4. Or double click on the GateManager Console shortcut to launch the Console.

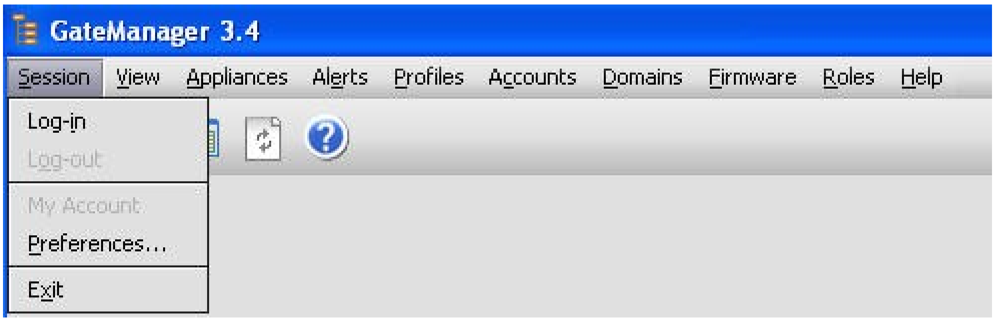
- **NOTE**: When you login, the console automatically checks for updates from the GateManager Server.

2.6. Open Login Dialog

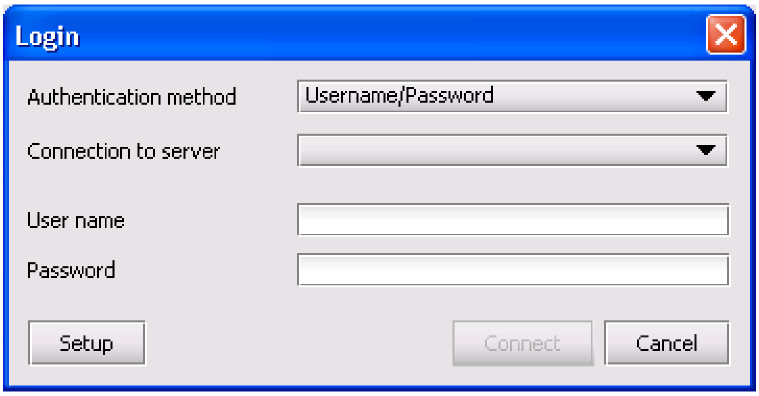
Click login on the main tool bar.

or

Select **Session > Login** from the main menu.



Result:



Authentication method: Username/Password

Connection to server:

User name:

Password:

If the **Connection to server** list is empty, as it is on this screen shot, go to Connection **Setup** (page 10).

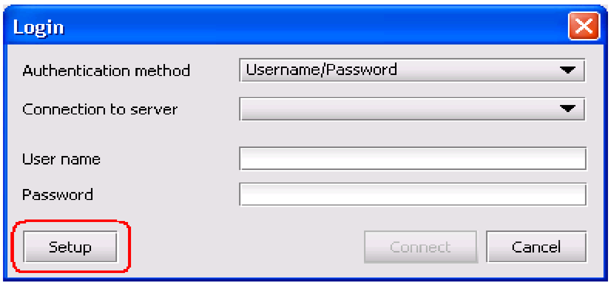
Otherwise log in (see "Login" page 11).

2.7. Connection Setup

- **IMPORTANT**:

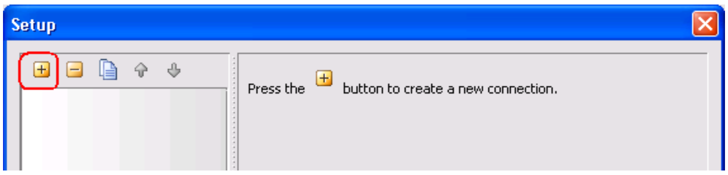
  Although the path to selecting **Setup** goes through the login screen, you can only add, edit or delete a connection while you are *not* logged in.

1. Open the **Login** dialog (see "Open Login Dialog" page 9).
2. Instead of logging in, click **Setup**.



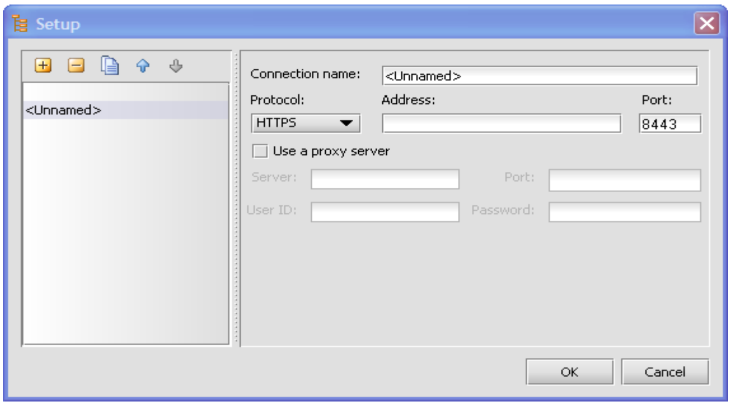
Authentication method: Username/Password

3. Result:



Press the ⊞ button to create a new connection.

4. Click the add button ⊞.
5. Result:



Connection name: <Unnamed>

Protocol: HTTPS

Address:

Port: 8443

☐ Use a proxy server

6. Fill out the fields.

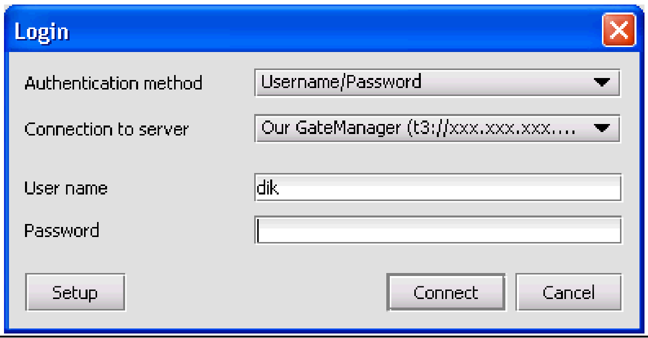
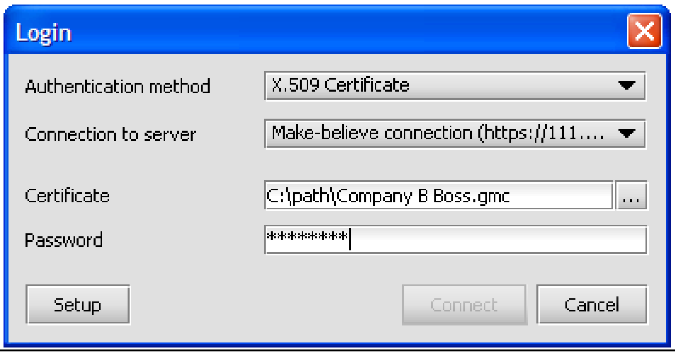
Field	Comments
Connection name	Delete the text **<Unnamed>** and type in a name for the connection.
Address	Type in the IP address or host name for the GateManager Server.
Protocol and Port	Starting with GateManager 3.4, the protocol is always **HTTPS.** Unless otherwise instructed, leave the Port set at the default **8443**.
Use a proxy server	Select this if the PC running the Console is behind an HTTP proxy. (Do not confuse this with the GateManager Proxy, which is the part of the GateManager that the Appliances connect to). Fill out **Server**, **Port**, **User ID**, **Password**.

7. If you want to define an additional connection, click the add button again.
8. Save changes and close the dialog by clicking **OK**. This will bring you back to the **Login** dialog.

2.8. Login

- Before you can login you must have defined at least one **Connection** (see "Connection Setup" page 10).

1. Open the **Login Dialog**.
2. Select **Authentication method** from the dropdown. This will either be **Username/Password** or **X.509 Certificate** ("X.509 Certificate - logging on without it" page 11).
3. **Connection to server**. This is the connection from your Console to the GateManager Server. If you have defined more than one Connection, take care to select the correct connection for the session you will be starting.
4. Do one of the following, depending on the authentication method chosen, i.e. User Name or X.509 certificate.

User name	Type in your **User name**. The name is case-sensitive.  Login Authentication method: Username/Password Connection to server: Our GateManager (t3://xxx.xxx.xxx.... User name: dik Password:
X.509 certificate	Using the **ellipsis button** ..., browse to your certificate and select it. The GateManager login dialog starts the search for the certificate in **My Documents** on your PC. If you have chosen another location, just navigate to it. The login dialog will remember your choice and suggest it next time you log in.  Login Authentication method: X.509 Certificate Connection to server: Make-believe connection (https://111.... Certificate: C:\path\Company B Boss.gmc Password: *********

5. **Password**. A password is necessary regardless of authentication method. Type in your password. The password is case-sensitive. *Authentication will fail if you use the wrong case*.
6. Click **Connect**. The Login screen will close.

2.8.1. X.509 Certificate - logging on without it

- **IMPORTANT:** If you have been given a *choice* of using the **X.509 certificate** or the **User name**, please note the following:

  Any time you log in by **User name**, *your privileges for that session are limited to read-only*. If you look at My Account (see "Managing your own Account with "My Account"" page 15), you can display the privileges that you have when logged in using the certificate.

2.9. How to remove the Console

1. In the Windows Control Panel, select the Add/Remove Programs icon.
2. Locate the Secomea GateManager Console in the program list
3. Click on the Remove button and follow the instructions.

3. Session Preferences for Console

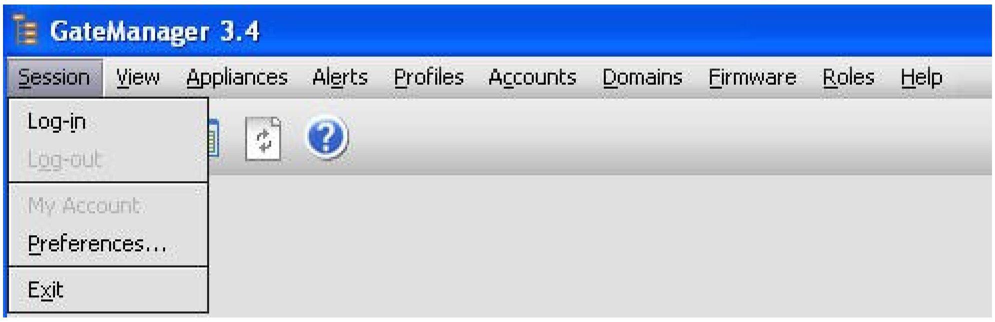
You may set the Console Session **Preferences** at any time. It doesn't matter whether you are logged in or not because the preferences are applied to the PC running the Console, and not the user.

Changes take effect as soon as you save them with an **OK**.

Preferences are remembered from session to session even after an upgrade of the Console (the settings are stored in an xml file which is not over-written in a standard upgrade).

3.1. Opening the Session > Preferences dialog

To open the **Preference** Dialog, click ▦ on the Main Tool Bar, or select **Session > Preferences** on the Main Menu.



3.2. Preferences for "Help" browser (Program)

By default, the PC's default browser will be selected, for example `C:\Program Files\Internet Explorer\IEXPLORE.EXE`. or

`C:\Program Files\Mozilla Firefox\firefox.exe`.

If you want to use a different browser for help, click the ellipsis button ... and navigate to an alternative browser.

For information on *why* you might want to select a different browser, see Optimizing your browser for online help (see "Browser for online help" page 78).

3.3. Go to Appliance (GTA Services) on the GateManager Console

In order to use **Go to Appliance**, a **Service** must be defined in the Console. The Service Name must also be known to the Appliance.

- **GateManager Console**: A GTA Service definition consists of a **Service Name** and an **Application/Command** string. The Application/Command String in the GTA Service on the Console looks up values on the Appliance.

  In many cases, if the protocol needed is http, https, or telnet, you do not need to think about the Service definition at all, because the **Default Service** will work. In other cases, you will have to add one or more service definitions.

- **Appliance**: The Service Name and the values looked up by the Service may be default values or values that you configure according to documentation for the product.

3.3.1. GTA: Default Service

Your console should include the following:

Service name: `<default>`

Application/Command: `cmd/c start %url%`

Let this definition stay as it is. It works like this:

`cmd/c start` indicates the Windows default application.

`%url%` is a placeholder for the up to six values needed so that the GateManager can target the Appliance: protocol, host, port, path, user, and password.

When Go to Appliance is executed, the GateManager will look for these values in the configuration of the Appliance. If the Appliance is an agent residing on another Appliance, values may be taken from both configurations.

The default service will support most commands using http, https, or telnet as protocol. Some commands require special service definitions.

Each GateManager-enabled product has online help or other documentation which gives additional information about special GTA Service Definitions that might be relevant.

3.3.2. GTA: Adding special service definitions

If you need special service definitions, Support will advise on how to configure them.

Below are instructions about how to add, export, or import service definitions.

To manually add a service

1. Click the add + button ⊞.
2. A dialog will open for configuring the Service.
3. Type in a **Service** name.

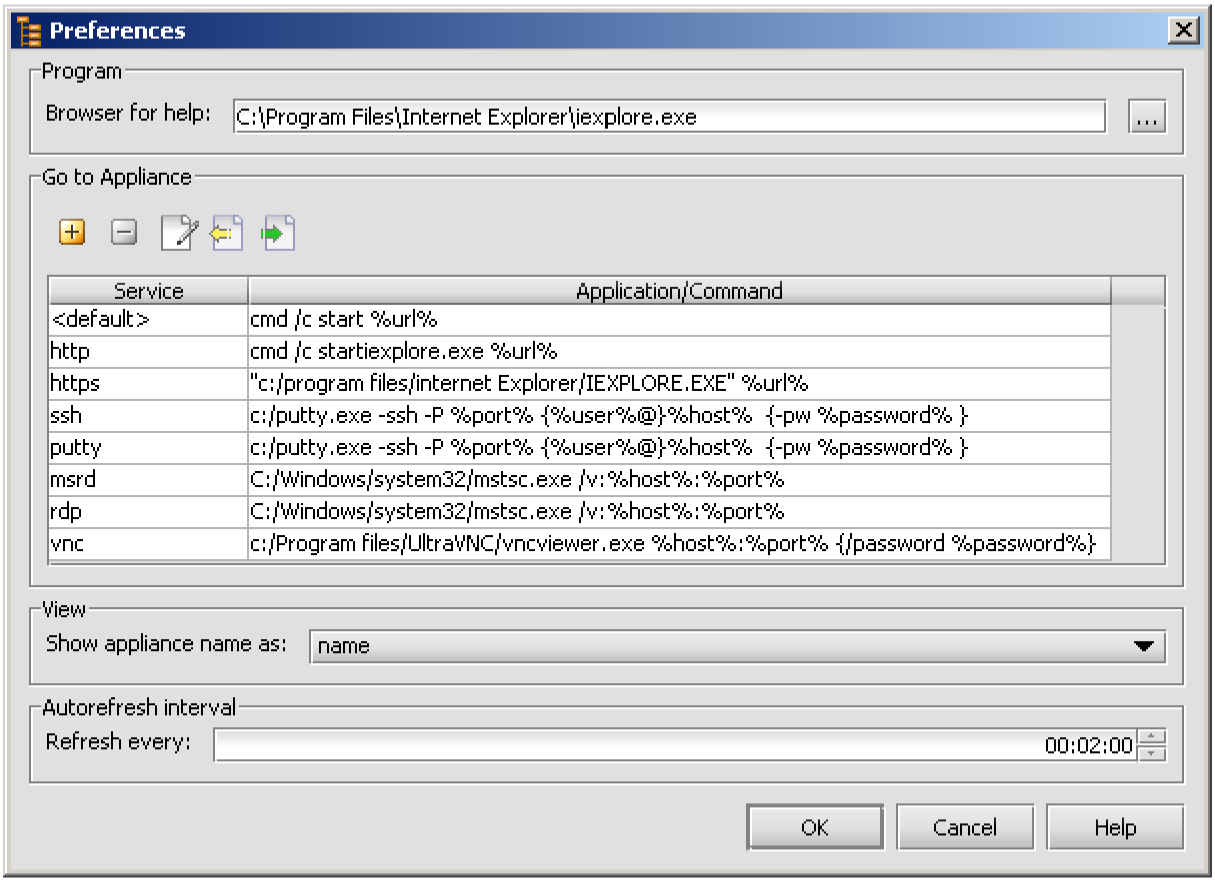
   IMPORTANT: Each Service name must be known to the appliance you want to Go to. On your list of Services, each Service must have a unique name.

4. **Application/Command** field: The right pane of the dialog has a list of parameters. A single click on a parameter displays a short description of it. A double click inserts it into the **Application/Command** field.

To export and import a file with service definitions

1. Open **Session > Preferences** on a Console with the definitions you want
2. In the **Go to Appliance** block, click the export service button ⇦.
3. Save to a file. The whole set of services will be included.
4. Open **Session > Preferences** on a Console you want the definitions imported to.
5. In the **Go to Appliance** block, click the import service button ⇨.

This example shows **Go to Appliance Service** definitions supplied in a file by Support or on the GateManager CD. (It also shows Internet Explorer specified for the help file because the user in this case uses a different default browser.)



Program

Browser for help: C:\Program Files\Internet Explorer\iexplore.exe

Go to Appliance

Service	Application/Command
<default>	cmd /c start %url%
http	cmd /c startiexplore.exe %url%
https	"c:/program files/internet Explorer/IEXPLORE.EXE" %url%
ssh	c:/putty.exe -ssh -P %port% {%user%@}%host% {-pw %password% }
putty	c:/putty.exe -ssh -P %port% {%user%@}%host% {-pw %password% }
msrd	C:/Windows/system32/mstsc.exe /v:%host%:%port%
rdp	C:/Windows/system32/mstsc.exe /v:%host%:%port%
vnc	c:/Program files/UltraVNC/vncviewer.exe %host%:%port% {/password %password%}

View

Show appliance name as: name

Autorefresh interval

Refresh every: 00:02:00

3.4. Preferences for viewing

Select **name** (default) or **serial number** from the drop-down list box. This choice will be used in the **Appliances View** Tree. **name** is the **GateManager Appliance Name**, which in many products is highly configurable.

3.5. Preferences for Autorefresh interval

The default interval for **Autorefresh** is 2 minutes, written **00:02:00** (the syntax is hh:mm:ss). You can change the interval here.

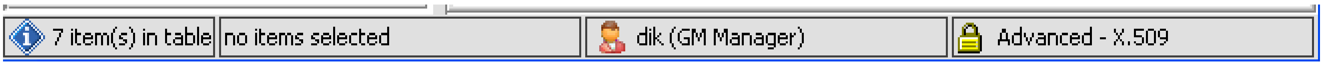
4. Managing your own Account with "My Account"

Your own account is never shown in the **Accounts View** tree pane. The **My Account** dialog is provided instead.

- **Note**: For information on working with other users' accounts, or on accounts in general, see Account Management (page 29).

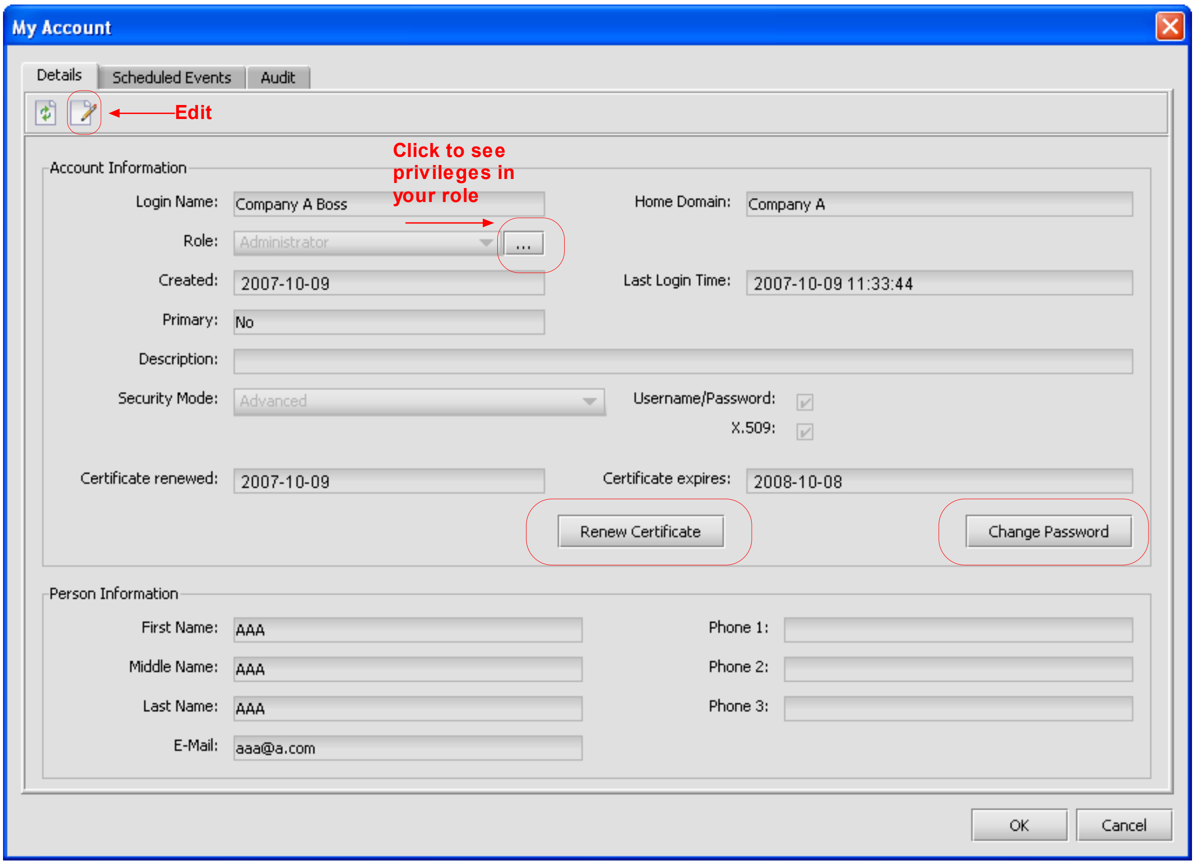
4.1. Opening "My Account" for viewing or editing

1. In any View, do one of the following:
   - Select **Session > My Account** on the main menu.
   - Double-click your Login name on the Status Bar at the bottom of the Console screen.



7 item(s) in table | no items selected | dik (GM Manager) | Advanced - X.509

2. The **My Account** dialog is displayed. It has three tabs of information:



Edit

Click to see privileges in your role

Account Information

Login Name: Company A Boss

Home Domain: Company A

Role: Administrator

Created: 2007-10-09

Last Login Time: 2007-10-09 11:33:44

Primary: No

Description:

Security Mode: Advanced

Username/Password: ☑

X.509: ☑

Certificate renewed: 2007-10-09

Certificate expires: 2008-10-08

Renew Certificate

Change Password

Person Information

First Name: AAA

Phone 1:

Middle Name: AAA

Phone 2:

Last Name: AAA

Phone 3:

E-Mail: aaa@a.com

- **Details**

  This is where you can edit selected information, change your password and renew your certificate. In addition, you can view your own account privileges. If you are the holder of a private domain, this is also where you can make the domain visible to higher domains in the branch by revoking primary account status (page 18).

- **Scheduled Events**

  This is where you can see the Events you have scheduled. Depending on the privileges in your role, it may be possible to cancel scheduled events from this screen.

- **Audit**

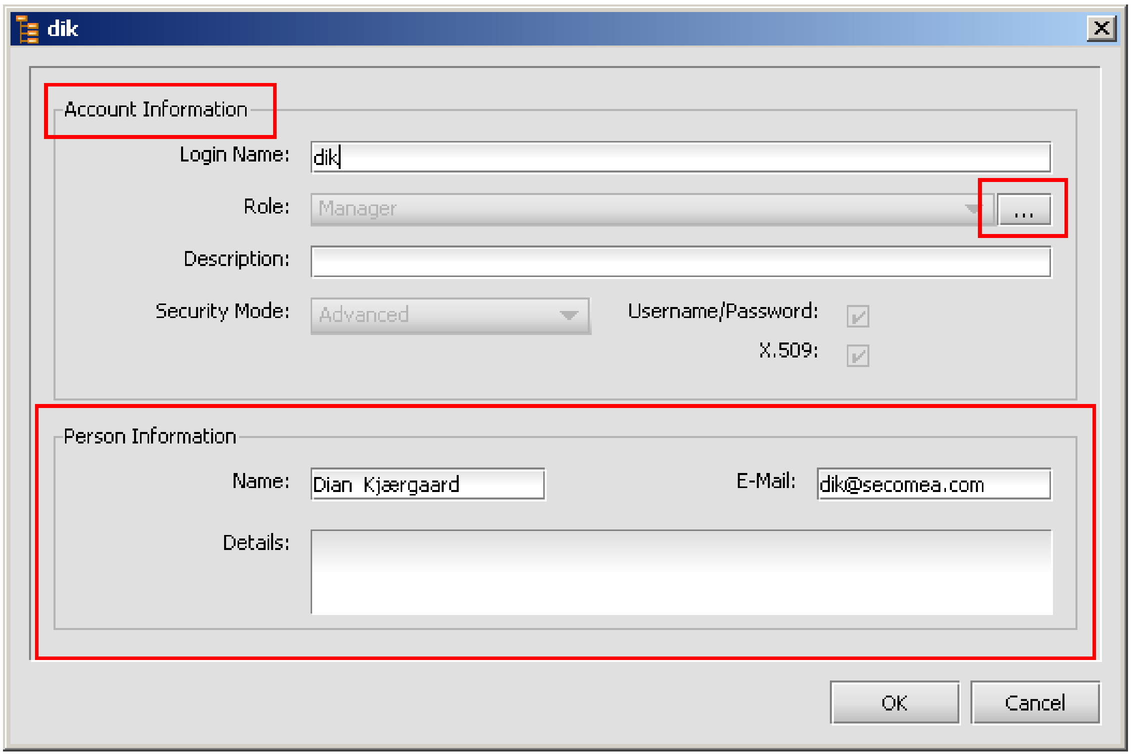
  This is where you can see the Audit log for your Account.

3. When you are finished, do one of the following:
   - Save changes and close the dialog by clicking **OK**.
   - To exit and close the window after simply viewing information, click **OK**, **Cancel**, or the close-window button ☒.
   - To exit and close the window without saving any changes click either **Cancel** or the close-window button ☒.

4.2. Editing your own account

Any user can edit his or her own account if the role assigned includes the necessary privileges.

Open the **Details** tab of the **My Account** dialog as shown in Opening "My Account" (see "Opening "My Account" for viewing or editing" page 15).



dik

Account Information

Login Name: dik

Role: Manager

Description:

Security Mode: Advanced

Username/Password: ☑

X.509: ☑

Person Information

Name: Dian Kjærgaard

E-Mail: dik@secomea.com

Details:

Click the Edit button ✎.

You may freely edit fields in the **Person Information** (see "Person Information (Accounts)" page 31) block. Make sure that your E-mail address is valid.

- **IMPORTANT**: Do not change the **Login Name** or **Description** in the **Account Information** block without permission from your administrator.

When you are finished, do one of the following

- Save changes and close the dialog by clicking **OK**.
- To exit and close the window without saving any changes click either **Cancel** or the close-window button ☒.

4.3. Changing your own password

1. Open the **Details** tab of the **My Account** dialog as shown in Opening "My Account" (see "Opening "My Account" for viewing or editing" page 15).
2. Click **Change Password** (in the **Account Information** block).
3. You will be asked whether or not you really want to do this. Note that if you do, the system will automatically generate a new certificate synchronized with your new password (see "Renewing your own certificate" page 17).
4. In the dialog box, enter the current password and the new password; repeat the new password.
5. The password must be at least 8 characters long, one of which must be numeric. Passwords are case-sensitive.
6. Save changes and close the dialog by clicking **OK**.
7. It may take some time for the dialog to close. Please be patient.
8. The system will automatically send you the new certificate along with the usual instructions in an e-mail.

- **Note**: If you are blocked from changing your own password, contact your administrator who will either explain why - or adjust the role for your account so that the necessary privileges are included.

4.4. Renewing your own certificate

When and why are certificates renewed?

Certificates must be renewed before they expire. Before GateManager 3.7, certificates only lasted for a year, but since GateManager 3.7, certificates now last for upto 30 years. Still, one month before your certificate expires, you will receive an e-mail; 5 days before the expiration date, you will receive a reminder via the Console when you log on.

Certificates must be coordinated with passwords. Therefore, if a password is changed. the system will automatically generate a new certificate which is synchronized with the new password and send it to the account's email address.

Note that a renewed certificate is, in fact, a new certificate. When it is created, any previous certificate for an account will become invalid.

How to renew your own certificate

1. Open the **Details** tab of the **My Account** dialog as shown in Opening "My Account" (see "Opening "My Account" for viewing or editing" page 15).
2. Click **Change Password** (in the **Account Information** block).
3. You will be asked whether or not you really want to do this. Note that if you do, the system will automatically generate a new certificate synchronized with your new password.
4. In the dialog box, enter the current password and the new password; repeat the new password.

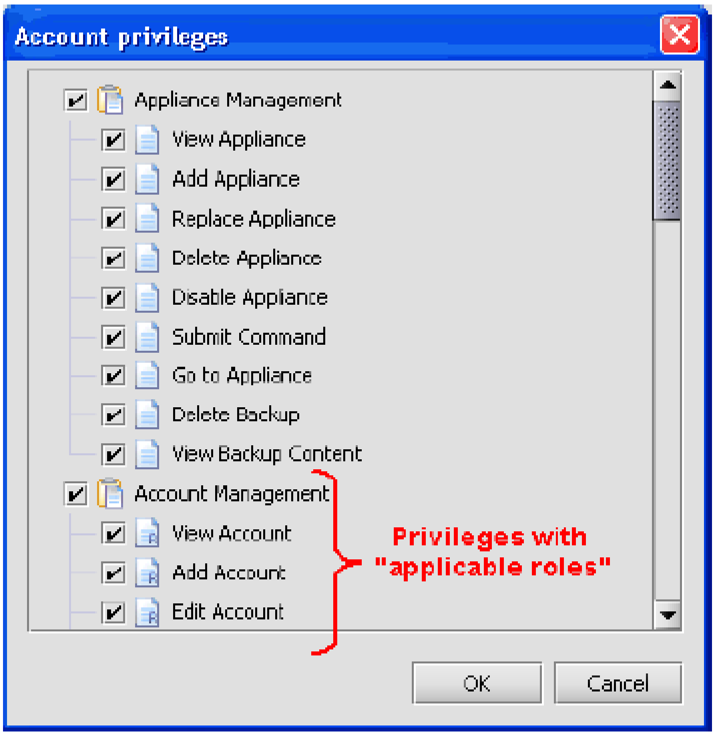
   The password must be at least 8 characters long, one of which must be numeric. Passwords are case-sensitive.

5. Save changes and close the dialog by clicking **OK**.
6. It may take some time for the dialog to close. Please be patient.
7. The system will automatically send you the new certificate along with the usual instructions in an e-mail.

- **Note**: If you are blocked from renewing your own password, contact your administrator who will either explain why - or adjust the role for your account so that the necessary privileges are included.

4.5. Viewing your account privileges

1. Open the **Details** tab of the **My Account** dialogue as shown in Opening "My Account" (see "Opening "My Account" for viewing or editing" page 15).
2. Do one of the following:
   - Click the ellipsis button … at the end of the **Role** field on the **Details** tab (in the **Account Information** block).
   - If you already have the **Edit My Account** dialog open, click the ellipsis button … at the end of the **Role** field (in the **Account Information** block).
3. The **Account privileges** screen is displayed.



- ☑ Appliance Management
  - ☑ View Appliance
  - ☑ Add Appliance
  - ☑ Replace Appliance
  - ☑ Delete Appliance
  - ☑ Disable Appliance
  - ☑ Submit Command
  - ☑ Go to Appliance
  - ☑ Delete Backup
  - ☑ View Backup Content
- ☑ Account Management
  - ☑ View Account
  - ☑ Add Account
  - ☑ Edit Account

Privileges with "applicable roles"

Note: Information about Principles for applicable roles is on page 38.

4. Scroll to see all of the privileges included in the role assigned to you.
5. To exit and close the window after simply viewing information, click **OK**, **Cancel**, or the close-window button ☒.

4.6. Revoking Primary Account status

If you own a private domain, your account will have been marked as Primary by a superior administrator (see "Making an account primary and a domain private" page 32).

Only you can change this.

1. Open the **Details** tab of the **My Account** dialogue as shown in Opening "My Account" (see "Opening "My Account" for viewing or editing" page 15).
2. On the **Details** tab, click **Revoke Primary** (in the **Account Information** block).
3. The setting in the **Primary** field will change to **No**.

5. Domains

Domains are the all-important administrative groupings in GateManager, not only of accounts and of Appliances, but also of alert rules and configuration profiles, which are created in domains before they can be associated with Appliances.

Furthermore, firmware managed in the Appliance Product View can only be used in a domain which includes the appliance product in its Product Bindings.

Domains are grouped into hierarchies. The domain in which an object is created is known as the object's **home domain**.

5.1. About domain hierarchies and access

The GateManager Owner creates the server's ROOT Domain and a domain structure.

Each user account is placed in a domain, known as its home domain.

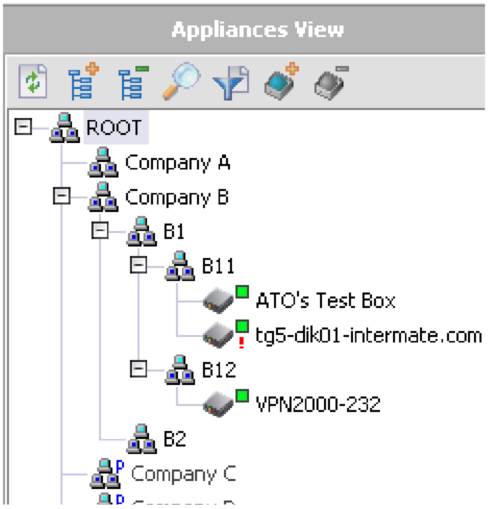
Domains are grouped into hierarchies. As a general rule, the domain hierarchy works such that domain characteristics are inherited downwards by a domain's child domains (sub-domains). This has the following consequences:

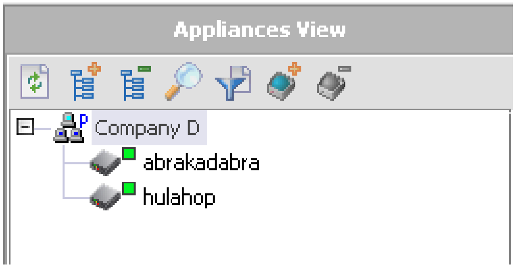
- The user of an account can see all of the domains downwards in the hierarchy with the exception of so-called private domains as explained here and in Private Domains - how they work (see "Private Domains - a summary of how they work" page 20).
- In the GateManager Console, the user of an account can never see domains at a higher hierarchical level than the account's own home domain.
- In the GateManager Console, the user of an account can never see domains at a parallel hierarchical level. For example, the user of the Account "B11 Boss" cannot see any information at all about the Domain "B12" .
- By default, the domain access restrictions from a LinkManager Console are the same as from the GateManager Console, but a LinkManager user *can* be granted access to specific domains outside the home domain and downwards. See "Cross-domain appliance access for LinkManager users" page 25.

Example: Owner at ROOT level and Company D Boss look at the Appliances View

Left screenshot: The Appliances View is completely expanded, so that the Owner sees every Appliance in every domain in the hierarchy - except those in private domains (Company C and Company D).

Right screenshot: There are, in fact, attached Appliances in Company D. They just cannot be seen by any superior user.

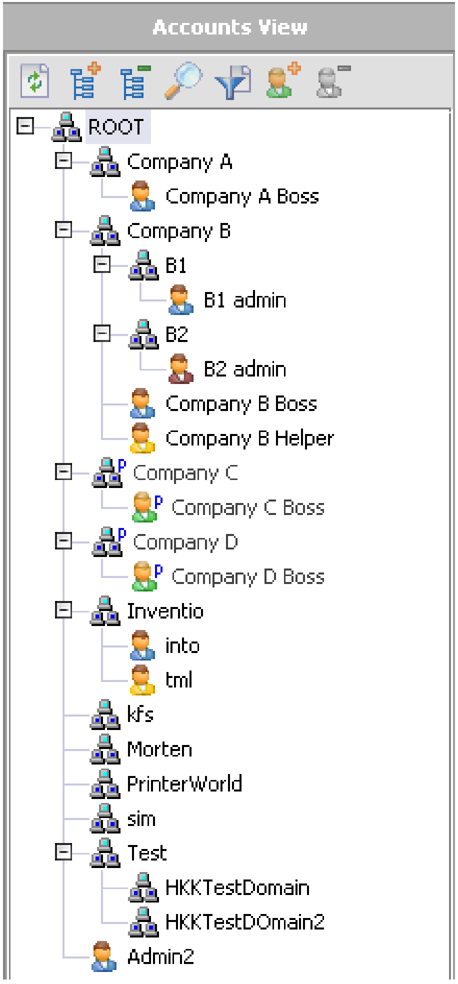




Example: Owner at ROOT level and Company D Boss look at the Accounts View

The Account View is completely expanded, and the Owner can see all accounts. The Owner is not allowed to edit an account in a private domain (Company C or Company D) – but is allowed to change password and renew certificates

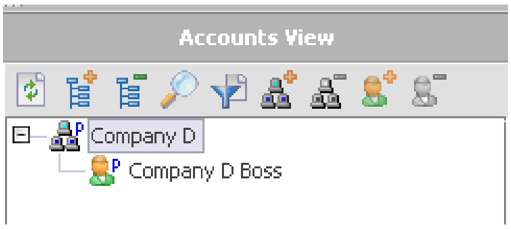
When ROOT Owner is logged in, he sees all of this:



Accounts View

- ROOT
  - Company A
    - Company A Boss
  - Company B
    - B1
      - B1 admin
    - B2
      - B2 admin
    - Company B Boss
    - Company B Helper
  - Company C
    - Company C Boss
  - Company D
    - Company D Boss
  - Inventio
    - into
    - tml
  - kfs
  - Morten
  - PrinterWorld
  - sim
  - Test
    - HKKTestDomain
    - HKKTestDOmain2
  - Admin2

When Company D boss is logged in, he will only see his own domain:



Accounts View

- Company D
  - Company D Boss

He will not see his own account (no-one ever sees their own account in the Accounts View – instead, they use “My Account“).

If there are other accounts in Company D, Company D boss will be allowed to see the other accounts (and, with the appropriate privileges edit them).

5.1.1. Private Domains - a summary of how they work

Private domains are only used if you want or need to give completely decentralized control over a domain, for example a domain used for a given customer’s Appliances.

Users at a higher level in the hierarchy can see that a private domain exists, but they cannot see any of the following contents of a private domain:

- Appliances
- Alert Rules
- Configuration Profiles (Profiles)
- Domains (sub-domains – child domains).

If Domain Preference values are propagated downwards, they will also affect Private Domains and their sub-domains.

Users at a higher level can not edit an account in a private domain. They can, however, see that it exists. And they may be able to do some rescue work: renewing a certificate, changing a password, or enabling an account that has been disabled because of too many unsuccessful log-in attempts, but this does not always work reliably. Therefore, it is important that a domain be properly prepared before making it private; see

5.2. Create and configure domains

5.2.1. About domain names

Before creating domains, you might want to have a naming plan ready. In any event, you need to be aware of naming characteristics and restrictions that are mainly due to the following:

- The system uses a domain token which ensures that an Appliance is placed correctly in the domain hierarchy any time it initiates a new connection to the server.
- Domain tokens are constructed of domain names connected with dots (periods, full stops).

Character restrictions on a domain's name

- Except for the dot (period, full stop), you can use any characters in the UTF8 character set. Dots are reserved for use in the domain token.
- Blank spaces can be used within a string, but not as the first or last character. You must not use more than one consecutive blank/space within a string.
- The characters you use should be supported by the Appliance and by the keyboards used by staff who configure the Appliance. Otherwise you can risk problems when domain tokens are entered in the Appliance configuration.
- Some appliances have set a limit on the maximum number of characters which can be used for the domain token. This can in turn suggest a limit for the number of characters you use in a domain's name. The dots separating the elements in the domain token are counted as characters. You do not need to enter the name of the top domain when you enter the domain token in an Appliance configuration.

Note that domain names are not case-sensitive.

5.2.2. How to create a domain

For each domain you need to create, do the following:

1. In the **Domains View**, right-click the parent domain, which in some cases will be ROOT.
2. Select **Create Domain**.
3. This opens the **New Domain** dialog.
4. Enter a Name. Be sure you are familiar with naming restrictions (see Domain names).
5. Enter (optionally) a **Description**.
6. Change **Domain Preferences** if desired (see "About domain preferences" page 22). You will probably not need to change these prferences, but check them.
7. Save changes and close the dialog by clicking **OK**.
8. Open the **Domains View** tree with the + button on a node or with the tree expand button .
9. Click on the new domain to select it.
10. Select the **Product Bindings** tab. The list of product bindings will show every product in the parent domain at the time the new domain is created.
11. Click each product that you do *not* want to be allowed in the domain. Each click will set a check-mark.
12. Click the delete button on the tab tool bar.
13. You will be asked to confirm that you want to unbind the selected product(s). Click **Yes**.

- **IMPORTANT**

  If you need a product that is not on the list, go up the hierarchy step by step until you find what you need, and then add it to all the levels back down to the new domain.

  If the product is not in the ROOT domain, the server Owner must add a plugin manually (see "Manual .jar file installation" page 74). Then the product must be bound manually to each domain down the relevant parts of the hierarchy.

5.2.3. About domain preferences

In most cases, you do not need to have different domain preferences for various domains in the hierarchy, and you can propagate preferences downwards very simply, like this:

If the domain has one or more child domains, the Details tab will show a Propagate button for each parameter. When a Domain Preference is propagated, it is set for all Child Domains - all the way down the particular Domain Hierarchy (but not sideways, of course). Private Domains are also affected. (see "Private Domains - a summary of how they work" page 20)

As you work with your installation, you may want to do familiarize yourself with the details of domain preferences to see if you want to adjust any of them.

Parameter	**Comments**
Heartbeat Interval	This is the length of time that the GateManager waits between its regular requests for a heartbeat packet from the Appliances in the domain. The Heartbeat Interval can be equal to or shorter than the Heartbeat Interval for the domain’s parent.
Keep-Alive Interval	This setting determines how often the GateManager Proxy sends a TCP packet to the appliance to keep the connection alive. If there is no reply the connection state becomes Failed. The Keep-Alive Interval for a domain should always be at least 1 second shorter than the Heartbeat Interval for that Domain. The Keep-Alive Interval can be equal to or shorter than the Keep-Alive Interval for the domain’s parent.
Heartbeat Latency Interval	This is a short period of time – usually just seconds – which is added to the Heartbeat Interval to define a timeout interval. If the system doesn’t receive a Heartbeat within this timeout, the Heartbeat status changes from OK (or Requesting) to Expired. The Heartbeat Latency Interval can be equal to or shorter than the Heartbeat Latency Interval for the Domain’s Parent.
Maximum Number of Backups	This parameter tells the GateManager how many backup configurations to retain on the system. Retained backups are displayed on the Configuration Backups tab for the individual appliance (use the Appliances View and select the Details tab). This number may be equal to or less than the number specified for the domain’s parent. When the limit is reached, the oldest backup is automatically deleted. Backups may also be manually deleted.
Maximum Number of Enrollment Reports (formerly called Audit Reports)	Enrollment reports can be generated to tally up the number of Appliances enrolled in a domain. This parameter tells the GateManager how many Enrollment Reports to retain on the system. Retained Enrollment Reports are shown on the Enrollment Reports tab for the individual domain (use the Domains View). When the limit is reached, the oldest retained report is automatically deleted. Enrollment Reports may *not* be manually deleted.
Maximum Number of Alert Log Entries Per Alert	This parameter tells the GateManager how many Alert Log Entries to retain on the system. Retained Alert Log Entries are shown on the Alert Log tab for the individual appliance (use the Appliances View). When the limit is reached, the oldest retained report is automatically deleted. Alert Log Entries may *not* be manually deleted.
Unknown State Timeout	The Unknown State (yellow) is limited to the time specified here. If the appliance is not connected within this timeout, the Appliance’s Connection State is changed to Failed (red). The Unknown State timeout may be equal to or shorter than the one specified for the Domain’s Parent.

5.2.4. How to edit a domain

In this example, you own the domain Company B and want to edit its child domain B2.

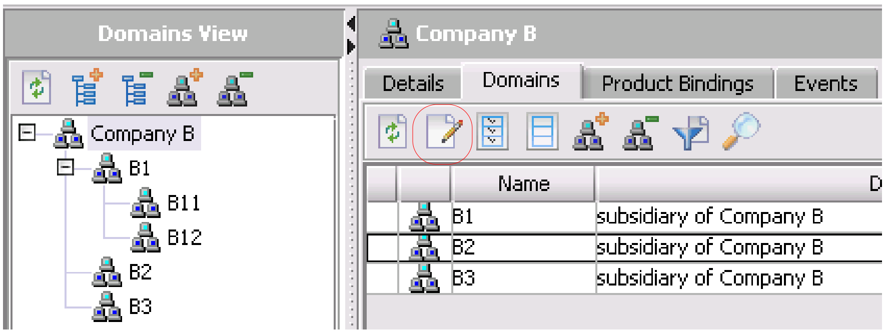
The editing dialog itself is exactly like the New Domain dialog (see "How to create a domain" page 21).

There are several different ways to select the domain you want to edit.

Start on the target domain in one of two ways

- Directly from the tree: Right-click the domain name in the **Domains View** tree to activate the context menu. Click **Edit Domain**.
- Invoking the Main Menu (not shown here): Highlight (left-click) the domain name in the **Domains View** tree - or select it by clicking the selection field for the row. On the Main Menu click **Domains**, and then click **Edit Domain**.

Start at a level higher



Name	D
B1	subsidiary of Company B
B2	subsidiary of Company B
B3	subsidiary of Company B

1. In the **Domains View** tree, find and highlight (left-click) the domain one level higher than your target.
2. Use the table on the **Domains** tab to access for example B2.
3. Access the **Edit** dialog in one of four ways
   - Highlight (left-click) the row or select it by clicking the selection field. Then click the **Edit** button (circled) on the Domains tab.
   - Double-click the table entry for domain B2.
   - Right-click the table entry for domain B2, and then select **Edit** from the context menu.
   - Invoking the Main Menu (not shown here): Highlight (left-click) the row or select it by clicking the selection field. On the Main Menu click **Domains**, and then click **Edit Domain**.

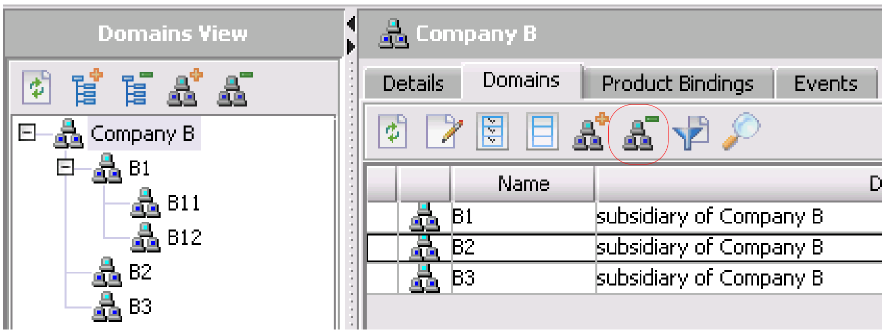
5.2.5. How to delete a domain

In this example, you own the domain Company B and want to delete its child domain B2. There are several different ways to select the domain you want to delete.

Start on the target domain in one of two ways

- Directly from the tree: Right-click the domain name in the **Domains View** tree to activate the context menu. Click Delete **Domain**.
- Invoking the Main Menu (not shown here): Highlight (left-click) the domain name in the **Domains View** tree - or select it by clicking the selection field for the row. On the Main Menu click **Domains**, and then click **Delete Domain**.

Start at a level higher



Name	D
B1	subsidiary of Company B
B2	subsidiary of Company B
B3	subsidiary of Company B

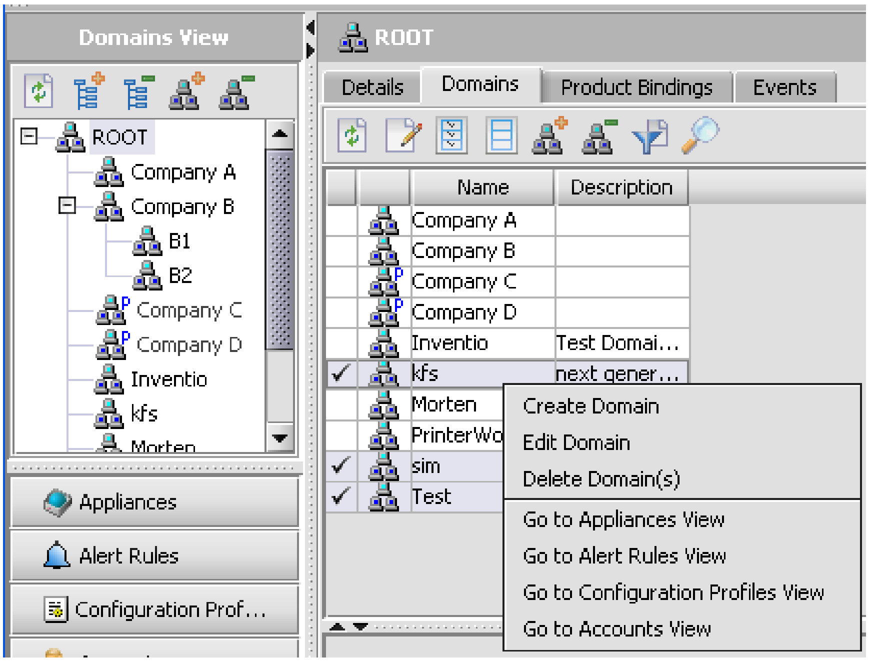
1. In the **Domains View** tree, find and highlight (left-click) the domain one level higher than your target.
2. Use the table on the **Domains** tab to access for example B2.
3. Access the **Delete** function in one of three ways
   - Highlight (left-click) the row or select it by clicking the selection field. Then click the **Delete** button (circled) on the Domains tab.
   - Right-click the row and select **Delete Domain**.
   - Invoking the Main Menu (not shown here): Highlight (left-click) the row or select it by clicking the selection field. On the Main Menu click **Domains**, and then click **Edit Domain**.

- **IMPORTANT**:

  The system will not allow you to delete a domain to which other objects – such as Appliances, accounts, alert rules or configuration profiles – are associated.

5.2.6. How to select and delete several domains at a time

Start: In the **Domains View** tree, find the domain one level higher than where you want to delete. For example, highlight ROOT if you want to delete "kfs", "sim" and "Test".



	Name	Description
	Company A	
	Company B	
	Company C	
	Company D	
	Inventio	Test Domai…
✓	kfs	next gener…
	Morten	
	PrinterWo	
✓	sim	
✓	Test	

Tip: You cannot recourse the Domains table. So, for example, an administrator whose Account has "ROOT" as Home Domain can delete the domain B2, but in order to do so, the domain Company B must be selected in the tree.

A. Highlight the domain.

B. Activate the **Domains** tab.

C. On the table, click each of the domains you want to work with. This example shows three selections.

D. Do one of the following to bring up a menu:

- Activate a context menu with a right click from anywhere in the selected domains; the result of this is shown in the screen shot.
- Use the Main Menu's Domains menu (not shown on the screen shot).

E. Click **Delete Domain(s)**.

- **IMPORTANT**:

The system will not allow you to delete a domain to which other objects – such as Appliances, accounts, alert rules or configuration profiles – are associated.

5.3. Cross-domain appliance access for LinkManager users

The hierarchical domain structure enforces strict access control for an account, allowing users of the account to access only the home domain and any sub-domains of that domain.

For administrative purposes, this is a sound access method, allowing an administrator to manage only the domains and appliances within the scope of the administrator's account.

However, for remote device management from a LinkManager, the strict domain structure typically gives access to either too few devices or too many devices. Consider a company with two production sites, each consisting of a number of production lines, each consisting of 10 devices from 4 different vendors.

Now, a logical domain structure for this setup could be:

- Production Site 1
  - Production Line 1
    - Vendor 1 Devices
    - Vendor 2 Devices
    - …
  - Production Line 2
    - Vendor 1 Devices
    - ...
- Production Site 2
  - …

In the strict domain access model, the LinkManager users from Vendor 1 would have to have different user accounts for each of the "Vendor 1 Devices" sub-domains, and use the proper account for accessing each of these domains.

Through the "Join Domains to Accounts" feature (new in GateManager 4.0), an administrator who has access to the entire domain structure above can grant a single LinkManager user account access to all of the "Vendor 1 Devices" domains. Typically, additional domains are created just to manage LinkManager users like this:

- LinkManagers
  - Internal
  - Vendor 1
  - Vendor 2

With these extra domains, all LinkManager appliances – and the related user accounts – can be held separate from the hierarchical domain structure.

The actual method to join domains to accounts is done via the "Account View" (see "Join Domains to Accounts" page 34).

5.4. Domain enrollment reports

5.4.1. About enrollment reports

An Enrollment Report shows all Appliances in the selected domain.

Two reports are created, a **Summary Report** and a **Detailed Report**. Each report is recursive. This means that the tally will include that domain and all of its child domains.

For any domain in which you have access rights you may schedule a report or generate one on demand.

All reports are automatically added to the **Reports history** table for the domain. The maximum number of Reports retained per Domain is controlled by the **Domain Preferences** (see "About domain preferences" page 22). Reports cannot be manually deleted.

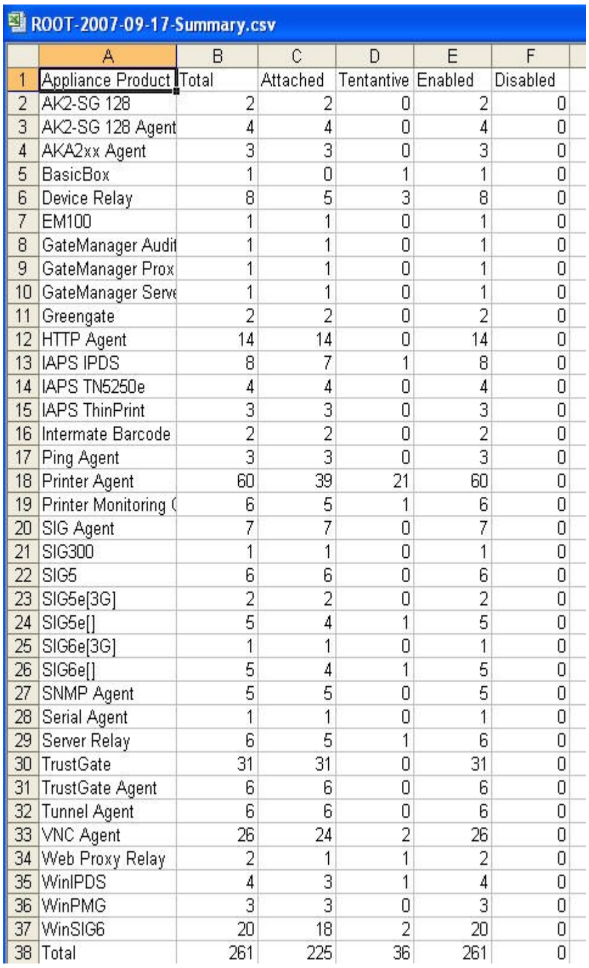
Any retained report can be viewed from the Console.

Any retained report can be sent at any time to one or more recipients.

5.4.2. Sample Domain Enrollment Reports

Contracts for billing may vary, so it is possible that not all of the information in an Enrollment Report will be relevant in a particular commercial situation.

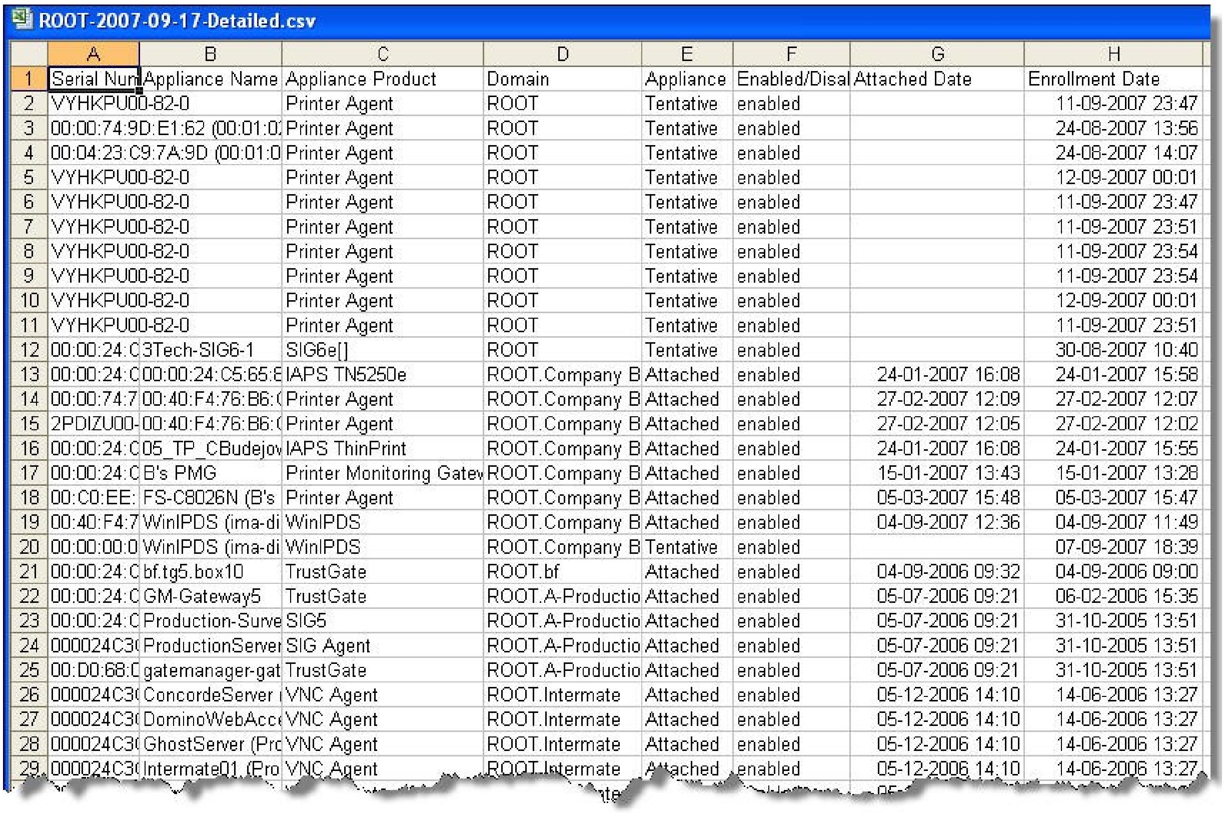
Summary report



ROOT-2007-09-17-Summary.csv

	A	B	C	D	E	F
1	Appliance Product	Total	Attached	Tentantive	Enabled	Disabled
2	AK2-SG 128	2	2	0	2	0
3	AK2-SG 128 Agent	4	4	0	4	0
4	AKA2xx Agent	3	3	0	3	0
5	BasicBox	1	0	1	1	0
6	Device Relay	8	5	3	8	0
7	EM100	1	1	0	1	0
8	GateManager Audit	1	1	0	1	0
9	GateManager Prox	1	1	0	1	0
10	GateManager Serve	1	1	0	1	0
11	Greengate	2	2	0	2	0
12	HTTP Agent	14	14	0	14	0
13	IAPS IPDS	8	7	1	8	0
14	IAPS TN5250e	4	4	0	4	0
15	IAPS ThinPrint	3	3	0	3	0
16	Intermate Barcode	2	2	0	2	0
17	Ping Agent	3	3	0	3	0
18	Printer Agent	60	39	21	60	0
19	Printer Monitoring (	6	5	1	6	0
20	SIG Agent	7	7	0	7	0
21	SIG300	1	1	0	1	0
22	SIG5	6	6	0	6	0
23	SIG5e[3G]	2	2	0	2	0
24	SIG5e[]	5	4	1	5	0
25	SIG6e[3G]	1	1	0	1	0
26	SIG6e[]	5	4	1	5	0
27	SNMP Agent	5	5	0	5	0
28	Serial Agent	1	1	0	1	0
29	Server Relay	6	5	1	6	0
30	TrustGate	31	31	0	31	0
31	TrustGate Agent	6	6	0	6	0
32	Tunnel Agent	6	6	0	6	0
33	VNC Agent	26	24	2	26	0
34	Web Proxy Relay	2	1	1	2	0
35	WinIPDS	4	3	1	4	0
36	WinPMG	3	3	0	3	0
37	WinSIG6	20	18	2	20	0
38	Total	261	225	36	261	0

Bit of a detailed report



ROOT-2007-09-17-Detailed.csv

	A	B	C	D	E	F	G	H
1	Serial Nun	Appliance Name	Appliance Product	Domain	Appliance	Enabled/Disal	Attached Date	Enrollment Date
2	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:47
3	00:00:74:9D:E1:62 (00:01:0		Printer Agent	ROOT	Tentative	enabled		24-08-2007 13:56
4	00:04:23:C9:7A:9D (00:01:0		Printer Agent	ROOT	Tentative	enabled		24-08-2007 14:07
5	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		12-09-2007 00:01
6	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:47
7	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:51
8	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:54
9	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:54
10	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		12-09-2007 00:01
11	VYHKPU00-82-0		Printer Agent	ROOT	Tentative	enabled		11-09-2007 23:51
12	00:00:24:C	3Tech-SIG6-1	SIG6e[]	ROOT	Tentative	enabled		30-08-2007 10:40
13	00:00:24:C	00:00:24:C5:65:E	IAPS TN5250e	ROOT.Company B	Attached	enabled	24-01-2007 16:08	24-01-2007 15:58
14	00:00:74:7	00:40:F4:76:B6:(	Printer Agent	ROOT.Company B	Attached	enabled	27-02-2007 12:09	27-02-2007 12:07
15	2PDIZU00-	00:40:F4:76:B6:(	Printer Agent	ROOT.Company B	Attached	enabled	27-02-2007 12:05	27-02-2007 12:02
16	00:00:24:C	05_TP_CBudejov	IAPS ThinPrint	ROOT.Company B	Attached	enabled	24-01-2007 16:08	24-01-2007 15:55
17	00:00:24:C	B's PMG	Printer Monitoring Gatev	ROOT.Company B	Attached	enabled	15-01-2007 13:43	15-01-2007 13:28
18	00:C0:EE:	FS-C8026N (B's	Printer Agent	ROOT.Company B	Attached	enabled	05-03-2007 15:48	05-03-2007 15:47
19	00:40:F4:7	WinIPDS (ima-di	WinIPDS	ROOT.Company B	Attached	enabled	04-09-2007 12:36	04-09-2007 11:49
20	00:00:00:0	WinIPDS (ima-di	WinIPDS	ROOT.Company B	Tentative	enabled		07-09-2007 18:39
21	00:00:24:C	bf.tg5.box10	TrustGate	ROOT.bf	Attached	enabled	04-09-2006 09:32	04-09-2006 09:00
22	00:00:24:C	GM-Gateway5	TrustGate	ROOT.A-Productio	Attached	enabled	05-07-2006 09:21	06-02-2006 15:35
23	00:00:24:C	Production-Surve	SIG5	ROOT.A-Productio	Attached	enabled	05-07-2006 09:21	31-10-2005 13:51
24	000024C3(	ProductionServer	SIG Agent	ROOT.A-Productio	Attached	enabled	05-07-2006 09:21	31-10-2005 13:51
25	00:D0:68:C	gatemanager-gat	TrustGate	ROOT.A-Productio	Attached	enabled	05-07-2006 09:21	31-10-2005 13:51
26	000024C3(	ConcordeServer (	VNC Agent	ROOT.Intermate	Attached	enabled	05-12-2006 14:10	14-06-2006 13:27
27	000024C3(	DominoWebAcce	VNC Agent	ROOT.Intermate	Attached	enabled	05-12-2006 14:10	14-06-2006 13:27
28	000024C3(	GhostServer (Prc	VNC Agent	ROOT.Intermate	Attached	enabled	05-12-2006 14:10	14-06-2006 13:27
29	000024C3(	Intermate01 (Pro	VNC Agent	ROOT.Intermate	Attached	enabled	05-12-2006 14:10	14-06-2006 13:27

A report that is sent on an e-mail includes the name of the Domain and the date of the report. Each of the reports (Summary and Detailed) is enclosed as a comma separated file (.csv), which will show as a spreadsheet file if you launch it in Windows.

5.4.3. Schedule Enrollment Reports

1. In the **Domains View**, highlight the Domain you want a report on.
2. Activate the **Enrollment Report** tab and click the Edit 📝 button.
3. If **Disabled** is selected, deselect it.
4. Select an interval for reporting (every year, every month, every week, every day). The report will be generated at 23:59 at the end of the stipulated period.
5. You can enter as many **Recipient e-mail** addresses as you like. If there are two or recipients, separate them with commas. To select e-mail addresses known to the GateManager, click the To….button [To...] and select the individual Account(s), then click **OK**.
6. Click **OK**.

- **IMPORTANT**:

  If the domain in question is ROOT, it may show a monthly report schedule your supplier as recipient. Do not remove or change this! You may, however, add other addresses to the scheduled report - and you can always generate a report on demand.

5.4.4. Generate Enrollment Report on demand

1. In the **Domains View**, highlight the Domain for which you want an Enrollment Report generated.
2. Activate the **Enrollment Report** tab.
3. Click on the Add button to generate a report. It will be automatically added to the **Reports History** table.
4. From the table you can view a report or request that the report be sent to one or more recipients.

5.4.5. View an Enrollment Report from the Console

1. In the **Domains View**, highlight the Domain for which you want an Enrollment Report generated
2. Activate the **Enrollment Report** tab.
3. Right-click on the desired report on the **Reports history** table and select either **Detailed** or **Summary**.

5.4.6. Send/re-send Enrollment Report on Demand

1. In the **Domains View**, highlight the desired Domain.
2. Activate the **Enrollment Report** tab.
3. Right-click on the desired report on the **Reports history** table and select **Send To**.

   You can enter as many recipient e-mail addresses as you like. If there are two or recipients, separate them with commas. To select e-mail addresses known to the GateManager, click the To…. To... and select the individual Account(s).

4. Click **OK**.

6. Account Management

Role: To manage others' accounts you must have account management privileges in the role assigned to your own account (see "Viewing your account privileges" page 18).

Hierarchy: Privileges to work with accounts apply to your own home domain and lower domains (excepting any Private domain).

- **Note**: If you need information on managing your own Account, see "My Account" (see "Managing your own Account with "My Account"" page 15)

6.1. Creating a new account

1. Select the **Accounts** View.
2. Highlight the domain where you want to place the account.

   IMPORTANT: Once you have chosen a Domain, it is not modifiable. If you want to change a domain, you must delete the account and start again.
3. Open the **New Account** dialog by doing one of the following:
   - On the Main Menu select **Accounts > New Account**. *Or*
   - On the Tree Pane tool bar click the New Account button. *Or*
   - RIght-click the domain name and select **Create New Account** from the context menu.

In the **Account Information** block (see "Account Information" page 30)

4. Enter a **Login Name**.

   IMPORTANT: Use a meaningful Login Name that can help to identify the account holder.

   Note that Login Names are case-sensitive.
5. Select a **Role** from the drop-down list.
6. Enter a **Description** (optional, but recommended).
7. For **Password** and **Security Mode** follow these instructions (see "Security mode, certificate and password" page 31).
8. Optional: **Select User must change password at next logon**.
9. Fill out the fields in the **Person Information** block (see "Person Information (Accounts)" page 31). It is very important that a valid e-mail address is included.
10. Save changes and close the dialog by clicking **OK**.

Follow up

The system will automatically e-mail an X.509 certificate to the e-mail address. The user is responsible for following the instructions in the e-mail and on the Console.

Be sure to tell the user the password you have created - and let him or her know if the first login will require a change of password.

Once the account has been created, most changes require opening the Edit Account dialog (see "Editing an account" page 32).

- Exceptions: From the Details tab itself it is possible to disable/enable an account, renew a certificate and change a password.

6.1.1. Account Information

Field or control	**Comments**
Login Name *(case sensitive!)*	This is the login name that will be used by this account to login to the GateManager. It should be meaningful and give some idea about who holds the account. It can include any kinds of letters, numbers, spaces and punctuation. Account maintenance: Use the Edit Account dialog if changes are required.
Home Domain	This is established automatically by where the account is placed on creation. After the account is saved, the field is read-only.
Role	Only those roles that you are allowed to assign will be included on the drop-down list. Account maintenance: Use the Edit Account dialog if changes are required.
Description	Free text. Follow company standards for user administration. Account maintenance: Use the Edit Account dialog if changes are required.
Security Mode	Please read the explanation here (see "Security mode, certificate and password" page 31). Account maintenance: Use the Edit Account dialog if changes are required.
Suspended (read-only)	Only the system can suspend an account. For more information see Login failures (page 33).
Primary + Set or Revoke button	When you work on another person's account, you can select **Set Primary** to make that person's home domain private. Do not do so without first reading this (see "Making an account primary and a domain private" page 32). If your own account shows **Yes** in the **Primary** field, there will also be a button for Revoking Primary Account Status (page 18).
Disable Yes/No + Disable or Enable button	An account can be disabled automatically by the system or manually by a superior user. Enabling can only be done by a superior user. See here (see "Disabling and enabling an account" page 33).
Created Last Login Time Certificate renewed Certificate expired	Read-only time stamps. Certificate time stamps are only shown if the Advanced Security Mode has been selected.
Renew Certificate Change Password	These operations are performed from the Details tab itself.
User must change password at next login	If you select this, be sure that the role you assign to the account includes the necessary privilege for "changing own password". And be sure to warn the user any time you select this. When the user logs on and changes the password, a new certificate will be generated, and the "User must change password..." box gets automatically cleared. Account maintenance: Use the Edit Account dialog if changes are required

6.1.2. Security mode, certificate and password

Account creation

Set a password and select a security mode on the **New Account** dialog.

Field	Comments
Password fields	A password must include at least 8 characters, one of which must be numeric. Passwords are case-sensitive.
Security Mode	**Basic Security Mode** means that the user can only authenticate log-in with a Username and Password. The **X.509** field is automatically not selected, and cannot be changed. The **Username/Password** box is automatically selected and cannot be changed. This mode should only be applied to an account which is assigned an Observer role. **Advanced Security Mode** means that an X.509 Certificate will be generated. The **X.509** field is automatically selected and cannot be changed. There are two ways to use the **Username/Password** field: If you clear the Username/Password box, the user will always have to authenticate log-in with the X.509 Certificate and Password. If you select the Username/Password box, the user can freely choose between the two authentication methods. However, if he or she logs in with Username/Password, Privileges will be reduced to *"See only"* for the duration of the session.

- **Tip:** The general rule should be to put all accounts in **Advanced Security Mode**. There is one exception, which is an account to which the **Observer** role will be assigned. Select **Basic Security Mode**, and no X.509 certificate will be generated. A user name and password is, of course, required - and you have complete control over this, as the user cannot change the account's password. Do *not* select **User must change password at next logon**.

Account maintenance

Once the account has been saved, you can use the **Details** tab itself (without opening the editing screen) to renew a certificate or change a password; changing a password will automatically renew the certificate.

6.1.3. Person Information (Accounts)

If your role includes the privilege "Edit Account", you can freely change the content of these fields for your own account as well as any other account whose role is "applicable" to your own role. Only the top-most (ROOT) administrator needs to think about organizing applicable roles. In your everyday work, you will easily see which accounts you are allowed to edit.

Field	Comment
Name	Complete Name required for X.509 certificate generation.
E-Mail	**It is extremely important that this is correct!**
Details	This is a free text field for any other relevant information like phone numbers, job title, which shift the account holder normally works, etc. These details are not used by any other part of GateManager.

6.2. Managing existing accounts

6.2.1. Editing an account

1. Select the **Accounts** View.
2. Select the account you want to edit and open the edit dialog by doing one of the following:
   - Highlight the relevant domain in the tree and activate the Accounts tab. Double-click the desired account on the table.
   - Highlight the relevant domain in the tree and activate the Accounts tab. Highlight the desired account on the table. Right-click and select Edit Account from the context menu.
   - Highlight the relevant domain in the tree and activate the Accounts tab. Highlight the desired account on the table. Click the Edit button on the Accounts tab.
   - Double-click the account directly in the tree.
   - Highlight the account directly in the tree; then click on the Edit button on the **Details** tab.
3. Edit as required.

   Login name, role, description, security mode, "allow login with username/password", and "user must change password on next login" can be edited from the Edit Account screen, Account Information block (see "Account Information" page 30).

   All fields in the Person Information block can also be edited (see "Person Information (Accounts)" page 31).
4. Save changes and close the dialog by clicking **OK**.

6.2.2. Making an account primary and a domain private

Any account can be set as a Primary account. The effect of this is that the account’s home domain becomes private (see "Private Domains - a summary of how they work" page 20).

1. Select the **Accounts View**.
2. Highlight the account in question.
3. Select the **Details** tab. The **Primary** field setting should be **No** and there should be a button labelled **Set Primary**.
4. In the **Account Information** block, click **Set Primary**.
5. You will be warned that you will no longer be able to carry out any operations in the domain and that only the account user him- or herself will be allowed to revoke the account's primary status (see "Revoking Primary Account status" page 18). If you are sure that you want to do this, Click **Ye**s.
6. The **Primary** field setting will change to **Yes**.

- **Note**: Just as an account is made private by making an account primary, making the domain non-private is done by revoking the primary status on the account. This can only be done by the account holder as explained in Managing your own Account with "My Account" (page 15).

6.2.3. Disabling and enabling an account

When an account is disabled, the account name will be greyed out in the **Accounts View** tree and the account holder can not log in.

An account can be disabled in two different ways.

- The system will disable an account after three times three unsuccessful logins (see also Suspended account - unsuccessful logins (see "Login failures" page 33)).
- A superior administrator can manually disable an account. This will have effect immediately, so the a disabled user that is logged in will be blocked from further actions.

An account can only be enabled manually by a superior administrator.

The button labeled **Disable ...** or **Enable ...** is controlled on the **Details** tab for the account.

6.2.4. Renewing another user's certificate

When and why are certificates renewed?

Certificates must be renewed before they expire. Certificates last for a year. One month before your certificate expires, you will receive an e-mail; 5 days before the expiration date, you will receive a reminder via the Console when you log on.

Certificates must be coordinated with passwords. Therefore, if a password is changed. the system will automatically generate a new certificate which is synchronized with the new password and send it to the account's email address.

Note that a renewed certificate is, in fact, a new certificate. When it is created, any previous certificate for an account will become invalid.

A user's certificate could be corrupted, compromised, or lost so you may need to issue a new certificate.

If the existing password is still thought to be OK, click **Renew Certificate** on the **Details** tab of the account.

If a new password is needed, click **New Password**.

6.2.5. Login failures

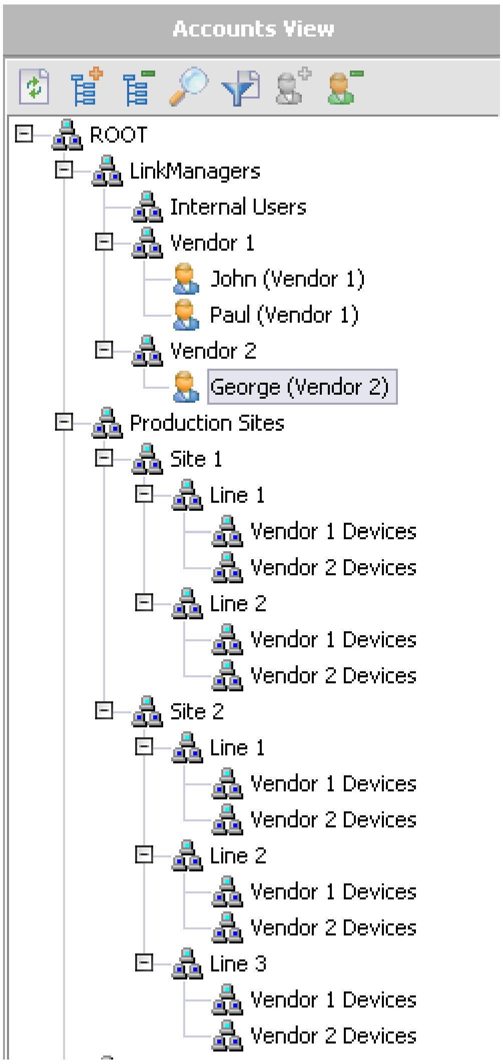
After three unsuccessful attempts to log in, the system will suspend the account for a number of seconds and then re-instate it. If you should happen to be looking at the **Details** tab of a suspended account, the read-only field **Suspended** will show **Yes**. Re-instatement is an automatic process.

If this sequence is repeated two times, the account is disabled. It can only be enabled by a superior administrator (see "Disabling and enabling an account" page 33).

6.3. Join Domains to Accounts

To allow a LinkManager to perform cross-domain device maintenance, it is possible to join domains outside a users home domain to the user account.

This is done through the “Account View”. Following up on the example on page 25, we suppose the following domain structure has been created and three users from two different vendors need to access selected devices at the production sites:

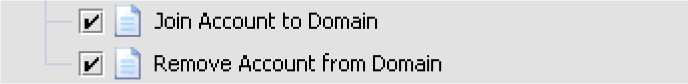


Accounts View

```
ROOT
  LinkManagers
    Internal Users
    Vendor 1
      John (Vendor 1)
      Paul (Vendor 1)
    Vendor 2
      George (Vendor 2)
  Production Sites
    Site 1
      Line 1
        Vendor 1 Devices
        Vendor 2 Devices
      Line 2
        Vendor 1 Devices
        Vendor 2 Devices
    Site 2
      Line 1
        Vendor 1 Devices
        Vendor 2 Devices
      Line 2
        Vendor 1 Devices
        Vendor 2 Devices
      Line 3
        Vendor 1 Devices
        Vendor 2 Devices
```

The users John and Paul from “Vendor 1” should be granted access to the devices in the various “Vendor 1 Devices” sub-domains, and George from “Vendor 2” should be granted access to devices in the various Vendor 2 Devices” sub-domains. Furthermore, John gets access to all production sites, while Paul only should have access to “Production Site 1”.

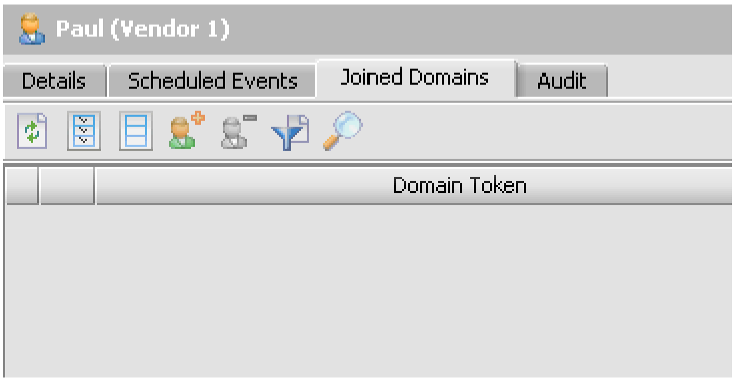
- **NOTE:** Only administrators with the following “Account” privileges may join domains to accounts:



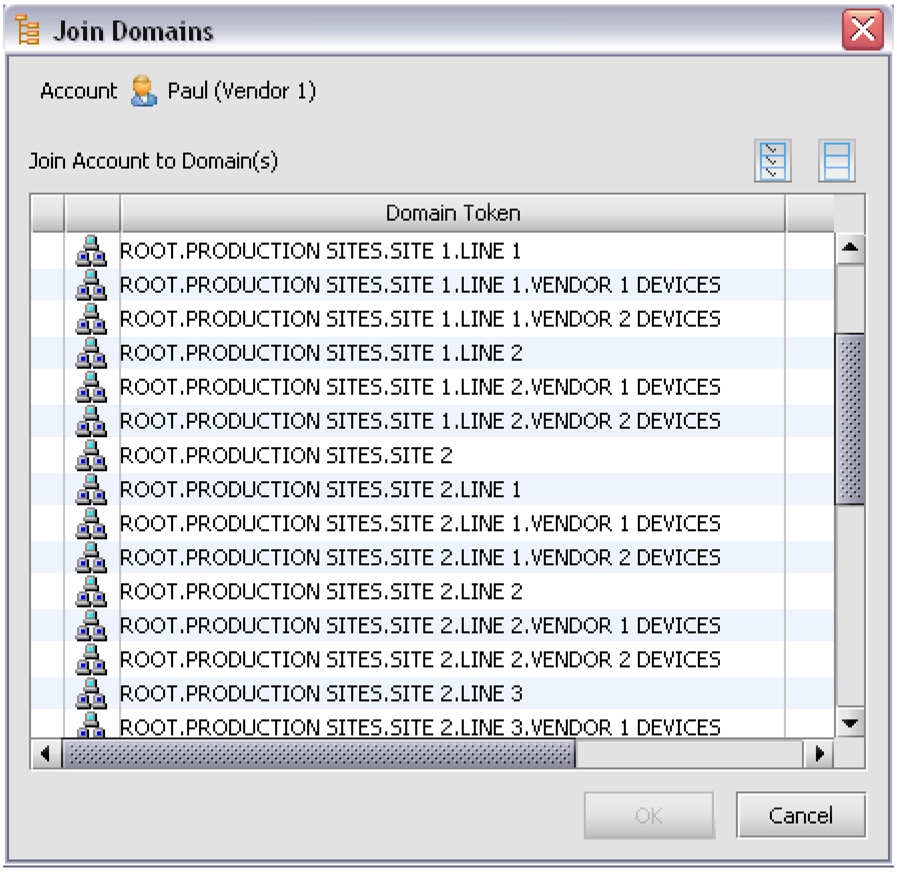
☑ Join Account to Domain

☑ Remove Account from Domain

To setup this, select the user in the left panel (here: Paul), and select the “Joined Domains” tab:



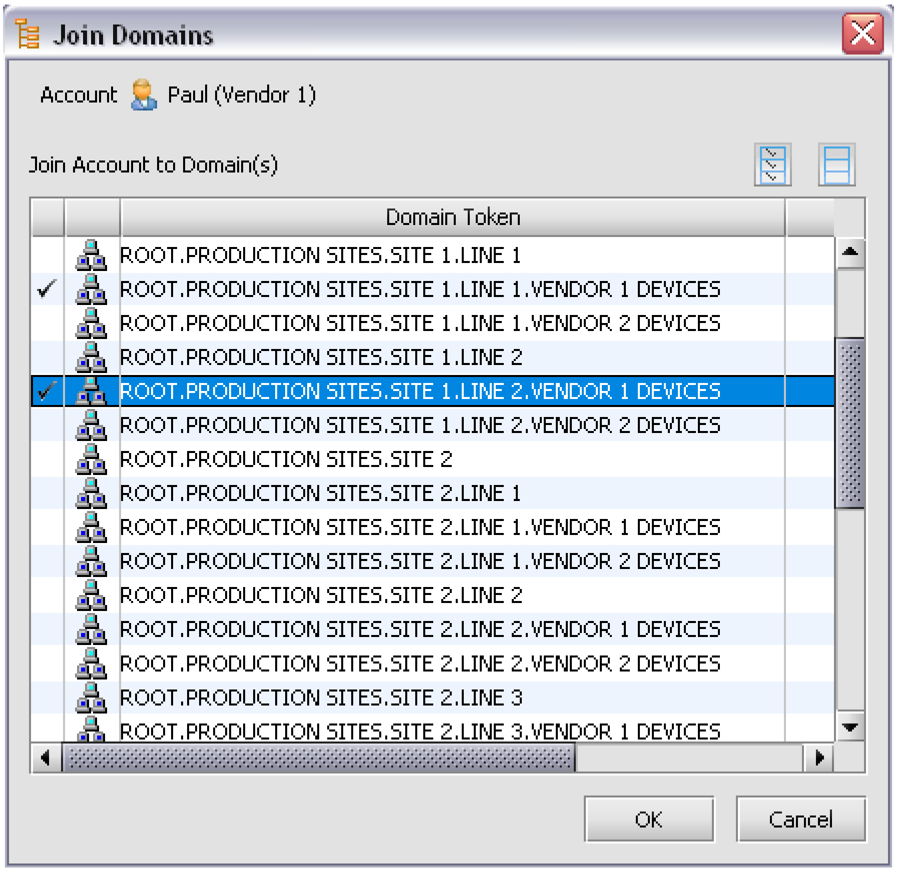
Now, click on the icon to select the domains to join to this account. This opens a selection panel:



Account: Paul (Vendor 1)

ROOT.PRODUCTION SITES.SITE 1.LINE 1
ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 2
ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 2
ROOT.PRODUCTION SITES.SITE 2.LINE 1
ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 2
ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 3
ROOT.PRODUCTION SITES.SITE 2.LINE 3.VENDOR 1 DEVICES

Now, select the sub-domains that Paul should have access to (in this case, only the sub-domains of Production Site 1):

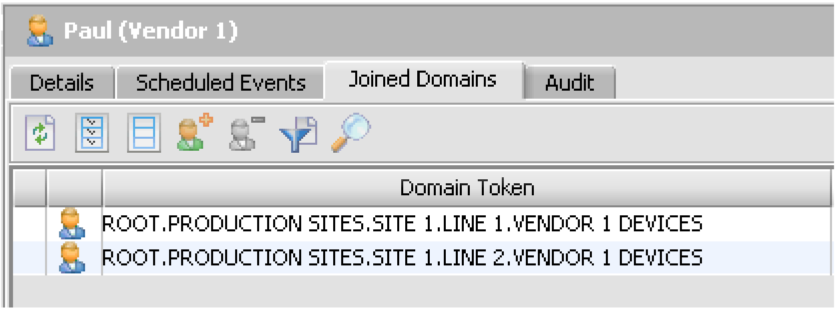


Account Paul (Vendor 1)

Join Account to Domain(s)

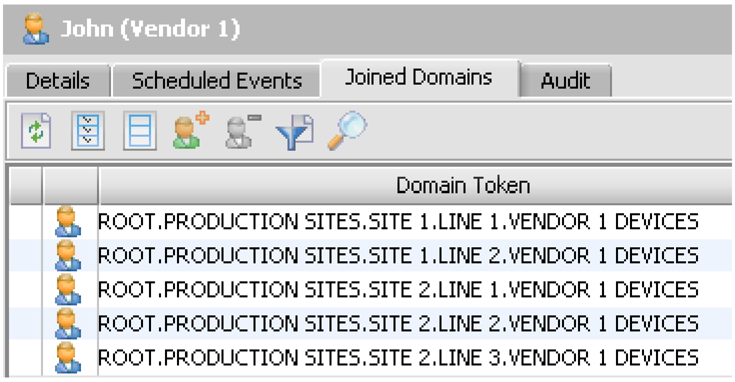
	Domain Token
	ROOT.PRODUCTION SITES.SITE 1.LINE 1
✓	ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 1 DEVICES
	ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 2 DEVICES
	ROOT.PRODUCTION SITES.SITE 1.LINE 2
✓	ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 1 DEVICES
	ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 2 DEVICES
	ROOT.PRODUCTION SITES.SITE 2
	ROOT.PRODUCTION SITES.SITE 2.LINE 1
	ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 1 DEVICES
	ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 2 DEVICES
	ROOT.PRODUCTION SITES.SITE 2.LINE 2
	ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 1 DEVICES
	ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 2 DEVICES
	ROOT.PRODUCTION SITES.SITE 2.LINE 3
	ROOT.PRODUCTION SITES.SITE 2.LINE 3.VENDOR 1 DEVICES

Click on "OK", and Paul will now have access to the selected domains:



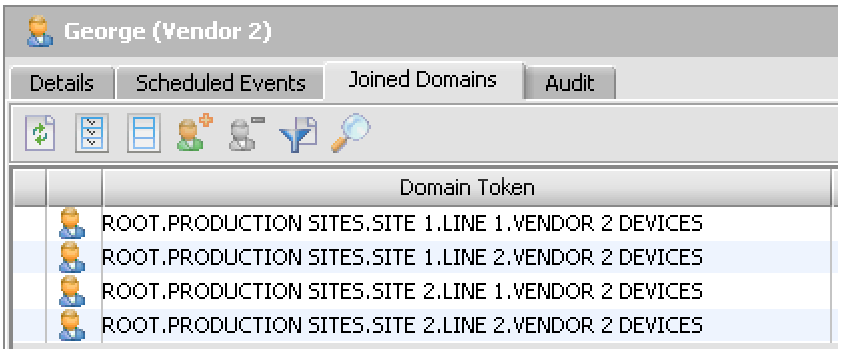
Domain Token
ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 1 DEVICES

Repeat this procedure for John ...



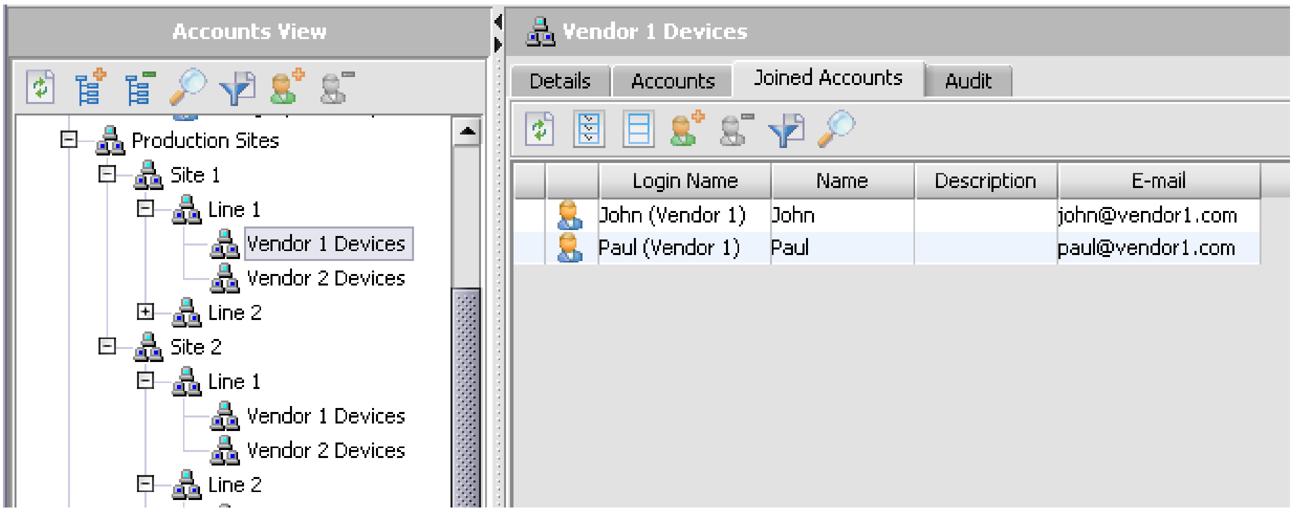
Domain Token
ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 1 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 3.VENDOR 1 DEVICES

… and George:



Domain Token
ROOT.PRODUCTION SITES.SITE 1.LINE 1.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 1.LINE 2.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 1.VENDOR 2 DEVICES
ROOT.PRODUCTION SITES.SITE 2.LINE 2.VENDOR 2 DEVICES

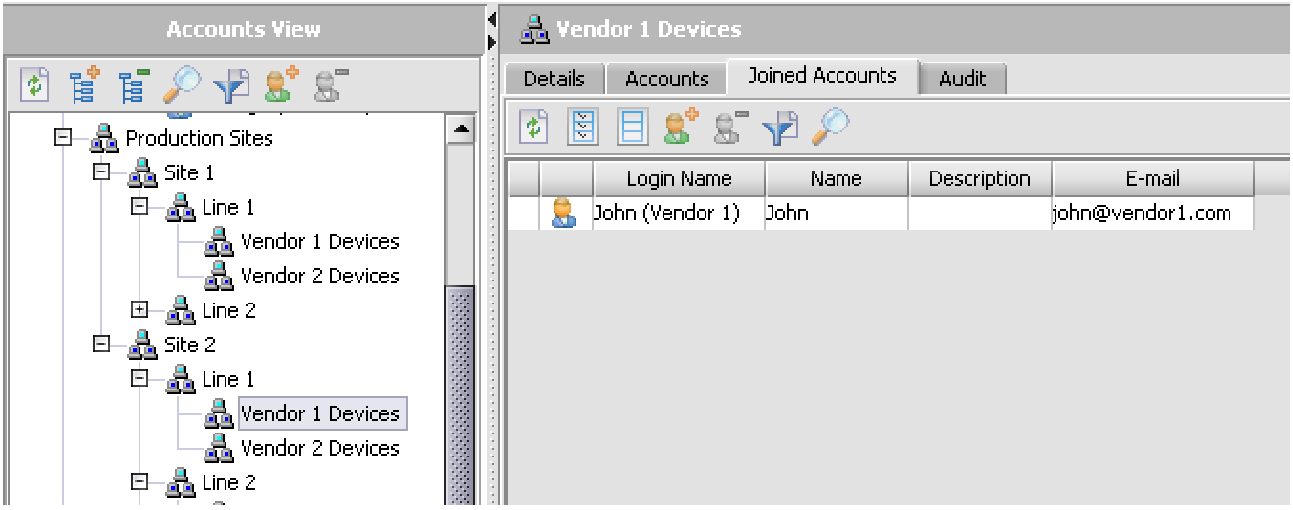
To verify the access for a specific domain, we select the domain in the left panel and use the "Joined Accounts" tab:



Login Name	Name	Description	E-mail
John (Vendor 1)	John		john@vendor1.com
Paul (Vendor 1)	Paul		paul@vendor1.com

As expected, both John and Paul may access the "Vendor 1 Devices" on "Production Site 1, Line 1".

But only John has access to "Vendor 1 Devices" on "Production Site 2, Line 1":



Login Name	Name	Description	E-mail
John (Vendor 1)	John		john@vendor1.com

You can also join specific accounts to a domain by clicking the icon in the "Joined Accounts" tab.

So logically, joining a Domain to an Account is equivalent to joining the Account to the Domain.

7. Accounts, roles, and privileges

An account corresponds to a user - not to the company or other legal entity holding a license to use the GateManager.

GateManager uses a so-called role-based access control.

Each account is assigned a role, which defines what the user is allowed to do within the limits posed by the domain hierarchy. Examples of roles: "Domain Administrator". "Appliance Administrator".

Roles are created as a collection of privileges. If you find yourself blocked from actions you believe you should be able to perform, check the full list of privileges (see "Privileges and groups of privileges" page 38). This can help you to discuss the problem with your superior administrator.

It is the Server Owner who defines the roles and creates a role hierarchy on the basis of information only given in the Server Setup Guide.

7.1. Principles for applicable roles

The applicable-role hierarchy is applied to privileges having to do with accounts and roles.

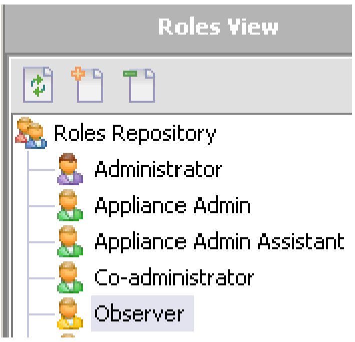
If a role, call it X, is on the list of Applicable Roles for another role, call it A, then - depending on the specific privileges in role A - a user with the role A can

- view the content of role X
- assign role X to other accounts within his or her own domain hierarchy
- manage any account within the domain hierarchy that has the role X
- edit role X

Roles are only applicable in one direction. That is, if X is on the Applicable Roles list for A, then A cannot be put on the Applicable Roles list for X. This uni-directionality is what creates the hierarchy.

7.2. Your own applicable roles

You cannot see your own applicable roles in My Account (see "Viewing your account privileges" page 18). But all of the roles that have been made applicable to your role are visible in the Roles repository (**Roles View**).

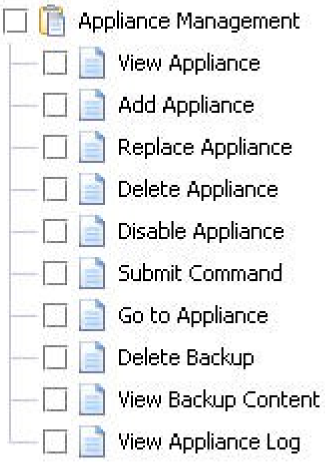


To see the **Applicable Roles** list for each of the roles you can view, select the role. The list is on the **Details** tab.

7.3. Privileges and groups of privileges

This section shows all possible privileges in each group. It also includes some comments that can help the GateManager Owner to decide whether or not to adjust the standard role set.

7.3.1. Appliance Management

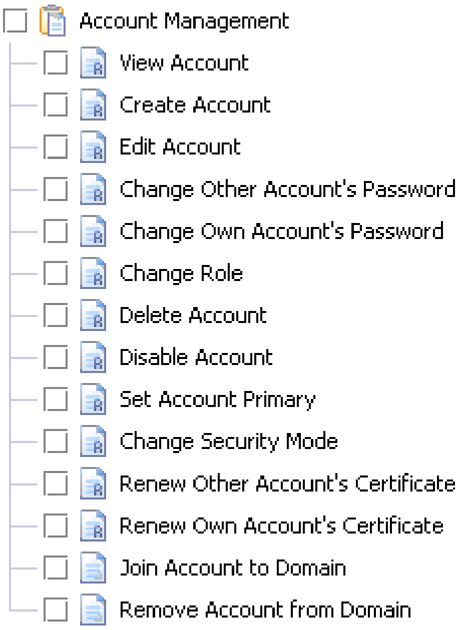


- ☐ Appliance Management
  - ☐ View Appliance
  - ☐ Add Appliance
  - ☐ Replace Appliance
  - ☐ Delete Appliance
  - ☐ Disable Appliance
  - ☐ Submit Command
  - ☐ Go to Appliance
  - ☐ Delete Backup
  - ☐ View Backup Content
  - ☐ View Appliance Log

Comments

Submit Command only covers immediate execution of commands. To support scheduling, privileges must be selected in the Scheduler group (see "Scheduler" page 41).

7.3.2. Account Management



- ☐ Account Management
  - ☐ View Account
  - ☐ Create Account
  - ☐ Edit Account
  - ☐ Change Other Account's Password
  - ☐ Change Own Account's Password
  - ☐ Change Role
  - ☐ Delete Account
  - ☐ Disable Account
  - ☐ Set Account Primary
  - ☐ Change Security Mode
  - ☐ Renew Other Account's Certificate
  - ☐ Renew Own Account's Certificate
  - ☐ Join Account to Domain
  - ☐ Remove Account from Domain

Comments

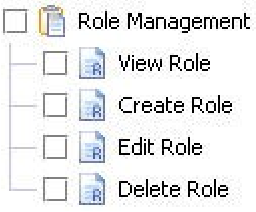
The "R" mark on each privilege indicates that using it is contingent on the applicable-roles hierarchy.

Selection of **Change Own Account's Password** automatically selects **Renew Own Account's Certificate**, and vice-versa. If an account is put into Basic Security Mode, it is not necessary to give a role with these privileges.

Selection of **Change Other Account's Password** automatically selects **Renew Other Account's Certificate**, and vices versa.

There is no special privilege to use the Revoke Primary button. Any account with an X.509 certificate that has been made “primary” (to create a private domain) is allowed to revoke primary status, regardless of the role assigned to the account.

7.3.3. Role Management



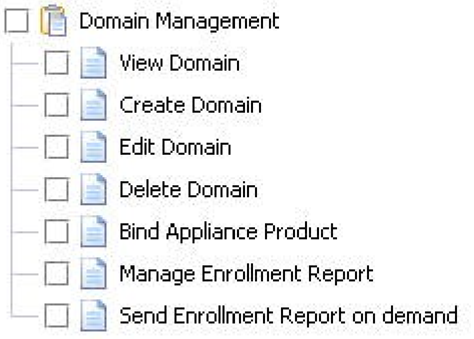
- □ Role Management
  - □ View Role
  - □ Create Role
  - □ Edit Role
  - □ Delete Role

Comments

The "R" mark on each privilege indicates that using it is contingent on the applicable-roles hierarchy.

- **IMPORTANT**: Because roles affect the entire installation, privileges for creating, editing or deleting roles should only be assigned to the **Manager** role.

7.3.4. Domain Management



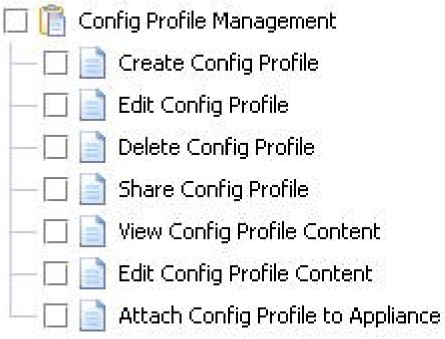
- □ Domain Management
  - □ View Domain
  - □ Create Domain
  - □ Edit Domain
  - □ Delete Domain
  - □ Bind Appliance Product
  - □ Manage Enrollment Report
  - □ Send Enrollment Report on demand

Comments about Enrollment Report

Enrollment Reports were called Appliance Audits before GateManager v 3.4.

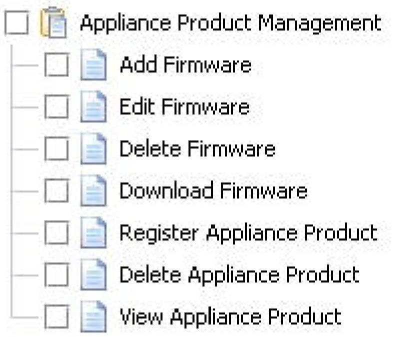
As of GateManager v3.5 the **Send Enrollment Report on demand privilege** has been removed as a separate privilege; the action involved is now automatically included in **Manage Enrollment** which also includes scheduling regular production and e-mailing of reports about the Appliances in a domain.

7.3.5. Configuration Profile Management



- □ Config Profile Management
  - □ Create Config Profile
  - □ Edit Config Profile
  - □ Delete Config Profile
  - □ Share Config Profile
  - □ View Config Profile Content
  - □ Edit Config Profile Content
  - □ Attach Config Profile to Appliance

7.3.6. Appliance Product Management



- □ Appliance Product Management
  - □ Add Firmware
  - □ Edit Firmware
  - □ Delete Firmware
  - □ Download Firmware
  - □ Register Appliance Product
  - □ Delete Appliance Product
  - □ View Appliance Product

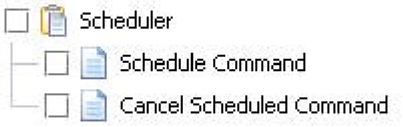
Comments

The first three firmware-related privileges refer to adding firmware file to a folder in the **Appliance Products View** on the GateManager, editing a firmware entry (description or content), and removing the file from the GateManager.

Download Firmware gives the user permission to download firmware from the GateManager to disk. As standard, we recommend that this permission is only included in the **Manager** role.

Because **Register Appliance Product** (install plugin) and **Delete Appliance Product** (delete plugin) affect the entire GateManager, as standard, these privileges are only assigned to the **Manager** role.

7.3.7. Scheduler

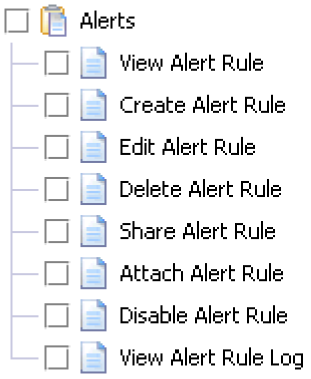


- □ Scheduler
  - □ Schedule Command
  - □ Cancel Scheduled Command

Comment

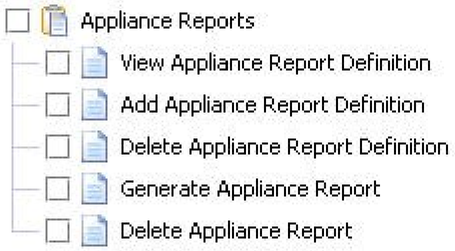
Scheduling applies to commands. Commands relate only to Appliances.

7.3.8. Alerts



- □ Alerts
  - □ View Alert Rule
  - □ Create Alert Rule
  - □ Edit Alert Rule
  - □ Delete Alert Rule
  - □ Share Alert Rule
  - □ Attach Alert Rule
  - □ Disable Alert Rule
  - □ View Alert Rule Log

7.3.9. Appliance Reports

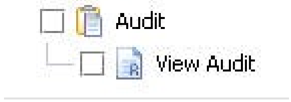


- □ Appliance Reports
  - □ View Appliance Report Definition
  - □ Add Appliance Report Definition
  - □ Delete Appliance Report Definition
  - □ Generate Appliance Report
  - □ Delete Appliance Report

Comments

Appliance Reports are queries about Appliances in any given domain. They are created and used in the **Appliances View**, **Reports** tab for the Domain.

7.3.10. Audits (Event Logs)



- □ Audit
  - □ View Audit

Comments

Audits are logs of actions taken upon objects in GateManager. Each GateManager object has an **Audit** tab.

The "R" mark on the View Audit privilege indicates that using it is contingent on the applicable-roles hierarchy.

- **Note**: Audits used to be called Events - and it used to be possible to give permission to delete an Event log.

8. Appliances: Enroll, Disable, Delete, Move, Replace

8.1. Enroll an Appliance

8.1.1. Three parameters are needed before you start

Parameter	Comments
GateManager Proxy IP address	Remember that it is always the Appliance which initiates connection to the GateManager. You may also be given a secondary IP address.
GateManager Domain Token	This is needed to make the Appliance announce itself in the appropriate place in the hierarchy. Domain tokens are not case-sensitive. Tip: You can leave out the first element "root" in the domain token as long as you do not have a domain called "root" anywhere within your own hierarchy.
GateManager Appliance Name	The system knows the Appliance by serial numbers and object codes. The GateManager Appliance Name is "only" for people - and can be changed at will. However, if you are going to be managing lots of Appliances, think about how to make your naming system people-friendly and stable. The online help or other documentation for the Appliance usually includes advice about why and how to use GateManager Appliance Names instead of (for example) network device names.

8.1.2. Enrollment steps - standard

If the Appliance you want to enroll is an agent hosted on another Appliance, you must, of course, enroll the hosting Appliance first.

1. Find an appropriate **Domain Token** in the GateManager Console. Use the **Domains View**.

   The token for any given domain is shown on the **Details** tab for the domain. If you operate both the GateManager Console and the individual appliance, it is advisable to copy the Domain Token from GateManager Console to your clipboard.

2. Enter and activate the three mandatory parameters (see "Three parameters are needed before you start" page 43) in the Appliance via its own interface.

   Do this directly, or by using the Appliance Launcher.

   The online help or other documentation for the product usually includes instructions for configuring additional parameters.

   Configuring the Appliance can, of course, be done by someone that does not have a GateManager Account.

3. Using the GateManager Console, find the Appliance in the **Appliances View** tree.
4. The Appliance state will be tentative.
5. Right click the Appliance in the **Appliances View** tree.
6. Select **Attach Appliance to Domain** from the context menu.
7. This starts a wizard to guide you through confirming or moving the Appliance’s placement.

   The wizard will also offer you some housekeeping, such as attaching an alert rule, or taking a configuration backup. Most of the actions must be triggered by a time-slot or a condition; if you just want the action carried out immediately, select a time-slot that starts within a few minutes.

   All of the actions offered can be done in other ways after the attachment is completed.

8. After you click **Finish** in the wizard, the ? or ! symbol will disappear.

- **IMPORTANT**:

When a tentative Appliance becomes attached, its domain placement is confirmed and unchangeable. If you need to move the Appliance, you must first delete it from the Console. Then configure the device, agent or relay with a new domain token, and activate the GateManager connection.

8.1.3. Enrollment steps - a "manual" alternative

The standard enrollment method is also known as the "Attach Tentative Appliance Method".

An alternative method is "Add New Appliance" - manually - which can only be used with physical appliances. The Add New Appliance method is rarely used; consult Support for information about when it could be relevant.

What "Add New Appliance" does

Add New Appliance allows you to place it precisely where you want from the beginning. It will never end up in the “unrecognized” appliance state. If there is any value for Domain Token in the appliance’s configuration, it will be ignored at the time of enrollment.

However, if you want to exercise this control, you need to Add the Appliance in the GateManager Console *before* you enter the GateManager Proxy Server IP into the appliance’s own configuration. Otherwise, the Appliance will announce itself before you have a chance to even think about it. When you try to use **Add New Appliance** in the Console, you will be told that an Appliance with that serial number already exists in the system.

Overview of steps

1. Add New Appliance using the GM Console. You must have the appliance's serial number at hand along with the standard three parameters.
2. Configure the appliance to be managed
3. Follow up using the GM Console

Add New Appliance Step 1 with the GateManager Console

1. In the Appliances View, do one of the following in order to select the Domain you want to place the Appliance in:
   - Directly from the tree: Right-click the domain name to activate the context menu. Click **Add New Appliance**.
   - Invoking the Main Menu: Highlight (left-click) the domain name. On the Main Menu click **Appliances**, and then click **Add New Appliance**.
2. This opens the first page of the **Add New Appliance Wizard**.
3. Select the correct **Appliance Product** from the drop-down list.
4. Type in the **Serial Number**.

   Tip: If you have the appliance’s own interface active, you may be able to copy the serial number from the appliance to your clip-board and paste it into the field.
5. Click **Next**.
6. The **Add New Appliance** wizard can also be used to upgrade firmware, do a configuration backup, attach an alert rule, and/or attach a configuration profile (with or without applying the profile). If you want to do any of these things, click Next as needed.
7. Click Finish.
8. The Appliance will show up in the Console in the Unknown (transitory) connection state (yellow), which will go over to failed (red) after the Unknown State timeout. The “Details” tab for the New Appliance will show that the Connection State is Failed (red) and the Appliance State is Attached.
9. Go to Step 2.

Add New Appliance Step 2 is done on the appliance

1. Type in the IP of the GateManager Proxy.
2. Type in the GateManager Appliance Name.
3. Option, but strongly recommended: Type in the Domain Token.

   Being that the GateManager is already prepared for an Appliance with this serial number, the Domain Token will be ignored in connection with this initial enrollment. However, should anything interrupt the connection, the Domain Token will be used to find the correct placement upon re-connection.

4. Activate the settings; in some appliances a reboot will be required.
5. Go to Step 3.

Add New Appliance Step 3 with the GateManager Console

Follow along with the Appliance's status on the Console by opening the Appliances View in the Tree and expanding it to where you have placed the Appliance.

The Appliance icon will turn green. The “Appliance Name” will be displayed (name or serial number, depending on your general Session “Preferences” for the Console). Shortly thereafter the **Details** tab for the Appliance will be filled out.

Done.

8.2. Disable and Enable an Appliance

Why disable an Appliance – and how it works

Sometimes you don’t need to follow along with an Appliance’s Status – and you don’t want to receive any alerts about it.

You could, of course, detach alert rules from the Appliance, or even delete the Appliance from the system. But if you temporarily disable the Appliance instead, you get to keep *all* of your configurations in the GateManager.

When you disable an Appliance, the Server Proxy tells the physical appliance to disconnect and not to attempt connecting again until after its timeout (retry-to-connect interval).

While an Appliance is Disabled, you can not use the **Go To Appliance** function and you cannot carry out immediate actions from the **Command** submenu . You can, however, schedule Commands.

To disable a single Appliance

1. Highlight (left-click) the Appliance's name in the **Appliances View Tree**.
2. Make sure that the **Details** tab is activated.
3. In the **Appliance Status** block, click the **Disable ...** button. The text on the button will switch to Enable...

To disable several Appliances within a Domain

1. In the **Appliances View** tree, find and highlight (left-click) the domain.
2. Activate the **Appliances** tab for the domain.
3. On the table, select the Appliance entries you want to disable.
4. On the **Main** menu, click **Appliances** and then **Disable Appliances**.

To enable a disabled Appliance

Only one Appliance can be enabled at a time.

Proceed in the same way as described for disabling a single Appliance. Click the **Enable ...** button.

How enabling works

While the Appliance is disabled, after each timeout, it will retry to connect; the timeout is specific to each appliance product. Once you enable the Appliance, the next time it tries to connect, the connection will be accepted.

If, after enabling the Appliance in the GateManager Console, you want the Appliance (physical appliance or hosted agent) to connect without waiting for the duration of this interval, reboot the physical appliance from its own interface.

8.3. Delete an Appliance

- **WARNING - BEFORE YOU START**:

  If you remove the Appliance from the system, all of its configurations and history will be lost. Consider disabling it instead as shown in Disable and Enable an Appliance (page 45).

The following method can be used for Appliances (both physical appliances and hosted agents), regardless of Appliance State or Connection State.

- **IMPORTANT**:

  To remove an Appliance from the system you must *both* delete it in the GateManager Console *and* change the physical appliance's configuration to prevent the Appliance from announcing itself again the next time it gets rebooted. In some appliances's GateManager configurations, you can de-activate GateManager; in others you need to remove the GateManager Proxy IP address. You should always do this before working with the Console.

To delete a single Appliance

1. Be sure that you have prepared the appliance itself so that it does not try to enroll itself as a Tenative Appliance.
2. Right-click the Appliance's name in the **Appliances View Tree Pane**.
3. Click **Delete Appliance** on the context menu.

To delete several Appliances within a Domain

1. Be sure that you have prepared the appliances so that they do not try to enroll themselves as Tentative Appliances.
2. In the **Appliances View** tree, find and highlight (left-click) the domain.
3. Activate the **Appliances** tab for the domain.
4. On the table, select the Appliance entries you want to delete. You can use this icon to select everything in the list .
5. Click the **Delete Appliance** button on the tab's tool bar.

8.4. Move an Appliance

Actually moving an attached Appliance is not possible

Because so many functions in the GateManager are associated with Domain placement, moving an attached Appliance is extremely complicated.

For example, alert rules and configuration profiles are always created in specific home domains, so moving an Appliance means thinking about alert rules and configuration profiles in detail – would they be appropriate in the new domain? Also, you need to be sure that the domain to which the Appliance will be attached has an appropriate product binding.

You should try to avoid having to move an attached Appliance. Perhaps a Wizard will be created one day to handle all of the domain issues. Until then, if it is truly necessary to move an attached Appliance, use the following work-around

Work-around

1. In the GateManager Console, delete the Appliance as shown in Delete an Appliance (page 46). This removes all information about it from the system, so you lose configuration backups, scheduled commands and events log.
2. Enroll the Appliance again as shown in Enroll Appliance (see "Enroll an Appliance" page 43).

8.5. Replace a physical appliance

An appliance could be damaged or develop a defect. You can use the Replacement wizard to ensure that the GateManager will handle the new appliance in the same way that it has handled the old one. And if you follow the instructions, the disruption will be absolutely minimal.

Hopefully, you will never have to replace an appliance. But as an insurance, you should be sure to schdule regular configuration backups on the GateManager.

- **IMPORTANT**:

  The order in which you do things is critical – make sure that all pre-requisites are in place, and then follow the replacent steps in the order they are shown.

8.5.1. Pre-requisites - before using the Replace Appliance Wizard

Decide whether or not it is appropriate to load the old appliance's configuration to the new appliance. Support can advise if you are in doubt.

Make sure that all of the following conditions are fulfilled

“Old” appliance = the appliance to be replaced

1. The **Appliance State** must be **Attached**. In other words, information about that appliance must be in the GateManager database and be associated with the correct domain. It doesn’t matter whether the Appliance is disabled (square icon decorated with a big red X) or not.
2. Any **Connection State** is OK if you will not be loading the old appliance's configuration to the new appliance.

   If you *are* going to load a configuration backup from the old appliance into the replacement appliance, you should physically remove the old appliance from the network before starting the replacement. Otherwise you can risk having two appliances/¬Appliances registered with the same IP address. So, in practice, the Connection State will usually be **Disconnected**. This is shown in the replacement example.

“New” appliance = the replacement appliance

1. Make sure that you have the necessary information for enrollment as shown in “Three parameters are needed before you start” (page 43).
2. If the appliance being replaced is an EasyTunnel client, you need to enter the MAC address of the new appliance into the EasyTunnel server’s configuration. This is done from the appliance's native interface.

8.5.2. How to use the Replace Appliance Wizard

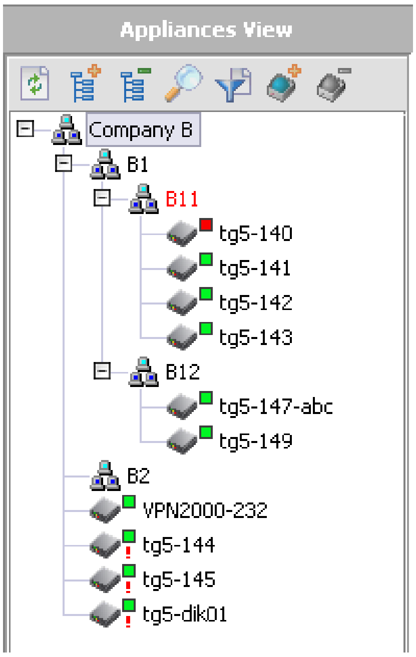
The following instructions are based on an example with the following starting point:

The appliance/Appliance tg5-140 in the “B11” Domain needs to be replaced. In this example, we assume that there is a configuration backup which is going to be loaded into the replacement appliance. You are logged in as “Company B Boss”, which is why it isn’t necessary to enroll tg-144 directly in the Domain “B11”.

Steps

1. Make sure that the old appliance tg5-140 has the Appliance State **Attached**.
2. Physically remove tg5-140 from the network, but do not delete the Appliance from the GateManager Console.
3. Physically connect the new appliance (tg5-144) to the network and enroll it using the Tentative Appliance approach as shown in Enrollment steps - standard (page 43).

   Result:

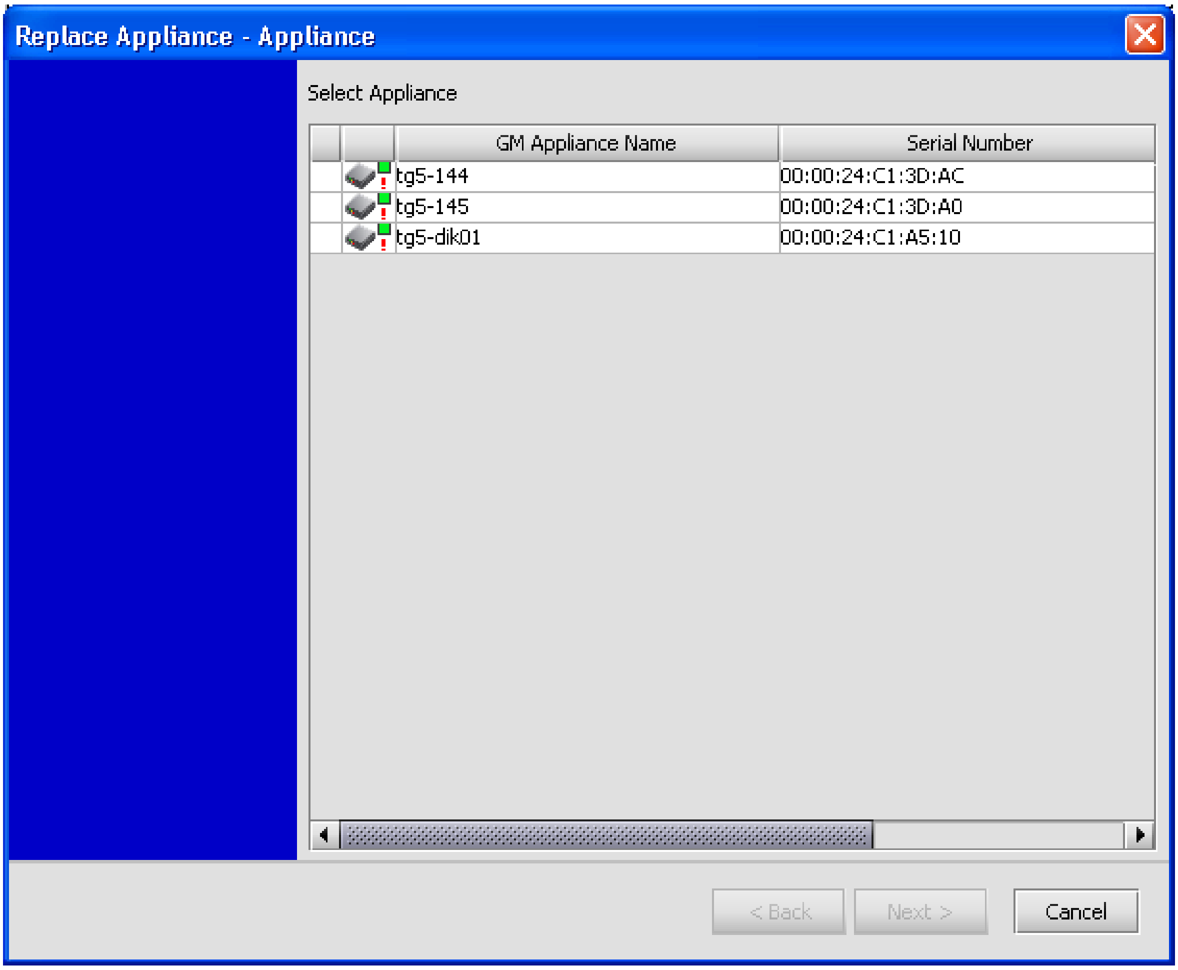
   

   Be sure that the following three conditions are fulfilled

   - The **Appliance State** must be Tentative - that is either New ! or Unrecognized ?.
   - The Appliance must not be Disabled.
   - The **Connection State** must be Connected.

4. To start the Replacement Wizard: right-click on the Appliance name (tg5-140) of the physical appliance to be replaced. Then click **Replace** on the context menu.

5. This brings up a list of all Tentative Appliances within the Domain of the Account that is logged in. (If there are no Tentative Appliances, the Console will hang).

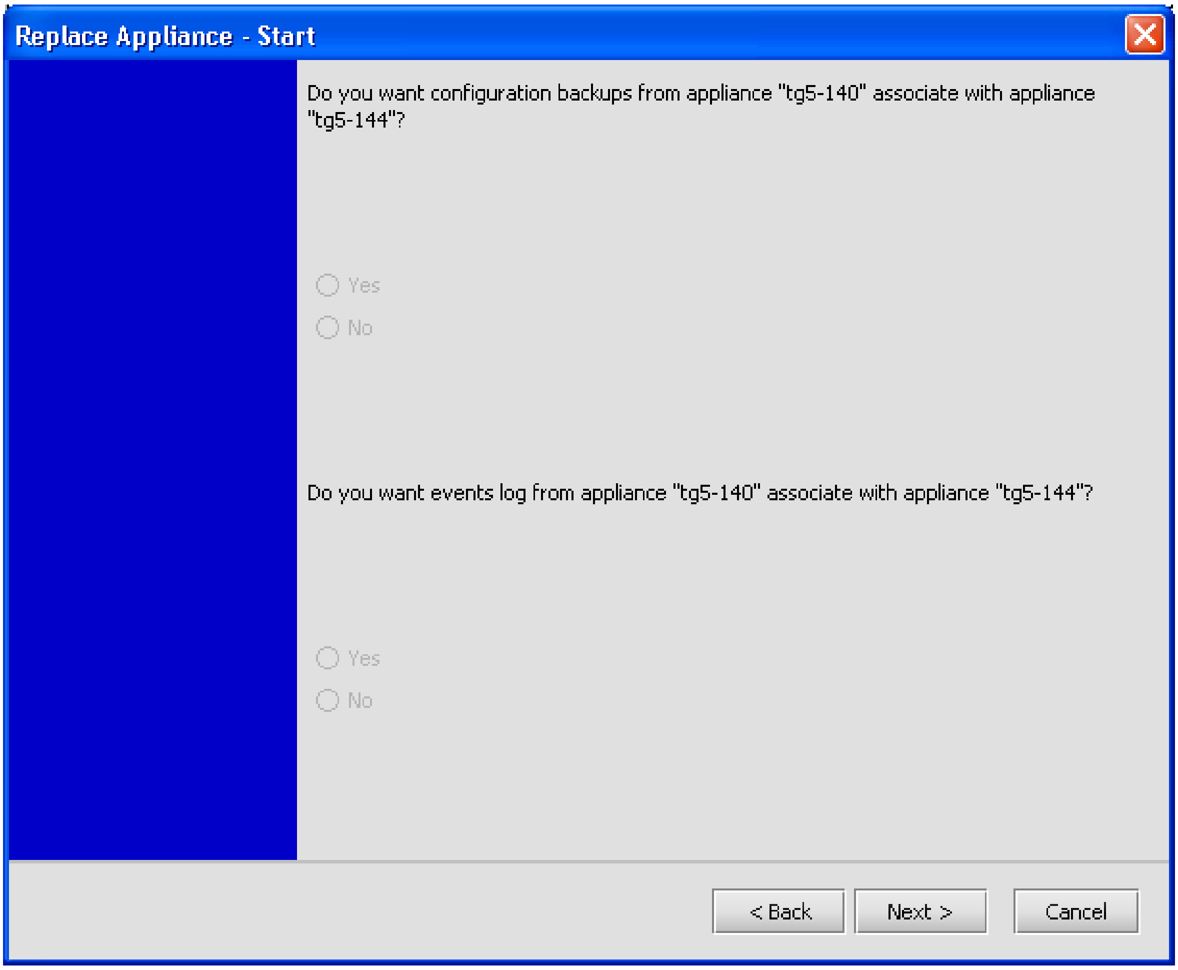


Select Appliance

		GM Appliance Name	Serial Number
		tg5-144	00:00:24:C1:3D:AC
		tg5-145	00:00:24:C1:3D:A0
		tg5-dik01	00:00:24:C1:A5:10

6. Select the Appliance to be used as a replacement – **tg5-144** in our example. The **Next** button will then be made available.
7. Click **Next**.

8. Result: A confirmation screen asks you whether or not you want to apply the old appliance’s/Appliance’s (tg140s) Configuration Backups and/or Audits log (previously called Events log) to the replacement appliance/Appliance (tg144).



Do you want configuration backups from appliance "tg5-140" associate with appliance "tg5-144"?

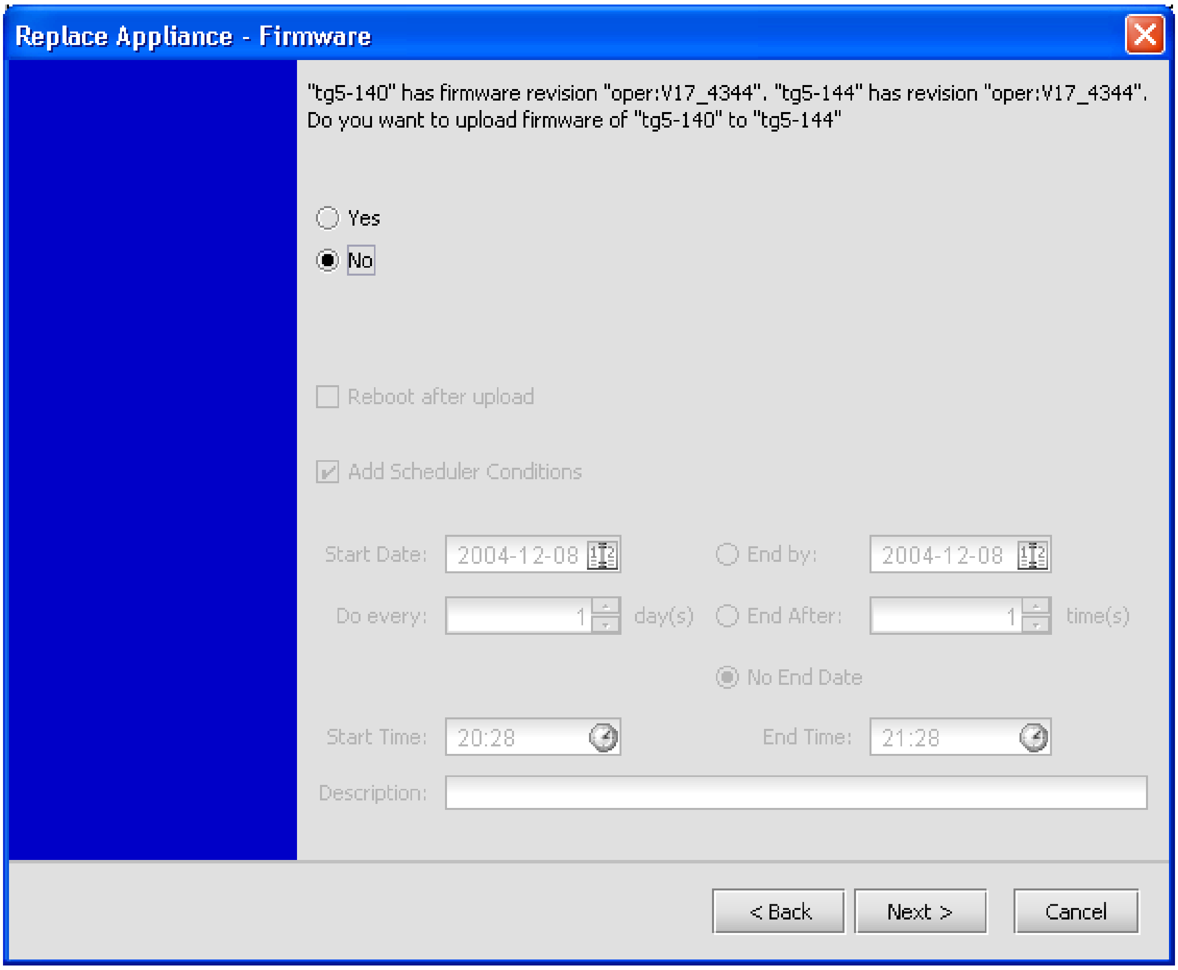
○ Yes
○ No

Do you want events log from appliance "tg5-140" associate with appliance "tg5-144"?

○ Yes
○ No

9. After selecting Yes or No to both questions, click Next.

10. Result: A screen tells you which firmware the old appliance is running.



Replace Appliance - Firmware

"tg5-140" has firmware revision "oper:V17_4344". "tg5-144" has revision "oper:V17_4344".
Do you want to upload firmware of "tg5-140" to "tg5-144"

○ Yes
● No

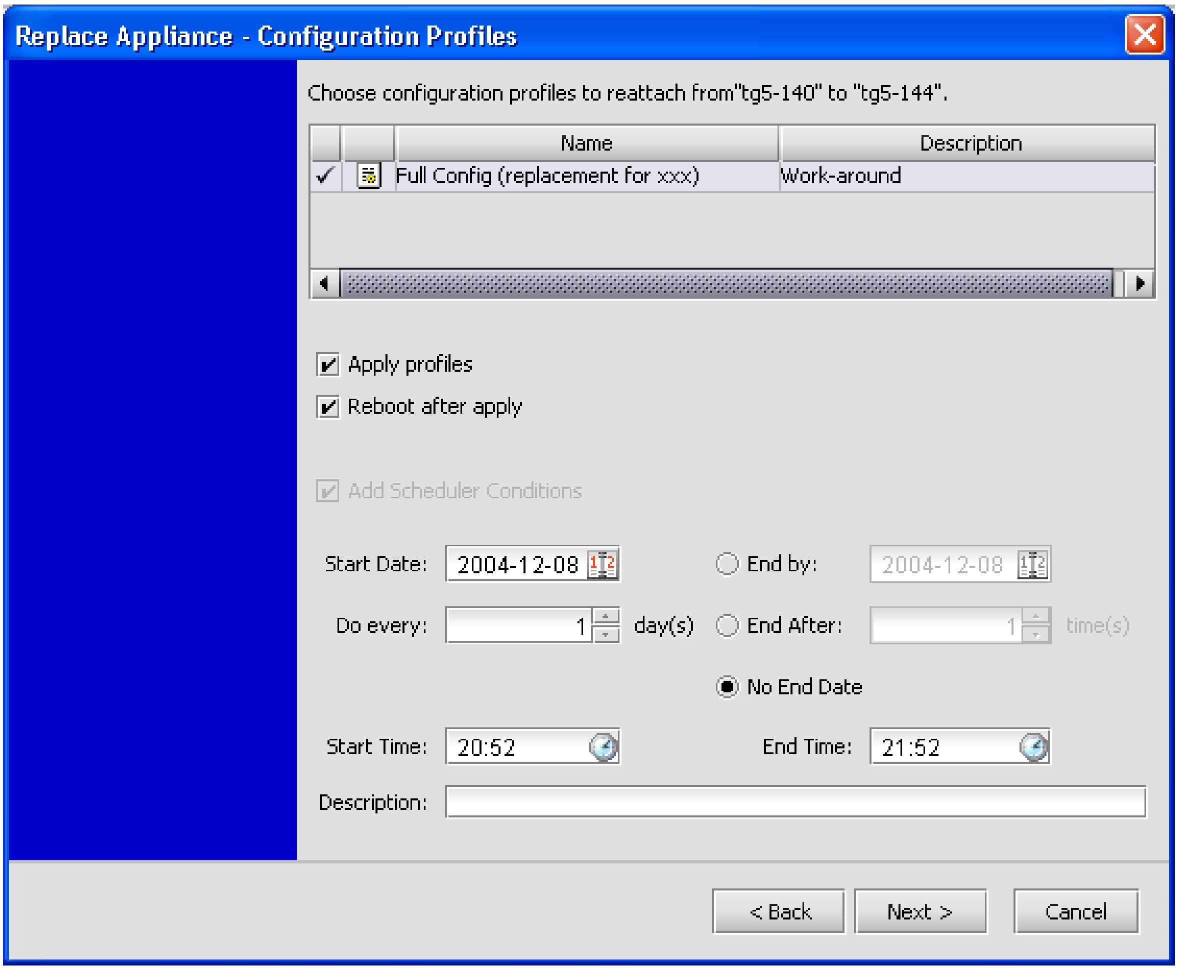
□ Reboot after upload

☑ Add Scheduler Conditions

Start Date: 2004-12-08 ○ End by: 2004-12-08
Do every: 1 day(s) ○ End After: 1 time(s)
● No End Date
Start Time: 20:28 End Time: 21:28
Description:

If the old appliance is loaded with a firmware known to the system (under Appliance Products), and you want to load the same firmware into the replacement appliance, select Yes. In this example, you click No. Click **Next**.

11. Result: A screen displays configuration profiles currently attached to the old appliance and allows you to select one or more of them to be attached to the new one.



Replace Appliance - Configuration Profiles

Choose configuration profiles to reattach from"tg5-140" to "tg5-144".

		Name	Description
✓		Full Config (replacement for xxx)	Work-around

☑ Apply profiles

☑ Reboot after apply

☑ Add Scheduler Conditions

Start Date: 2004-12-08 ○ End by: 2004-12-08

Do every: 1 day(s) ○ End After: 1 time(s)

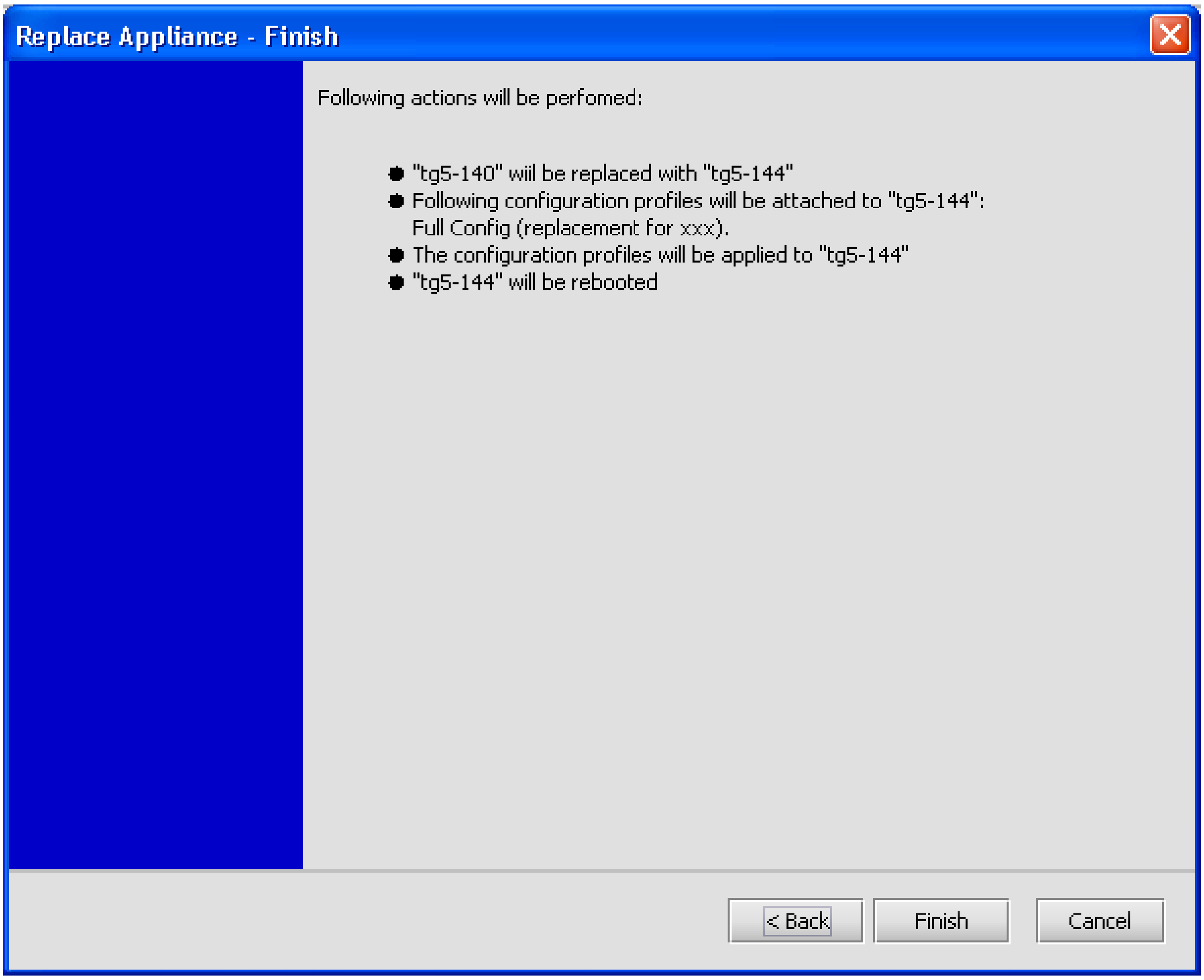
● No End Date

Start Time: 20:52 End Time: 21:52

Description:

12. Click **Next**.

13. Result: The Finish screen shows you all of your selections.



Following actions will be perfomed:

- "tg5-140" wiil be replaced with "tg5-144"
- Following configuration profiles will be attached to "tg5-144": Full Config (replacement for xxx).
- The configuration profiles will be applied to "tg5-144"
- "tg5-144" will be rebooted

Click **Finish** if you are satisfied. Otherwise you can **Cancel** the entire operation or use the **Back** button to change previous screens.

Done.

9. Alerts

9.1. Introduction to Alerts

The GateManager can generate alerts (alert notifications) on triggers defined in alert rules.

You can create alert rules that just contain the same information found on the Console. And you can create alert rules that contain a range of additional information.

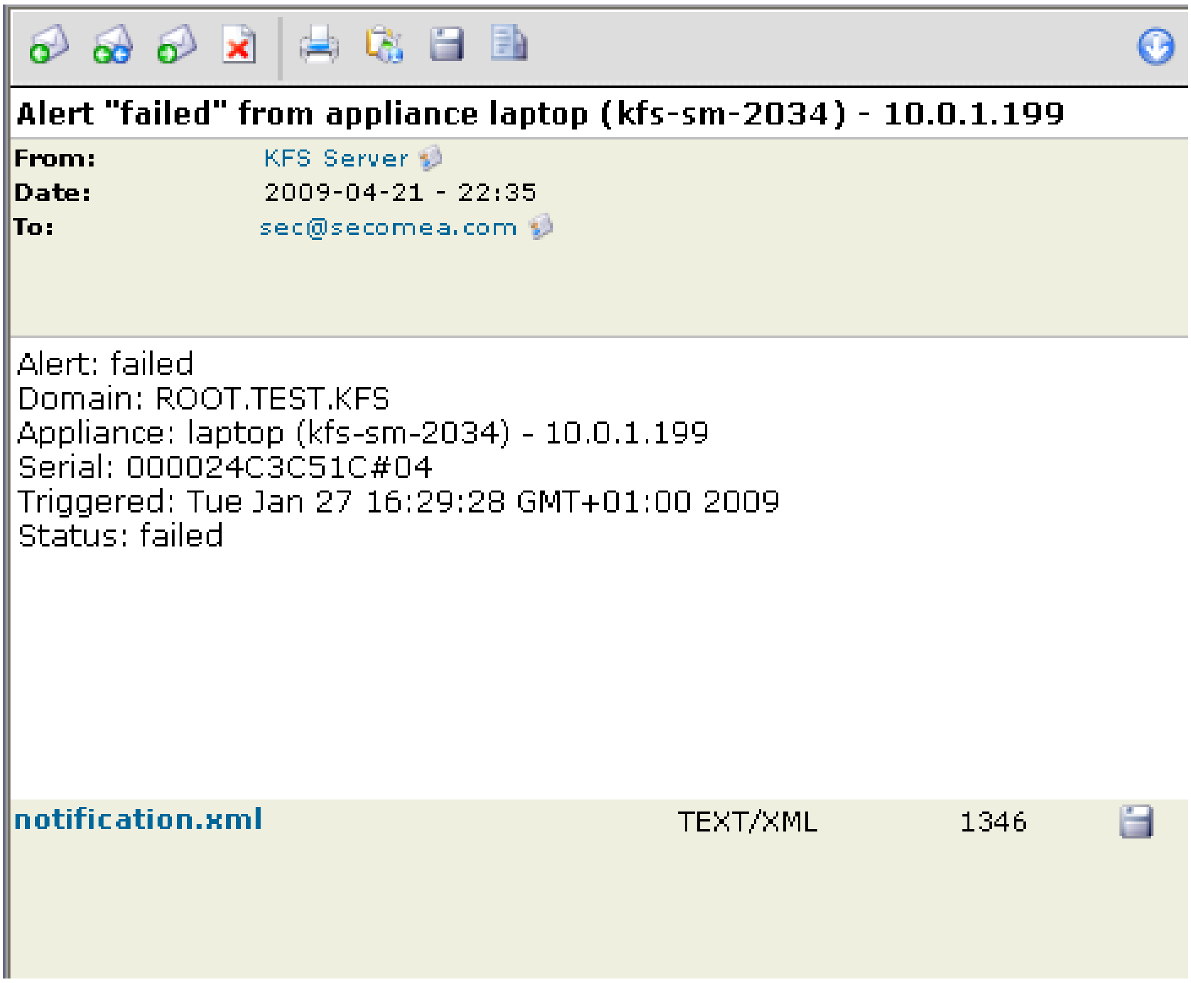
An alert rule is created in a given home domain and can be shared downward in the tree to all child domains.

To use an alert rule, you attach it to an Appliance and specify one or more recipients for alert notifications. When a rule is triggered, the alert is registered in the Appliance's Alert Log and an e-mail notification is sent.

9.2. Alert notification example

The alert always concerns an individual Appliance to which the alert rule is attached.

Example:



Alert "failed" from appliance laptop (kfs-sm-2034) - 10.0.1.199

From: KFS Server
Date: 2009-04-21 - 22:35
To: sec@secomea.com

Alert: failed
Domain: ROOT.TEST.KFS
Appliance: laptop (kfs-sm-2034) - 10.0.1.199
Serial: 000024C3C51C#04
Triggered: Tue Jan 27 16:29:28 GMT+01:00 2009
Status: failed

notification.xml TEXT/XML 1346

The subject line in an alert shows the name you have given to the alert rule – in this example “failed” – as well as the GateManager Appliance Name and serial number for the Appliance - and the Appliance's current home domain.

The notification.xml file attached contains additional information, including the current status of all "General" parameters. The file is prepared to be imported into e.g. Microsoft Excel (spread sheet) or a management and analysis application.

9.3. Product-specific vs generic alert rules

Alert rules are product-aware. An alert rule can be configured to be generic or to be specific to an Appliance Product.

In a **generic** alert rule, you are limited to a set of so-called general parameters: Configuration Changed, Connected, Disabled, Disconnected, Failed, Last Heartbeat, Unknown. (Not all Appliance Products actually support Configuration Changed because they do not support using the GateManager for configuration backup and restore, or manipulation of configuration profiles - but with time, they may).

In an **appliance product-specific** alert rule there are additional parameters such as IP Address for various interfaces and actions unique to the appliance product.

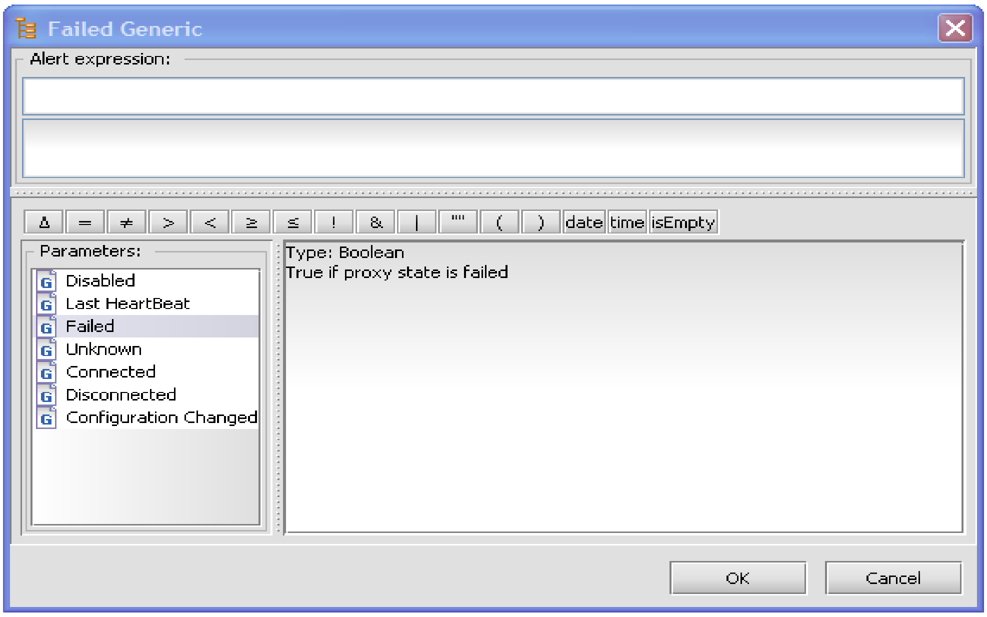
9.4. Create an alert rule

1. In the **Alert Rules View**, select (left-click) the Domain you want to create the rule in.
2. Activate the **Alert Rules** tab and click the shared icon to see what is already available in your domain.
3. If you see a usable rule, go to Attach alert rule to Appliance (see "Attach alert rules to Appliances" page 58). Otherwise click to add a new rule.
4. The **Select Appliance Product** window will pop up. Select either **Generic** or a specific **Appliance Product**. The list of Appliance Products includes only those that are bound to the domain.

   Tip: If you seem to be missing an Appliance Product, follow the instructions here (see "Domain does not have the necessary product binding" page 81).
5. On the **New Alert Rule** dialog, enter a meaningful Alert Name.
6. Click the **Edit** button to start the Alert Rule editor.
7. Create the expression (triggers) for the rule as shown here (see "Alert rule editor: generic rule" page 56).
8. Save changes and close the dialog by clicking **OK**. This returns you to the New Alert Rule dialog.
9. Save changes and close the dialog by clicking **OK**.
10. If you want to share the rule downward in your hierarchy, find the new rule on the Alert Rules tab for the domain, right-click, and then click **Share Alert Rule(s)**.

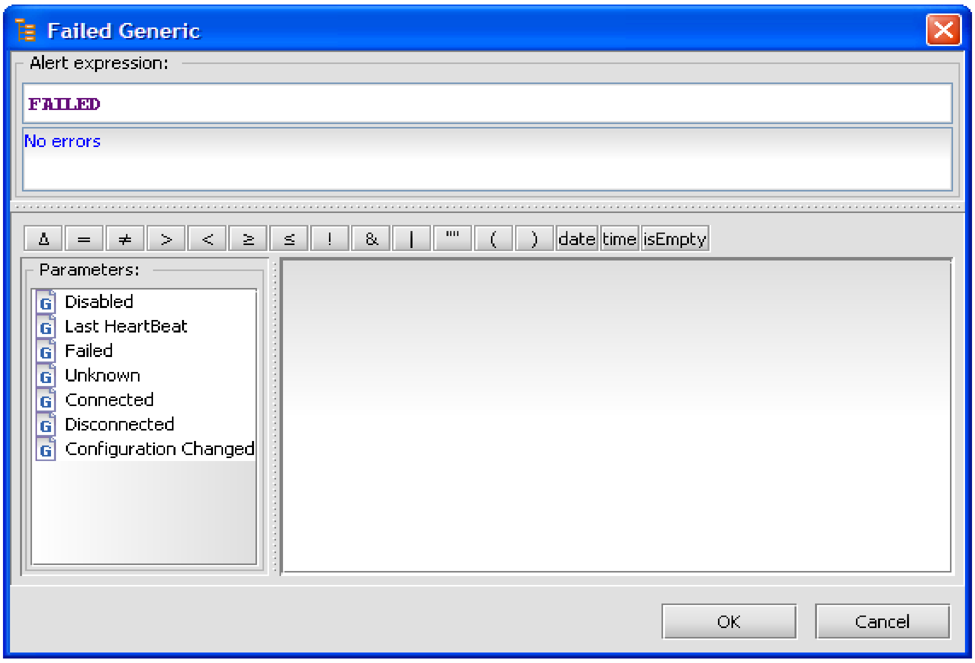
9.4.1. Alert rule editor: generic rule

If you highlight a parameter, such as Failed (as shown here), you will see a description of the **Type**.



Type: Boolean
True if proxy state is failed

If you double-click on the parameter, it will be added to the **Alert expression**.



FAILED

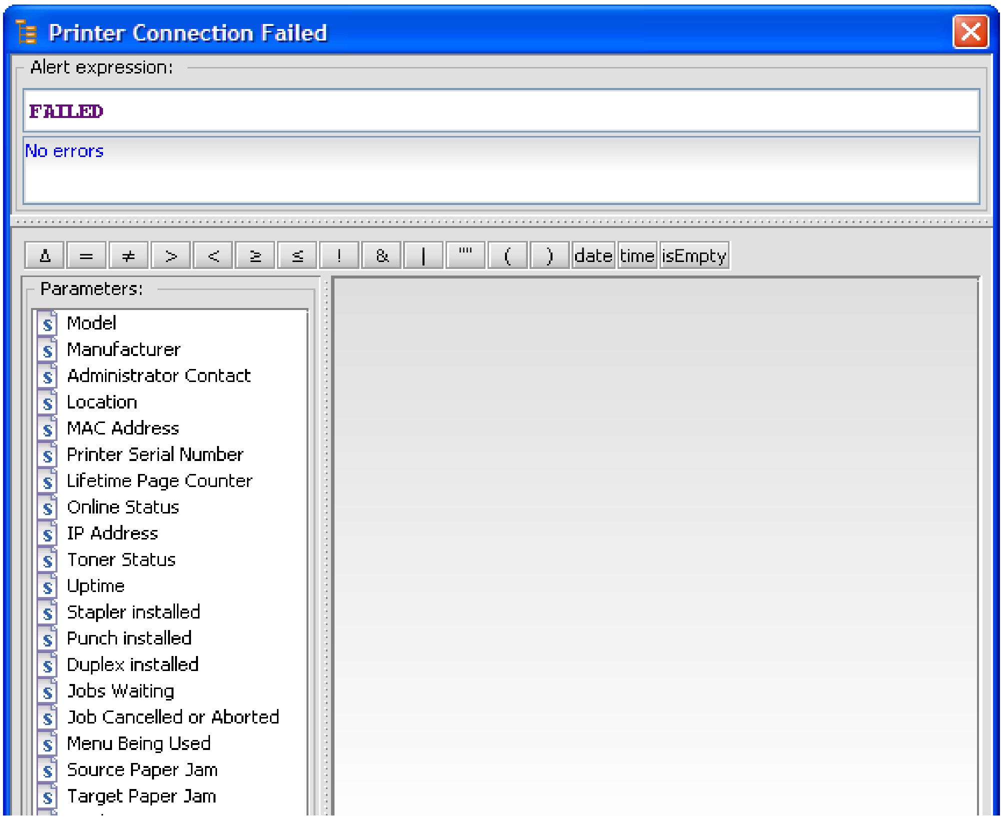
No errors

Save changes and close the dialog by clicking **OK**. This returns you to the New Alert Log dialog.

Save changes and close the dialog by clicking **OK**.

9.4.2. Alert rule editor: appliance product-specific rule

If you don't resize the window, you may need to scroll down the list of parameters to find the one(s) you want. The General parameters are always at the bottom of the list. This screen shot shows a rule applicable to the Printer Agent appliance product.



Printer Connection Failed

Alert expression:

FAILED

No errors

Parameters:

- Model
- Manufacturer
- Administrator Contact
- Location
- MAC Address
- Printer Serial Number
- Lifetime Page Counter
- Online Status
- IP Address
- Toner Status
- Uptime
- Stapler installed
- Punch installed
- Duplex installed
- Jobs Waiting
- Job Cancelled or Aborted
- Menu Being Used
- Source Paper Jam
- Target Paper Jam

9.5. Share / Don't share an alert rule

When you create a rule, by default it is not shared.

Sharing a single rule

1. In the **Alert Rules View** tree, highlight the rule you want to share. An unshared rule displays an bell icon with no hand.
2. Activate the **Details** tab.
3. Click the **Share ...** button. The button text will change to **Don't Share...**. A hand will appear under the bell icon by the Alert Rule name in the tree.

Sharing more than one rule

1. In the **Alert Rules View**, highlight the rules' home domain.
2. Activate the **Alert Rules** tab.
3. On the table in the upper window, select one or more Alert Rules (click in the selection field, far left). You can use this icon to select everything in the list .
4. Do one of the following
   - On the Main Menu, click **Alerts** and then **Share Alert Rules(s)**.
   - Right click any selected table entry to bring up the context menu. Click **Share Alert Rules (s)**.

Share/Don't Share

An unshared role will always display buttons and icons that allow you to share it, and only the **Share** option will be on the menu.

A shared role will always display buttons and icons that allow you to not share it, and only the **Don't Share** option will be on the menu.

If a shared rule is already attached to an Appliance in a child domain, you will not be allowed to select **Don't Share**.

9.6. Attach alert rules to Appliances

During Appliance enrollment, you can - but do not have to - attach alert rules using a wizard. This chapter shows several different approaches attaching Alert Rules to already enrolled and attached Appliances.

When you attach an alert rule and an Appliance to each other, you specify one or more e-mail addresses or Web Service URLs as recipients for the alert about that Appliance.

- **IMPORTANT**:

  Think twice: If you enter more than one recipient email for multiple rules, be sure that you really want all of the recipients to receive all of the alerts.

  What happens when you attach a rule and an Appliance to each other and specify more than one recipient: A separate alert rule is generated for each of them. For example, if you want three people notified if Appliance X fails, the Attached Alert Rules tab for Appliance X will show three alert rules on the table.

9.6.1. Attach Alert Rule(s) - Single Appliance

In the **Appliances View**, highlight the Appliance (left click).

Activate the **Attached Alert Rules** tab.

Click the **Attach Alert Rule** icon.

Two tables are presented on the **Alert Rule Attachment** dialog. The **Appliances** table shows the selected appliance. The **Alert Rules** table shows the rules available to the Appliance's domain.

Select one or more rules and open the attachment dialog.

- For a single rule, double-click the rule or right-click it. Then click **Attach Alert Rule**.
- For multiple rules, select each rule desired (click the selection field far left). You can use this icon to select everything in the list . Right-click on any of the selections. Then click **Attach Alert Rule(s)**.

Type Recipient: Using the pull-down, select **Email** or **WS URL**.

Note: WS URL can only be used if the GateManager is integrated with a backend application *and* the backend application is configured to receive alerts.

Email configuration: Define one or more recipients. You can select among accounts by using the To... button, or you can type in e-mail addresses. Use a comma to separate more than one address. One of the main reasons for typing in the email address of a non-user is to select an e-mail address that can generate SMSs.

WS URL configuration: Type in the exact URL of the web service on the backend application.

Save changes and close the dialog by clicking **OK**.

9.6.2. Attach Alert Rules(s) - Multiple Appliances

1. In the **Appliances View**, highlight the desired domain (left-click).
2. Activate the **Appliances** tab.
3. Select the Appliances you want to work with; click the selection field far left. You can use this icon to select everything in the list .
4. Right-click on any part of the table to bring up the context menu. Click **Attach Alert Rule(s)**.
5. Two tables are presented on the **Alert Rule Attachment** dialog. The **Appliances** table shows the selected Appliances. The **Alert Rules** table shows the rules available to the Appliances' domain.
6. Select one or more rules
7. **Type Recipient**: Using the pull-down, select **Email** or **WS URL**.

   Note: WS URL can only be used if the GateManager is integrated with a backend application *and* the backend application is configured to receive alerts.
8. **Email configuration**: Define one or more recipients. You can select among accounts by using the To... button, or you can type in e-mail addresses. Use a comma to separate more than one address. One of the main reasons for typing in the email address of a non-user is to select an e-mail address that can generate SMSs.

   WS URL configuration: Type in the exact URL of the web service on the backend application.
9. Save changes and close the dialog by clicking **OK**.

9.7. Detach alert rules and Appliances from each other

Detach one or more alert rules from an Appliance

1. In the **Appliances View**, highlight the Appliance (left click).
2. Activate the **Attached Alert Rules** tab.
3. Select one or more rules and open the attachment dialog.
   - For a single rule, double-click the rule or right-click it. Click **Detach Alert Rule**.
   - For multiple rules, set a checkmark for each rule; you can use this icon to select everything in the list . Right-click, then click **Detach Alert Rule**.
4. Save changes and close the dialog by clicking **OK**.

Detach one or more Appliances from an alert rule

1. In the **Alert Rules View**, select (left-click) the rule you want to work with.
2. Activate the **Attached Appliances** tab.
3. Select one or more Appliance and open the detachment dialog.
   - For a single Appliance, right-click it. On the context menu, click **Detach Alert Rule**.
   - For multiple Appliances, select each one desired (click the selection field far left). You can use this icon to select everything in the list . Right-click on any of the selections. Then click **Detach Alert Rule(s)**.
4. Save changes and close the dialog by clicking **OK**.

9.8. Disable, enable, delete alert rule

Disabling, enabling and delteing can only be done in the home domain of the alert rule in question.

- **CAUTION**:

  You will be allowed to delete an alert rule even if it is attached to one or more Appliances.

One alert rule at a time

Right-click on the rule in the **Alert Rules View** tree to bring up the context menu.

More than one alert rule at a time

1. Highlight the appropriate domain (left-click) in the **Alert Rules View** tree.
2. Activate the **Alert Rules** tab.
3. Select the rules you want to work with; click the selection field far left. You can use this icon to select everything in the list ☑.
4. Right-click on any of the selected lines to bring up the context menu.

10. Configuration Backups

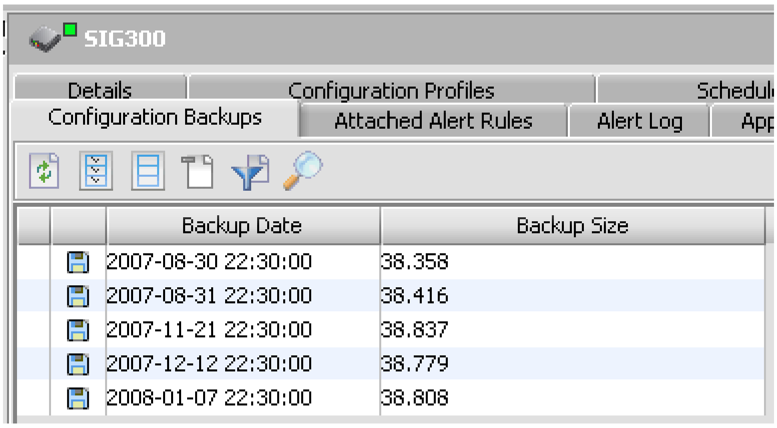
About Configuration Backups

There are two configuration-related concepts in GateManager:

Configuration - which is only used in connection with Configuration Backups - and Configuration Profile, which is often simply called Profile (explained in Configuration Profiles (page 67)).

A **Configuration** is the complete configuration of a physical appliance – including all network settings and hosted agents.

Backups are retained in the GateManager database and can be viewed via the **Configuration Backups** tab for individual Appliances.



	Backup Date	Backup Size
💾	2007-08-30 22:30:00	38.358
💾	2007-08-31 22:30:00	38.416
💾	2007-11-21 22:30:00	38.837
💾	2007-12-12 22:30:00	38.779
💾	2008-01-07 22:30:00	38.808

The maximum number of backups per Appliance is set in the Domain Preferences (see Domain preferences (see "About domain preferences" page 22)). When you reach the maximum, the oldest backup is automatically deleted from the system.

Backups can be used in connection with appliance replacement as explained in Replace a physical appliance (page 47). It is important to make regular backups in order to be prepared if a replacement becomes necessary. This is easily accomplished by scheduling regular backups.

Overview of configuration backup operations

1. Backup a configuration backup manually or by scheduling.
2. Restore a configuration backup to the appliance from which it was taken.
3. View a configuration backup (only in certain Appliance Products, such as the TrustGate, SIG, or SiteManager).
4. Save the configuration backup to a file (only useful in certain Appliance Products).
5. Delete a configuration backup.

10.1. Back up a configuration

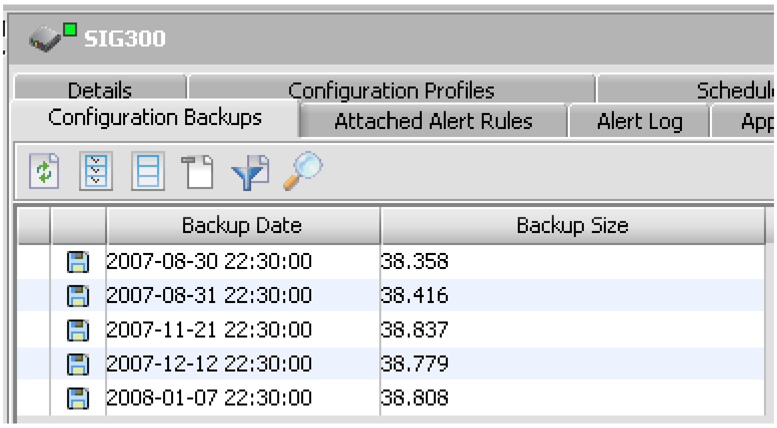
During Appliance enrollment, you can – but do not have to – back up the configuration using a wizard. The following information shows how to manage Backups for already enrolled (Attached) Appliances.

1. From the **Appliances View** tree, do one of the following:
   - Right-click the desired Appliance to bring up the context menu.
   - Highlight the Appliance (left-click) and use the Main Menu's **Appliances** menu.
2. Click the **Command** submenu to open it.
3. Click **Backup Configuration**.
4. The **Backup Configuration** dialog comes up.
5. If you want to delay execution, fill out the bottom part of the dialog; for instructions, see Scheduling Events (Commands) (page 71)
6. Click **OK** to finish and close the screen.

10.2. Restore an individually selected configuration

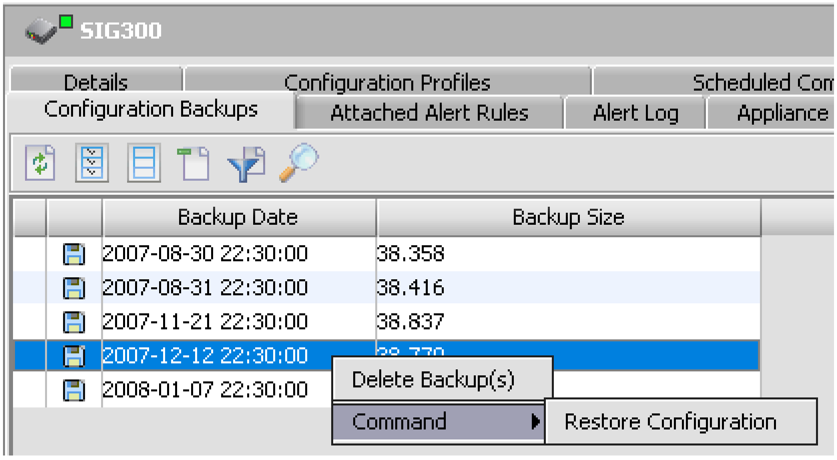
To restore a selected configuration on single appliance

1. Highlight (left-clik) the Appliance's name in the **Appliances View Tree**.
2. Make sure that the **Configuration Backups** tab is activated.



	Backup Date	Backup Size
	2007-08-30 22:30:00	38.358
	2007-08-31 22:30:00	38.416
	2007-11-21 22:30:00	38.837
	2007-12-12 22:30:00	38.779
	2008-01-07 22:30:00	38.808

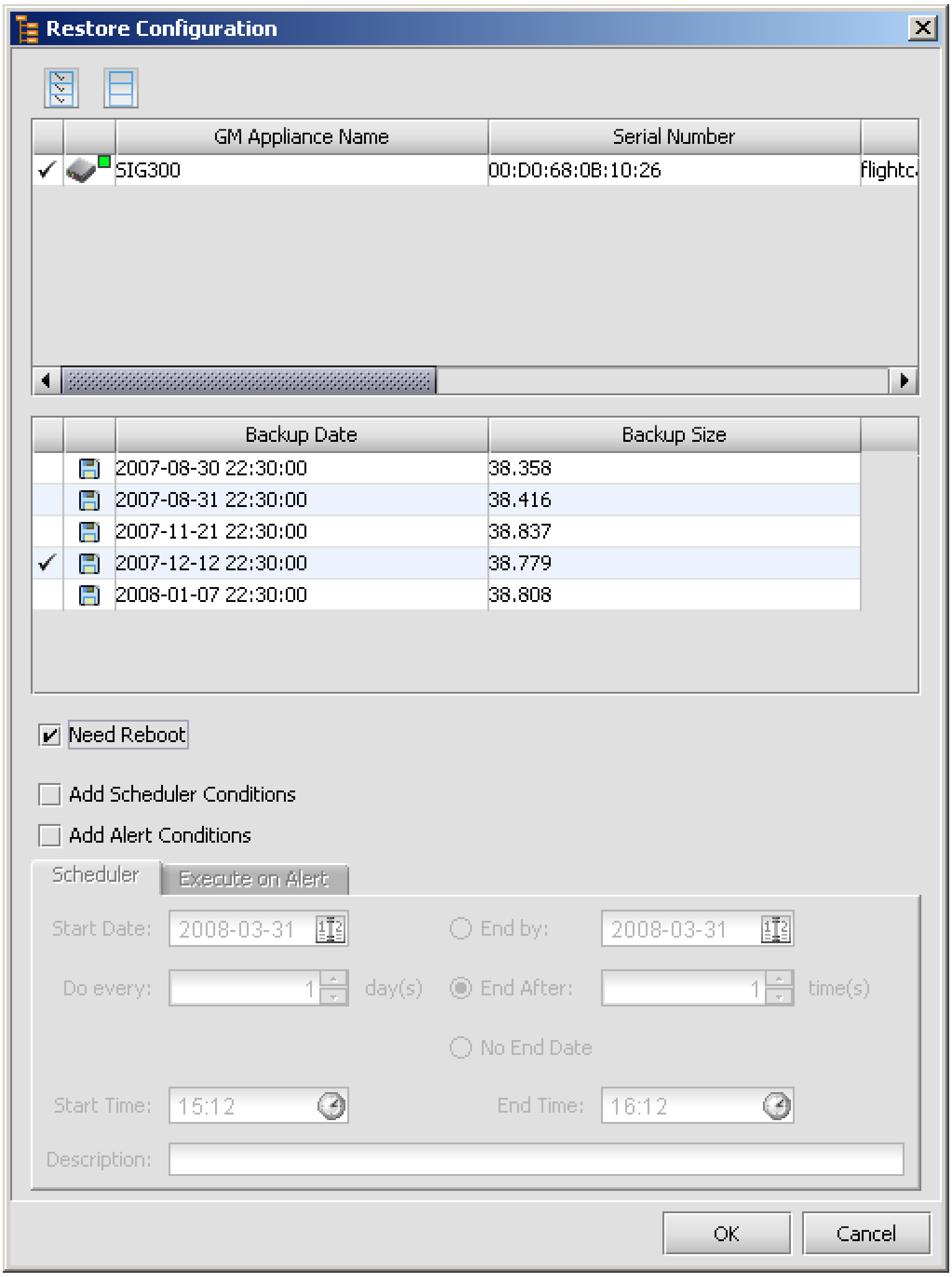
3. Right-click the backup you want restored.
4. This brings up a context menu



	Backup Date	Backup Size
	2007-08-30 22:30:00	38.358
	2007-08-31 22:30:00	38.416
	2007-11-21 22:30:00	38.837
	2007-12-12 22:30:00	38.779
	2008-01-07 22:30:00	

5. Click **Restore Configuration**.

6. This opens a dialog used to confirm and, if desired, adjust your selections on the top part of the dialog.



Restore Configuration

		GM Appliance Name	Serial Number	
✓		SIG300	00:D0:68:0B:10:26	flightc

		Backup Date	Backup Size
		2007-08-30 22:30:00	38.358
		2007-08-31 22:30:00	38.416
		2007-11-21 22:30:00	38.837
✓		2007-12-12 22:30:00	38.779
		2008-01-07 22:30:00	38.808

☑ Need Reboot

□ Add Scheduler Conditions

□ Add Alert Conditions

Scheduler | Execute on Alert

Start Date: 2008-03-31 ○ End by: 2008-03-31

Do every: 1 day(s) ● End After: 1 time(s)

○ No End Date

Start Time: 15:12 End Time: 16:12

Description:

7. On the middle part of the dialog, select the **Need Reboot** box if applicable to the Appliance Product.
   - **TIP**:

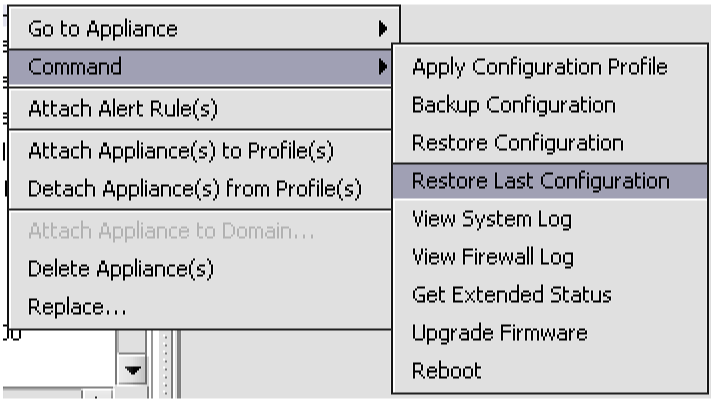
     Because rebooting an appliance in order to activate a configuration change can be disruptive, it can be a good idea to avoid selecting reboot. Instead, schedule a reboot as a command in itself; see Example - Reboot in order to activate a firmware upgrade (page 72).

8. If you want to delay execution of the restoral itself, fill out the bottom part of the dialog; for instructions, see Scheduling Events (Commands) (page 71).

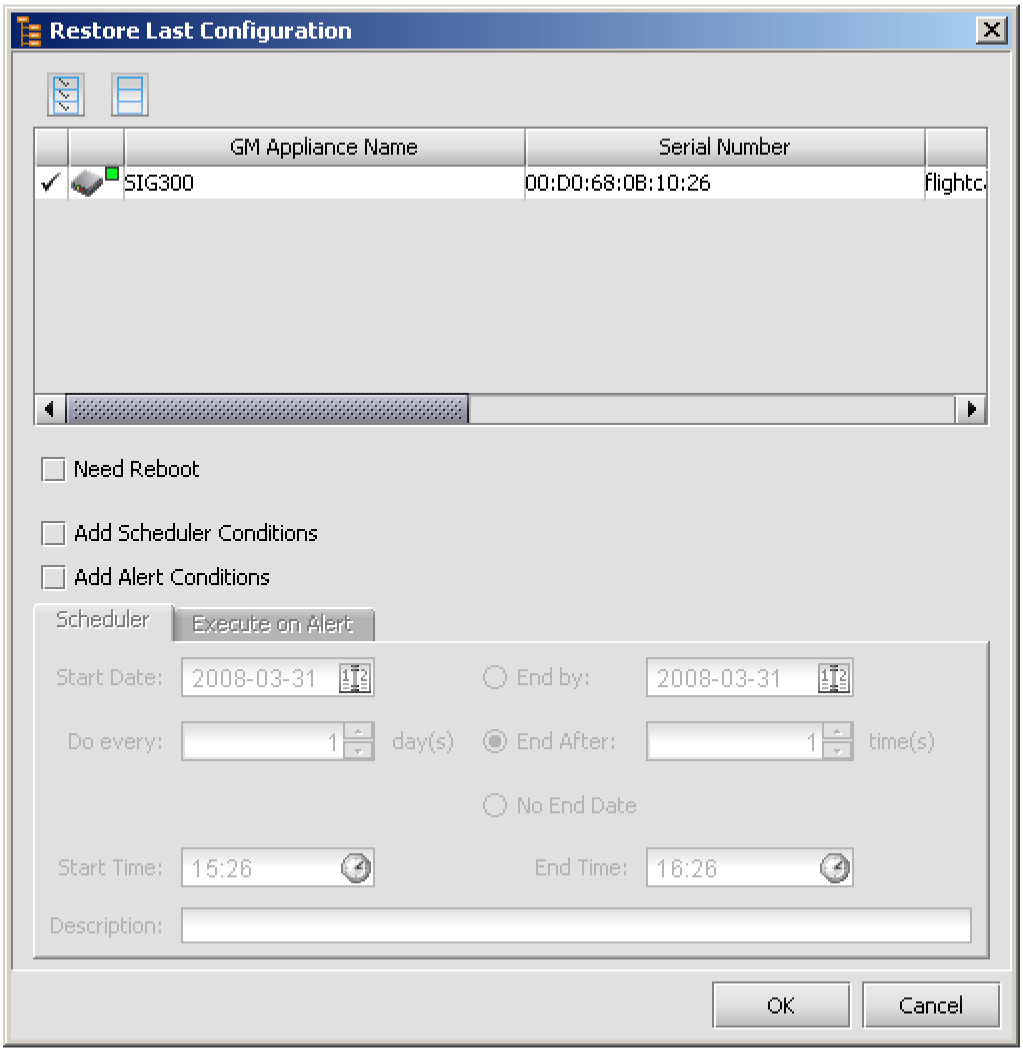
9. Click **OK** to finish and close the dialog.

10.3. Restore last configuration

1. Right-click the Appliance's name in the **Appliances View Tree**.
2. This brings up a context menu.



3. Click **Command** and then **Restore Last Configuration**. Result:


Restore Last Configuration

		GM Appliance Name	Serial Number	
✓		SIG300	00:D0:68:0B:10:26	flightc

□ Need Reboot

□ Add Scheduler Conditions

□ Add Alert Conditions

Start Date: 2008-03-31

○ End by: 2008-03-31

Do every: 1 day(s)

● End After: 1 time(s)

○ No End Date

Start Time: 15:26

End Time: 16:26

Description:

4. Leave the top part of the dialog as it is.
5. On the middle part of the dialog, select the **Need Reboot** box if applicable to the Appliance Product.

- **TIP**:

  Because rebooting an appliance in order to activate a configuration change can be disruptive, it can be a good idea to avoid selecting reboot. Instead, schedule a reboot as a command in itself; see Example - Reboot in order to activate a firmware upgrade (page 72).

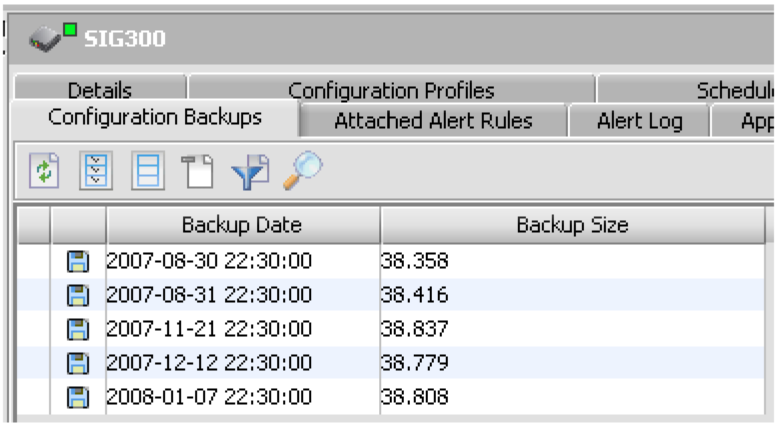
6. If you want to delay execution of the restoral itself, fill out the bottom part of the dialog; for instructions, see Scheduling Events (Commands) (page 71).
7. Click **OK** to finish and close the dialog.

10.4. View the contents of a backup

Not all appliance products have human-readable configurations. Among those that do are the TrustGate family, the SIG families, the SiteManager family, and the PlantManager family.

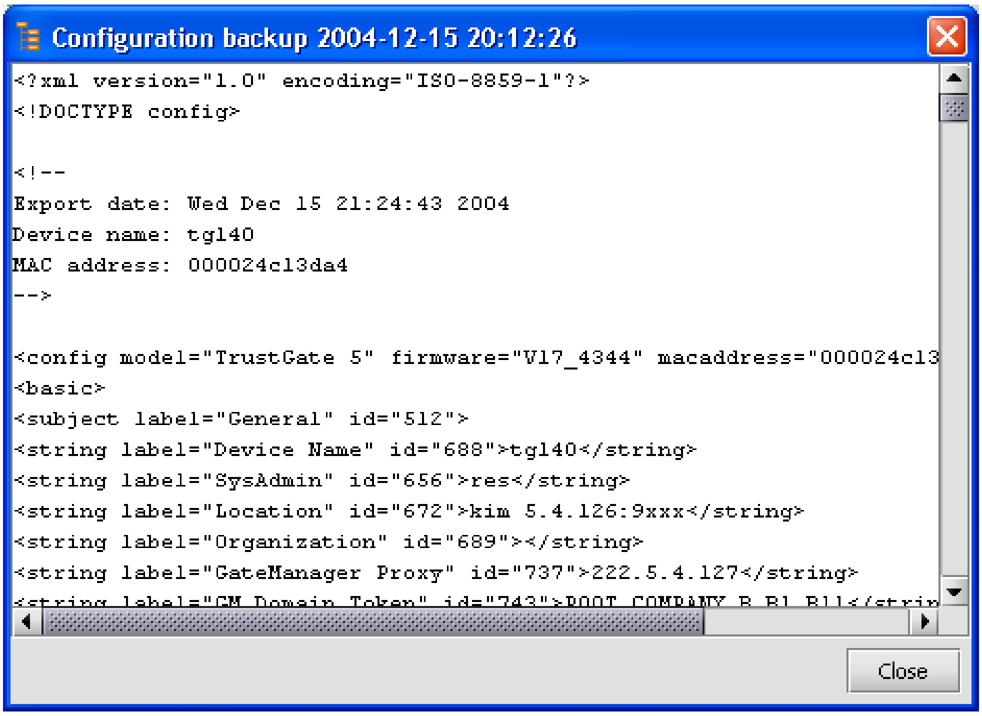
To view the contents of a backup

1. Highlight (left-click) the Appliance's name in the **Appliances View Tree**.
2. Make sure that the **Configuration Backups** tab is activated.



	Backup Date	Backup Size
🖫	2007-08-30 22:30:00	38.358
🖫	2007-08-31 22:30:00	38.416
🖫	2007-11-21 22:30:00	38.837
🖫	2007-12-12 22:30:00	38.779
🖫	2008-01-07 22:30:00	38.808

3. On the table, double-click the backup of interest.
4. Example of a result:



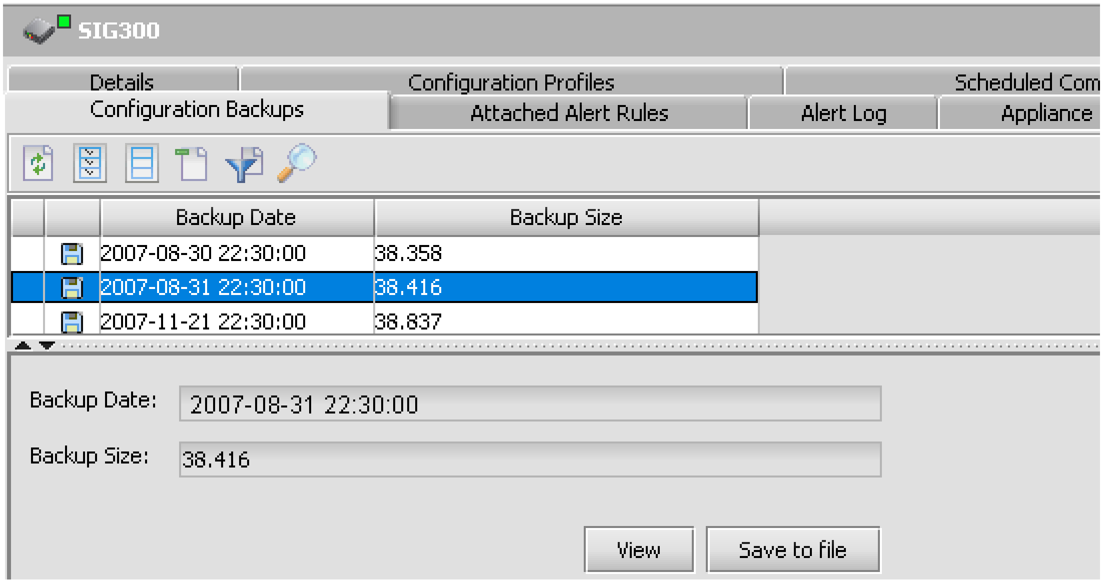
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config>

<!--
Export date: Wed Dec 15 21:24:43 2004
Device name: tgl40
MAC address: 000024cl3da4
-->

<config model="TrustGate 5" firmware="V17_4344" macaddress="000024cl3
<basic>
<subject label="General" id="512">
<string label="Device Name" id="688">tgl40</string>
<string label="SysAdmin" id="656">res</string>
<string label="Location" id="672">kim 5.4.126:9xxx</string>
<string label="Organization" id="689"></string>
<string label="GateManager Proxy" id="737">222.5.4.127</string>
<string label="GM Domain Token" id="743">ROOT COMPANY B B1 B11</strin
```

10.5. Save Configuration Backup to File

Certain GateManager-enabled appliances allow you to load or import a saved file. With a saved file, you can work through an appliance's own interface instead of using GateManager. Remember that a configuration backup includes all parameters; if you don't want IP settings loaded, you need to work with Configuration Profiles.

To save a backup to file

1. Highlight (left-click) the Appliance's name in the **Appliances View Tree**.
2. Make sure that the **Configuration Backups** tab is activated.
3. Highlight (left-click) the desired profile. You may have to adjust the divider between the two windows, so the result looks something like this:



		Backup Date	Backup Size
	🖫	2007-08-30 22:30:00	38.358
	🖫	2007-08-31 22:30:00	38.416
	🖫	2007-11-21 22:30:00	38.837

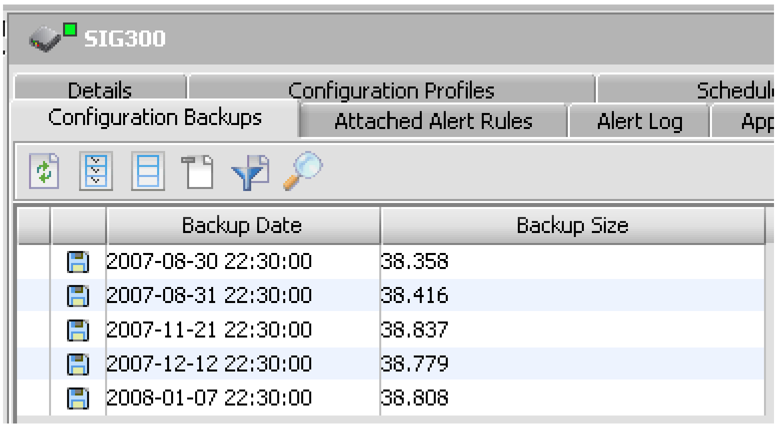
Backup Date: 2007-08-31 22:30:00

Backup Size: 38.416

4. Click the **Save to file** button.
5. A **Save ... as** dialog opens so you can select a placement for the file and, if desired, adjust the name of the file.

10.6. Delete one or more configuration backups

1. Highlight (left-click) the Appliance's name in the **Appliances View Tree**.
2. Make sure that the **Configuration Backups** tab is activated.



		Backup Date	Backup Size
	🖫	2007-08-30 22:30:00	38.358
	🖫	2007-08-31 22:30:00	38.416
	🖫	2007-11-21 22:30:00	38.837
	🖫	2007-12-12 22:30:00	38.779
	🖫	2008-01-07 22:30:00	38.808

3. Select one or more backups by clicking each in the selection field (far left).
4. Right-click on any of the selected entries.
5. This brings up a context menu. Click **Delete Backup(s)**.

11. Configuration Profiles

About Configuration Profiles

There are two configuration-related concepts in GateManager:

Configuration Profile and Configuration - which is only used in connection with Configuration Backups (see Backup configuration (see "Back up a configuration" page 62)).

A **Configuration Profile** is a subset of a configuration. It is typically used to push a partial configuration to many physical appliances. The profile can, if desired, include the complete contents of a configuration; and this can be useful with some appliance products. However, this is an exception to the rule, and it is not covered in this guide.

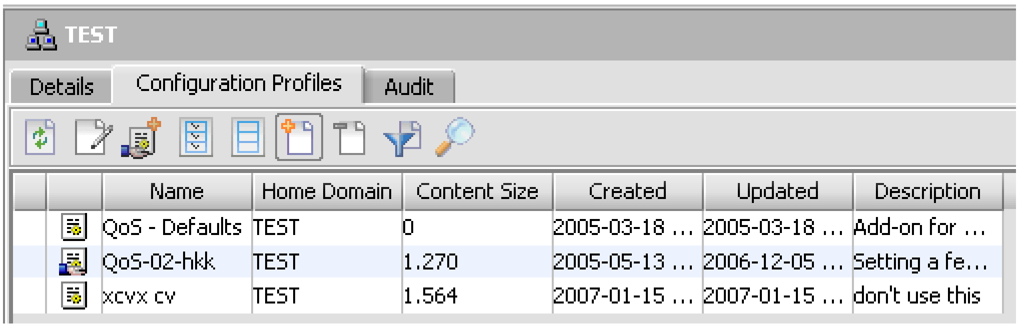
Overview of configuration profile operations

1. **Add Profile**. A configuration profile is added to a domain. You create the contents of the profile either by uploading a file or by typing into the internal editor. The editor can only be used for very small profiles to be used on appliances that accept configurations in a plain text format.
2. **Share Profile**. If you want to be able use a profile in child domains, you must first share the profile. The principles of sharing are the same that are used in sharing alert rules.
3. **Attach To Configuration Profile** (from a selected Appliance), and **Attach Profile to Appliance** (from a selected Profile).

   You need to associate an Appliance and a profile with each other ("Attach") before you actually apply the profile. Attaching Appliances to Profiles and Attaching Profiles to Appliances work in slightly different ways. This guide only describes attaching profiles to appliances, which is the most common way of working.
4. **Command: Apply Configuration Profile**. When you apply a profile, it is loaded into the physical appliance. If a parameter is already configured in the appliance, the configuration will be over-written when the profile is loaded. Otherwise, the configurations in the profile are simply added to those already in the physical appliance.
5. **Detach ….** This facility is provided to clean up in your lists of attached profiles on an Appliance.
6. **Edit Profile**. An editable profile can only be edited in its home domain. If you update a configuration profile, you will be asked by the system if you want it applied to the Appliances attached to it.
7. **Delete Profile**. A profile can be deleted in the domain where it was added (its home domain). You will not be allowed to delete a profile if it is attached to one or more Appliances.

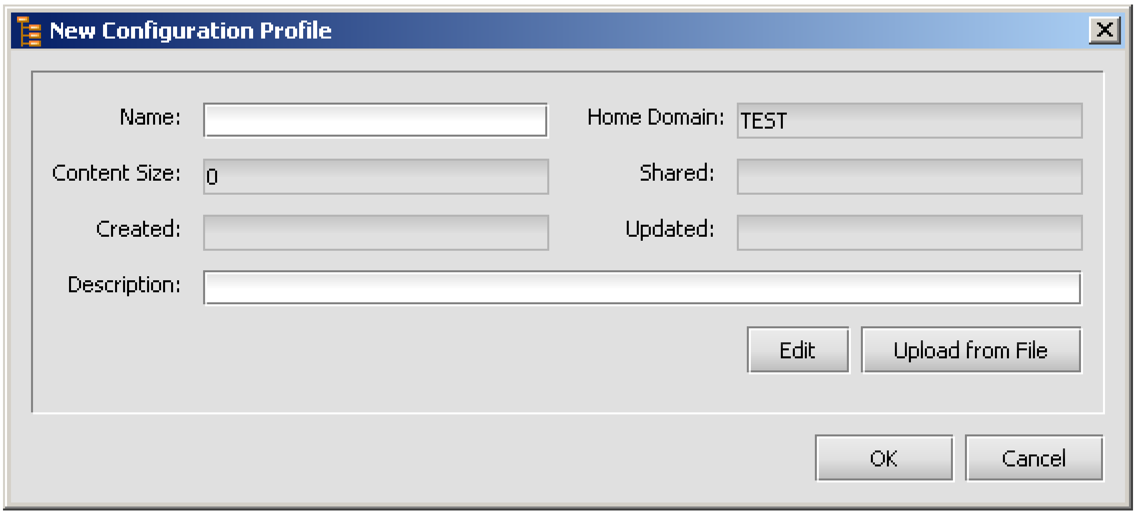
11.1. Add a profile to a domain

1. In the **Configuration Profiles View**, highlight (left-click) the domain you want to create the profile in.
2. Make sure that the **Configuration Profiles Tab** is activated.
3. Click the Show Shared Profiles button to be sure that all available profiles are shown.



	Name	Home Domain	Content Size	Created	Updated	Description
	QoS - Defaults	TEST	0	2005-03-18 …	2005-03-18 …	Add-on for …
	QoS-02-hkk	TEST	1.270	2005-05-13 …	2006-12-05 …	Setting a fe…
	xcvx cv	TEST	1.564	2007-01-15 …	2007-01-15 …	don't use this

4. Click the Add button on the tab tool bar.
5. This starts the **New Configuration Profile** dialog.



New Configuration Profile

Name:

Home Domain: TEST

Content Size: 0

Shared:

Created:

Updated:

Description:

Field information

- Name is mandatory and should be filled in first.
- Description is optional, but highly recommended.
- Content Size will be displayed by the system after you have entered conted by editing or uploading.
- Created and Updated will only be shown after you save the text with OK.

6. Select either Upload from File or Edit.

Upload from File:

- Click the button
- Browse on your network to where the file is
- Click OK or double click the file name.
  The file name does not have to match the name you typed in the dialog.
- The New Configuration Profile dialog re-appears.
- Click OK (do not click Upload from File a second time).

Edit:

- Click the button.
- A small internal editor opens.
- Type or paste/insert the text
- Exit the editor and save the text by clicking OK.
- The New Configuration Profile dialog re-appears.
- Click OK.

11.2. Share one or more profiles

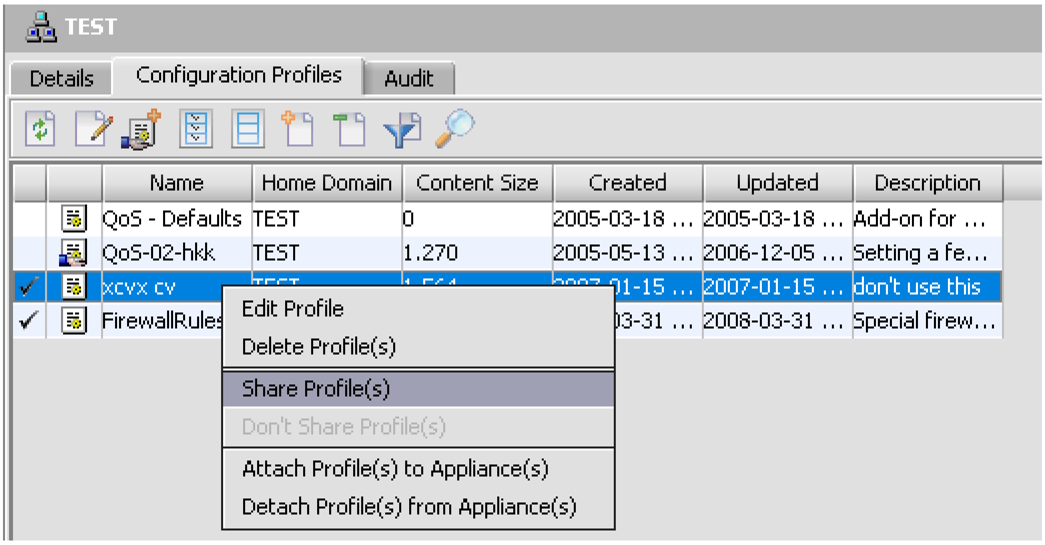
When you add a profile, by default it is not shared.

Sharing a single profile

1. In the **Configuration Profiles View** tree, right-click the profile you want to share. An unshared profile displays a profile icon with no hand.
2. The result is a context menu.
3. Click **Share Profile**.
4. Activate the **Details** tab.
5. Click the **Share ...** button. The button text will change to **Don't Share...**. A hand will appear under the bell icon by the Alert Rule name in the tree.

Sharing more than profile

1. In the **Configuration Profiles View** tree, highlight the profiles' home domain.
2. Activate the **Configuration Profiles** tab.
3. On the table in the upper window, select one or more profiles (click in the selection field, far left). You can use this icon to select everything in the list .



		Name	Home Domain	Content Size	Created	Updated	Description
		QoS - Defaults	TEST	0	2005-03-18 ...	2005-03-18 ...	Add-on for ...
		QoS-02-hkk	TEST	1.270	2005-05-13 ...	2006-12-05 ...	Setting a fe...
✓		xcvx cv	TEST	1.564	2007-01-15 ...	2007-01-15 ...	don't use this
✓		FirewallRules			3-31 ...	2008-03-31 ...	Special firew...

4. Do one of the following
   - On the Main Menu, click **Profiles** and then **Share Profile(s)**.
   - Right click any selected table entry to bring up the context menu. Click **Share Profile(s)**.

If a profile is already shared, the menus will activate Don't Share Profile(s) while greying out Share Profile(s).

11.3. Attach a profile (or several profiles) to one or more Appliances

Attachment does nothing to the physical appliance. It just prepares relationships that can be used for actually pushing profiles to appliances. So it is easy to attach multiple profiles to multiple Appliances, as long as all of them are in - or available to - the same domain.

1. In the **Configuration Profiles View** tree, navigate to the home domain of the Appliances you want to attach the profile to.
2. Activate the **Configuration Profiles** tab.
3. Click the Show Shared Profiles button to be sure that you can see everything that is available.
4. On the table, right-click the profile you want to attach.
5. This opens a context menu.
6. Click **Attach Profile(s) to Appliance(s)**.
7. This opens a dialog.
8. The top part of the dialog lists Appliances in the domain. Select at least one by clicking in the selection field(s) (far left).
9. The bottom part of the dialog lists all the available profiles in the domain - not just the one already selected. You can adjust your selection.
10. Click **OK** to save settings and exit the dialog.

11.4. Apply a profile to one or more appliances

Applying a profile pushes it to one or more appliances. Therefore, you should only work with one profile at a time. Before applying a profile it must be associated (by attachment) to the appliance(s); see Attach a profile (or several profiles) to one or more Appliances (page 70)

1. Being that a shared profile will appear in all domains it is available to, start by navigating in the **Configuration Profiles View** tree to the home domain of the Appliances you want to attach the profile to. Then hghlight the desired profile (left-click).
2. Activate the **Attached Appliances** tab.
3. Select the Appliances (click in the selection field, far left) on the table.
4. Right-click on any of the selections in the table.
5. This brings up a context menu.
6. On the context menu click **Command**, and then **Apply Configuration Profile**. Follow the instructions.

Tip: If you need to see which appliances have had a profile pushed to them, look at the Audit tab for the profile.

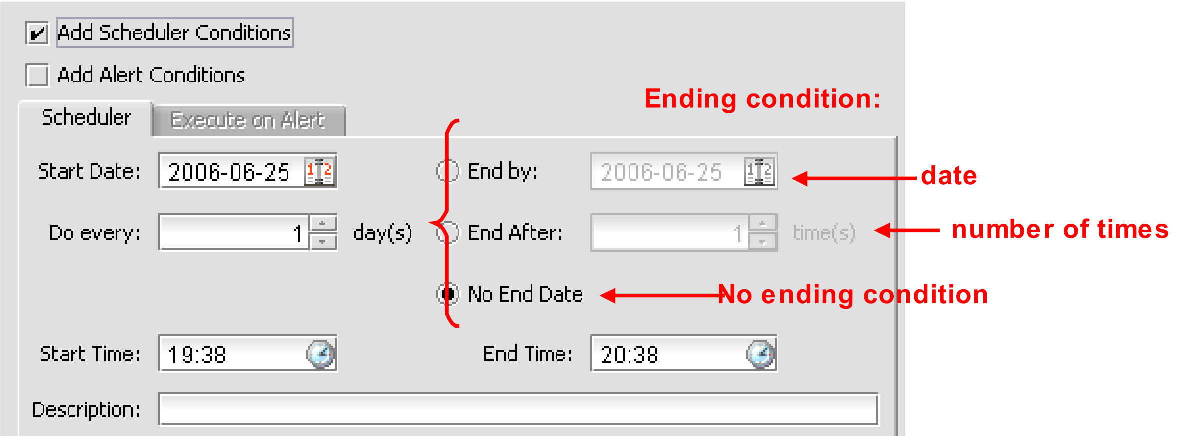
12. Scheduling Events (Commands)

You can schedule Reboot Appliance, Upgrade Firmware, Backup Configuration, Restore (Last) Configuration Backup, and Apply Configuration Profile. These events are all Appliance Commands.

Whenever you schedule a command, you must fill out the conditions on the bottom of the dialog. There are two types of scheduling conditions: time-based and alert-triggered. You can choose one or the other (the GUI should show radio buttons instead of checkboxes.)

12.1. Time-based scheduling

When you select **Add Scheduler Conditions**, the time-based scheduling parameters become accessible for setting.



☑ Add Scheduler Conditions

☐ Add Alert Conditions

Start Date: 2006-06-25

Do every: 1 day(s)

○ End by: 2006-06-25

○ End After: 1 time(s)

● No End Date

Start Time: 19:38

End Time: 20:38

Description:

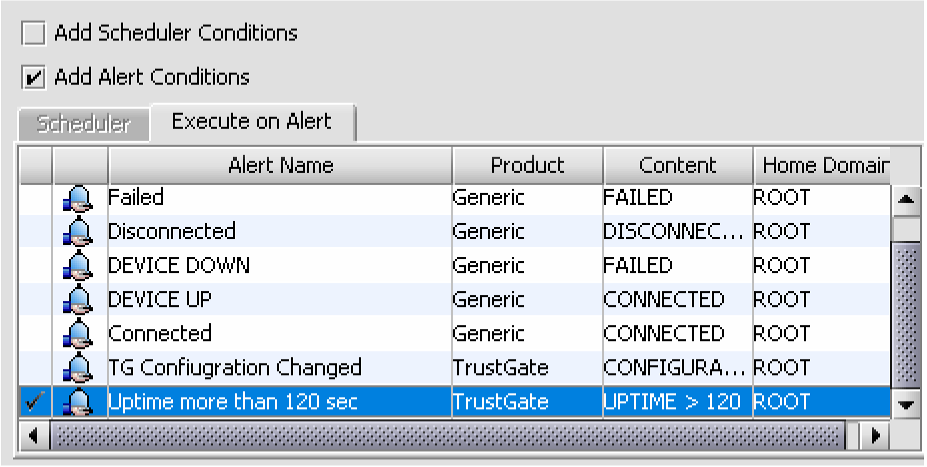
Start Time and **End Time**: Taken together, these values define the interval within which the system will attempt to perform the scheduled command. Both fields are mandatory. Choose a realistic interval, for example minimum one hour.

To configure date and time fields, use one of these two methods:

- Types values directly in the field / each defined part of a field.
- Use the buttons. This one 📅 opens a calendar- and this one 🕘 opens a dropdown list of times (quarter-hours from 00:00 to and including 23:45).

12.2. Alert-triggered scheduling

When you select **Add Alert Conditions**, you will be presented with a list of alert rules available in the domain. Select one, and only one, Alert Rule, as shown in this example.



☐ Add Scheduler Conditions

☑ Add Alert Conditions

	Alert Name	Product	Content	Home Domair
	Failed	Generic	FAILED	ROOT
	Disconnected	Generic	DISCONNEC...	ROOT
	DEVICE DOWN	Generic	FAILED	ROOT
	DEVICE UP	Generic	CONNECTED	ROOT
	Connected	Generic	CONNECTED	ROOT
	TG Confiugration Changed	TrustGate	CONFIGURA...	ROOT
✓	Uptime more than 120 sec	TrustGate	UPTIME > 120	ROOT

This selection will temporarily attach the rule to the Appliance - this will not be visible on the Attached Alert Rules tab, but it *will* be visible on the **Scheduled Commands** tab for the individual Appliance   When the Command has been triggered and carried out, the Scheduled Command disappears from the list.

12.3. Example - Reboot in order to activate a firmware upgrade

Imagine that you have done firmware upgrade– here and now – on several TrustGates. In order for the upgrade to take effect, the TrustGates need to be rebooted. But if you select **Needs reboot**, all of the reboots will happen more or less at once – and possibly at a very inconvenient time for users. So, instead of simply selecting Needs reboot, you schedule the reboots. Iin this example, a *pair* of scheduled commands is used.

Time-based:

The basic command is to Reboot at a particular time, say around midnight, once and only once. To schedule this, configure a **Start Date and time**. Use **End After 1 time** as the ending condition.

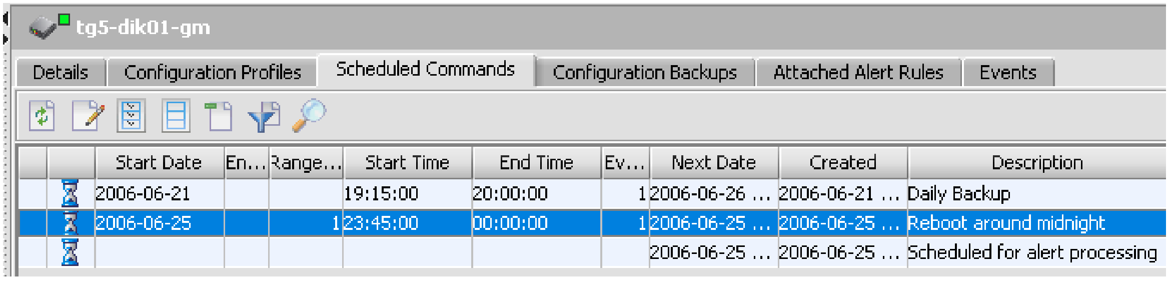
This will update all appliances that are not turned off at the time of the Reboot.

Alert-triggered:

Some appliances may be turned off when the time-triggered command is carried out. In order to be sure that the Reboot is carried out, you want to catch these appliances the next time they are turned on. You want this to happen quickly in order to minimize user disturbances, but also need to wait a bit to be sure that all the connections are in order. To schedule this, make sure there is an appropriate alert rule available in the domain that is triggered on **Uptime more than 120 sec**. An example of this is shown in Alert-triggered scheduling (page 71).

Scheduling an additional alert-triggered command:

In this kind of situation, you may *also* want to create an **Upgrade Firmware** schedule triggered on **Uptime more than ...**, just using a shorter interval for the **Upgrade Firmware** than for the **Reboot**.



		Start Date	En...	Range...	Start Time	End Time	Ev...	Next Date	Created	Description
	⌛	2006-06-21			19:15:00	20:00:00	1	2006-06-26 ...	2006-06-21 ...	Daily Backup
	⌛	2006-06-25		1	23:45:00	00:00:00	1	2006-06-25 ...	2006-06-25 ...	Reboot around midnight
	⌛							2006-06-25 ...	2006-06-25 ...	Scheduled for alert processing

12.4. See scheduled commands

See scheduled commands for a given Appliance

Highlight (left-click) an Appliance in the **Appliances View** tree. Activate the **Scheduled Commands** tab.

See commands (events) scheduled by a given user

Highlight (left-click) an Account in the **Accounts View** tree. Activate the **Scheduled Events** tab.

13. Appliance Product and Plugin Management

13.1. Plugins: general information

13.1.1. What plugins are and what they do

The plugin is a file with the extension `.jar`.

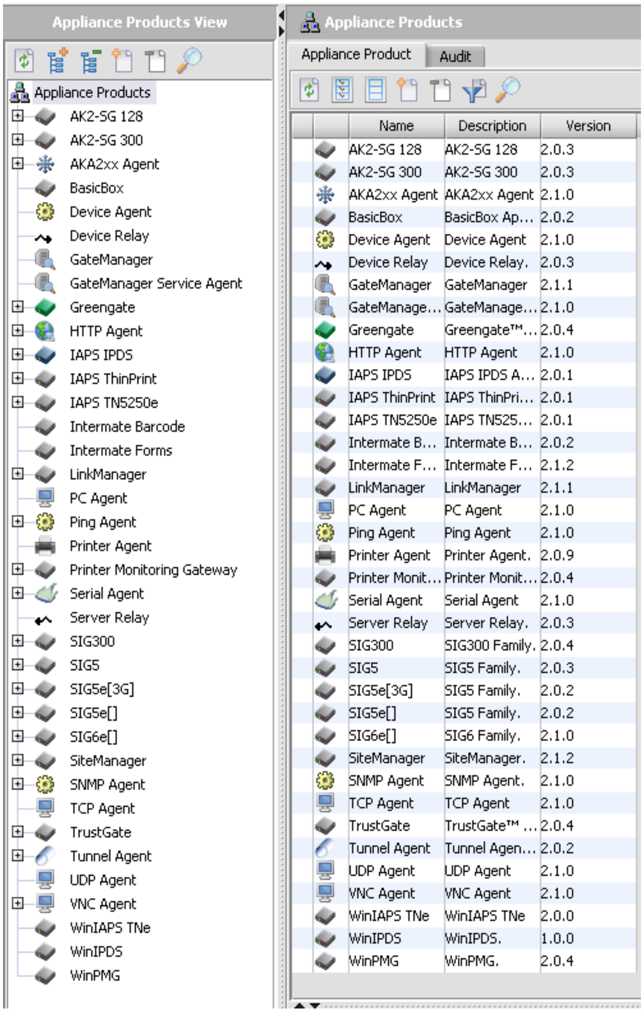
Each plugin creates support for one Appliance Product (type of Appliance).

When a plugin is installed, a folder is created in the **Appliance Products View**. The GateManager can then accept Appliance enrollments for that particular Appliance Product.

If you select an Appliance Product in the tree, the information pane will show two tabs: **Details** and **Appliances**. The Appliances tab lists all enrolled Appliances of that particular type.

This screenshot shows an example of what the Appliance Products View looks like with many different plugins.

This is an example of what the **Appliance Products View** looks like with many different plugins. The + shows that there are already firmware files in the folder created by the plugin.



Appliance Products View

Appliance Products
- ⊞ AK2-SG 128
- ⊞ AK2-SG 300
- ⊞ AKA2xx Agent
- BasicBox
- Device Agent
- Device Relay
- GateManager
- GateManager Service Agent
- ⊞ Greengate
- ⊞ HTTP Agent
- ⊞ IAPS IPDS
- ⊞ IAPS ThinPrint
- ⊞ IAPS TN5250e
- Intermate Barcode
- Intermate Forms
- ⊞ LinkManager
- PC Agent
- ⊞ Ping Agent
- Printer Agent
- ⊞ Printer Monitoring Gateway
- ⊞ Serial Agent
- Server Relay
- ⊞ SIG300
- ⊞ SIG5
- ⊞ SIG5e[3G]
- ⊞ SIG5e[]
- ⊞ SIG6e[]
- ⊞ SiteManager
- ⊞ SNMP Agent
- TCP Agent
- ⊞ TrustGate
- ⊞ Tunnel Agent
- UDP Agent
- ⊞ VNC Agent
- WinIAPS TNe
- WinIPDS
- WinPMG

Appliance Products

Name	Description	Version
AK2-SG 128	AK2-SG 128	2.0.3
AK2-SG 300	AK2-SG 300	2.0.3
AKA2xx Agent	AKA2xx Agent	2.1.0
BasicBox	BasicBox Ap...	2.0.2
Device Agent	Device Agent	2.1.0
Device Relay	Device Relay.	2.0.3
GateManager	GateManager	2.1.1
GateManage...	GateManage...	2.1.0
Greengate	Greengate™...	2.0.4
HTTP Agent	HTTP Agent	2.1.0
IAPS IPDS	IAPS IPDS A...	2.0.1
IAPS ThinPrint	IAPS ThinPri...	2.0.1
IAPS TN5250e	IAPS TN525...	2.0.1
Intermate B...	Intermate B...	2.0.2
Intermate F...	Intermate F...	2.1.2
LinkManager	LinkManager	2.1.1
PC Agent	PC Agent	2.1.0
Ping Agent	Ping Agent	2.1.0
Printer Agent	Printer Agent.	2.0.9
Printer Monit...	Printer Monit...	2.0.4
Serial Agent	Serial Agent	2.1.0
Server Relay	Server Relay.	2.0.3
SIG300	SIG300 Family.	2.0.4
SIG5	SIG5 Family.	2.0.3
SIG5e[3G]	SIG5 Family.	2.0.2
SIG5e[]	SIG5 Family.	2.0.2
SIG6e[]	SIG6 Family.	2.1.0
SiteManager	SiteManager.	2.1.2
SNMP Agent	SNMP Agent.	2.1.0
TCP Agent	TCP Agent	2.1.0
TrustGate	TrustGate™ ...	2.0.4
Tunnel Agent	Tunnel Agen...	2.0.2
UDP Agent	UDP Agent	2.1.0
VNC Agent	VNC Agent	2.1.0
WinIAPS TNe	WinIAPS TNe	2.0.0
WinIPDS	WinIPDS.	1.0.0
WinPMG	WinPMG.	2.0.4

If you select an Appliance Product in the tree, the information pane will show two tabs: **Details** and **Appliances**. The Appliances tab lists all enrolled Appliances of that particular type.

Each Appliance Product folder can be used for storing firmware files. The + shows that there are already firmware files in the folder created by the plugin.

13.1.2. Initial plugin installation

On a freshly installed GateManager, the relevant `.jar` files must be installed manually from the GateManager CD (see "Manual .jar file installation" page 74).

Plugins should only be installed by a ROOT-level user with the **Manager** role. In order to keep an installation simple, you should only install plugins for the Appliances (products, agents, etc) that you use in your solution; guidelines are given in Which plugins are needed for a given solution? (page Error: Reference source not found)

13.1.3. Updated plugins

The CD for each release of GateManager includes a full set of plugins that are compatible with that release. Any time the GateManager is updated, already installed plugins will be updated.

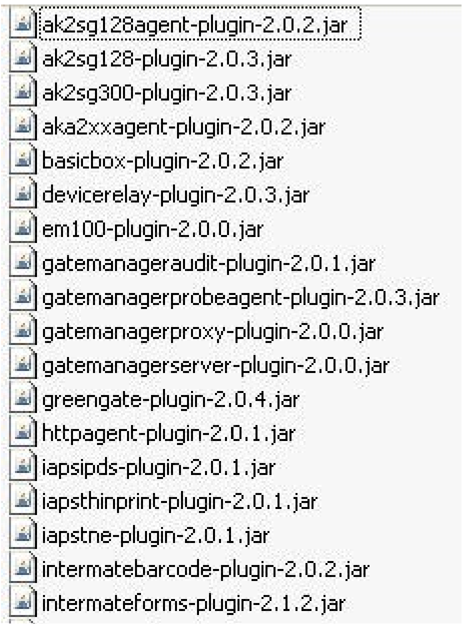
Updated plugins over-write earlier versions.

The name of an appliance product may change over time. The GateManager server only recognizes the plugin by its unique identifier (which is hidden) and its version number (which you can see on the Console). Name changes do not affect functionality.

Information about versions and name changes is provided in release notes for the GateManager release or in notes about releases of plugins between GateManager releases.

13.2. Manual .jar file installation

1. Select the **Appliance Products View**.
2. Click the **Add plug-in** button in the tool bar.
3. This opens an **Upload Appliance Product** dialog.
4. **Look In**: Use the drop-down list to navigate to the plugins folder on the GateManager CD (or to a drive where you have saved plugins, e.g. when they are released in between GateManager updates). The list looks something like this:



ak2sg128agent-plugin-2.0.2.jar
ak2sg128-plugin-2.0.3.jar
ak2sg300-plugin-2.0.3.jar
aka2xxagent-plugin-2.0.2.jar
basicbox-plugin-2.0.2.jar
devicerelay-plugin-2.0.3.jar
em100-plugin-2.0.0.jar
gatemanageraudit-plugin-2.0.1.jar
gatemanagerprobeagent-plugin-2.0.3.jar
gatemanagerproxy-plugin-2.0.0.jar
gatemanagerserver-plugin-2.0.0.jar
greengate-plugin-2.0.4.jar
httpagent-plugin-2.0.1.jar
iapsipds-plugin-2.0.1.jar
iapsthinprint-plugin-2.0.1.jar
iapstne-plugin-2.0.1.jar
intermatebarcode-plugin-2.0.2.jar
intermateforms-plugin-2.1.2.jar

5. Select .jar files you need (for information about which plugins are needed for various solutions, see Which plugins are needed for a given solution? (page Error: Reference source not found)). The dialog allows you to select more than one plugin at a time for installation.
6. Click the **Open** button. A message box will ask you to confirm the action for any plugin that has already been installed.

Handling domain-plugin bindings

If this is the first time the plugin is being added to the GateManager, you must create a product binding for it in the **ROOT** domain as explained in ROOT domain Product Bindings .

Any domain created after a plugin is installed will automatically receive the binding, which you can remove if the appliance product is not relevant for that domain.

Any domain created before a plugin is installed for the first time must be manually given a product binding if you want the product available to users of that domain. If a product is not available on a list, it has not been made available on the parent domain.

14. Firmware management

14.1. Recommended procedures

Firmware files are stored on the GateManager for two purposes:

- updating firmware in managed Appliances from the GateManager respository
- being able to find which Appliances are running any given firmware version

So, the Server Owner should make sure that any firmware running on an enrolled Appliance is kept in the **Appliance Products** repository, even if you do not foresee a need to use the firmware file for updates of managed Appliances.

The person responsible for adding firmware files should always inform other users about which firmware files have been made available for the appliance products they use.

If you expand the **Appliance Products** folder, you will see all of the firmware files in the repository for that particular type of Appliance.

14.2. How to add a firmware file to the repository

1. Select the **Appliance Products View**.
2. Right-click the desired folder.
3. Click **Add Firmware** .
4. In the **Add firmware** dialog, enter information about the **Revision**.
   - **IMPORTANT**

     The revision field is free text, and is not inspected by the Appliance. However, if you want to be able to see which appliances are running any particular firmware revision, you should follow the instructions in Revision field when adding a firmware file (see "About the revision field when adding a firmware file" page 76).
5. Enter a **Description**. This is particularly important if the product is one that has Upgrade and Setup variants, because both variants are identified with the same Revision field text.
6. Click **Upload from File**.
7. In the **Upload Firmware** dialog, browse to where you have the firmware and highlight the desired file.
8. Click **OK**. This will close the dialog, return you to the **Add firmware** dialog and insert the file's name in the **File name** field.
9. Save changes and close the dialog by clicking **OK**.

14.3. About the revision field when adding a firmware file

The firmware information that you see in the an appliance's own configuration information or GUI does not show the special prefix (such as **oper:** or **agent:** or **base:** or **bios:**) that is used in the **Firmware** field reported by the Appliance in GateManager. For most firmware releases after June 2006, the release notes for the product tell you the prefix to use.

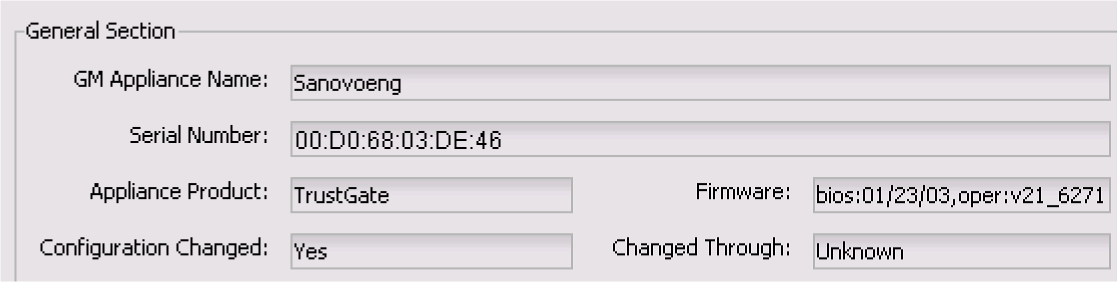
How to find the correct revision description if you cannot find the prefix in a release note or on a product support portal:

1. Locate an enrolled Appliance that uses the same type firmware.
2. Look at the **General Section**, **Firmware** field.

   This example shows two firmware files in the selected Appliance:

bios:01/23/03

oper:v21_6271



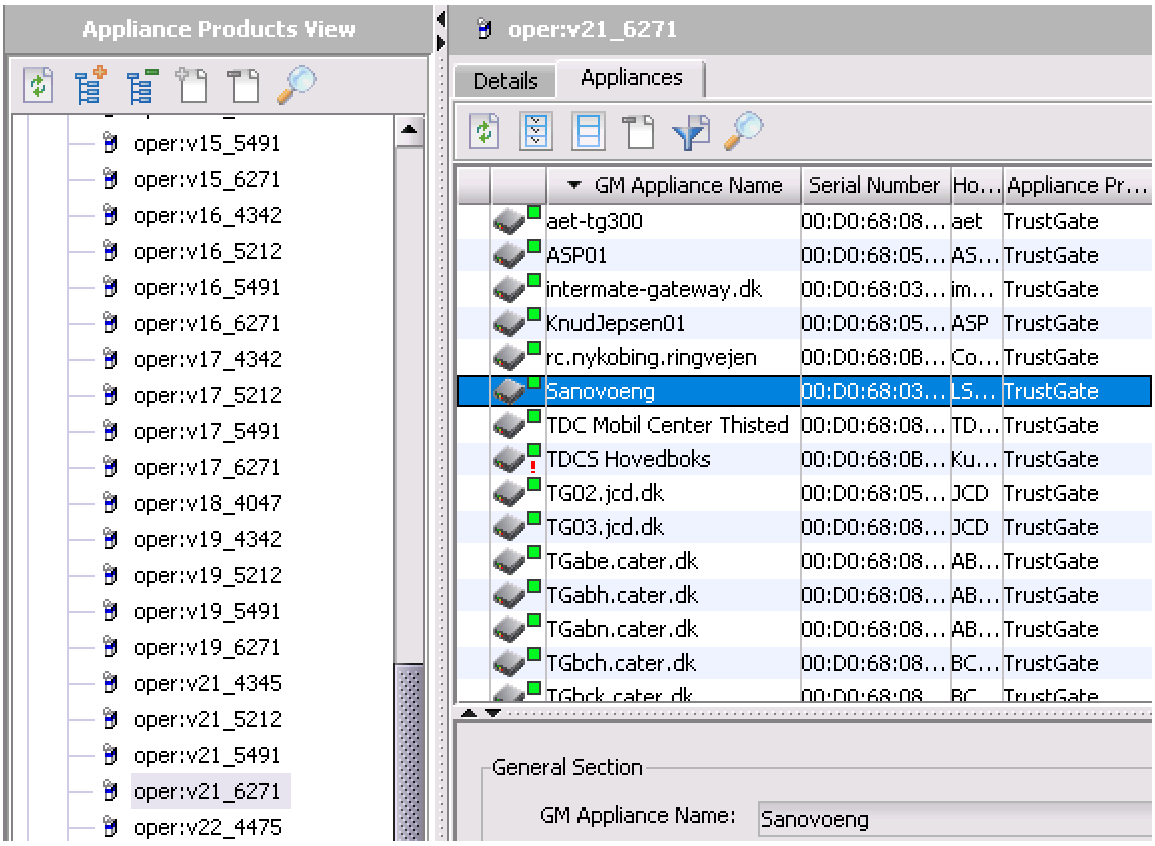
General Section

GM Appliance Name:	Sanovoeng		
Serial Number:	00:D0:68:03:DE:46		
Appliance Product:	TrustGate	Firmware:	bios:01/23/03,oper:v21_6271
Configuration Changed:	Yes	Changed Through:	Unknown

3. Make a note of the firmware files listed and use the same syntax for the firmware file you are adding.

14.4. How to find Appliances running a particular firmware

From the **Appliance Products** View, you can see which Appliances running which particular firmware file version – given, of course, that the appropriate file has been added (see "How to add a firmware file to the repository" page 76), that the Revision field text is correct (see "About the revision field when adding a firmware file" page 76), and that there are one or more Appliances running that firmware.



GM Appliance Name	Serial Number	Ho...	Appliance Pr...
aet-tg300	00:D0:68:08...	aet	TrustGate
ASP01	00:D0:68:05...	AS...	TrustGate
intermate-gateway.dk	00:D0:68:03...	im...	TrustGate
KnudJepsen01	00:D0:68:05...	ASP	TrustGate
rc.nykobing.ringvejen	00:D0:68:0B...	Co...	TrustGate
Sanovoeng	00:D0:68:03...	LS...	TrustGate
TDC Mobil Center Thisted	00:D0:68:08...	TD...	TrustGate
TDCS Hovedboks	00:D0:68:0B...	Ku...	TrustGate
TG02.jcd.dk	00:D0:68:05...	JCD	TrustGate
TG03.jcd.dk	00:D0:68:08...	JCD	TrustGate
TGabe.cater.dk	00:D0:68:08...	AB...	TrustGate
TGabh.cater.dk	00:D0:68:08...	AB...	TrustGate
TGabn.cater.dk	00:D0:68:08...	AB...	TrustGate
TGbch.cater.dk	00:D0:68:08...	BC...	TrustGate
TGbck.cater.dk	00:D0:68:08...	BC...	TrustGate

General Section

GM Appliance Name: Sanovoeng

Actions you can take from the Appliances table in the Appliance Products View

- If you select an entry in the table, the **Appliance Details** are shown below the table. From here, you can "**Go to Appliance**" if GTA is supported.
- If you right-click on the entry, the **Command** menu will be displayed.

15. Optimizing your browser

A browser is used for reading the online help for the GateManager console and for "Go to Appliance" using http or https. Use the information in this section to solve any problems you experience with these operations.

15.1. Browser for online help

The online help system uses JavaScript and frames.

If you open a topic page directly via a link or from **Search** or **Index**, and you want to see where the topic is in the Contents hierarchy, click twice on the **Contents icon** at the top of the topic page.

The help system has been tested on Microsoft Internet Explorer (MSIE), Firefox, and Opera.

MSIE v 6.x and 7.0

If you want to navigate without being asked to give special permission with every click, adjust your browser settings like this:

1. Select **Tools > Options (or Tools > Internet Options)**.
2. Click the **Advanced** tab.
3. In the **Security** group, select **Allow active content to run on files on My Computer**.

Firefox v2.0

If you want to use **Search** in this help system you must install the **IE Tab** extension in Firefox. Switch to **IE** as **rendering engine** when viewing the help system. Read more here: Online help has no "search" in Firefox (page 80).

Opera 9.02

The **Contents** tab in the help system does not dynamically show the placement of the page you are looking at.

- If you do not want to use the PC's default browser for using the help system, set the path for a different browser in the **Program** block of Session Preferences for Console (page 12). For example, if your default browser is Firefox, you can set the Help browser to Internet Explorer.

15.2. Go to Appliance Browser

Many Go to Appliance operations are done with a browser using http or https.

Some appliance products will accept logon using the special GateManager user name and session password; others will always present you with a native login dialog.

If you want to "Go to" an appliance that *can* support *automatic* presentation of session credentials in the URL, and **Microsoft Internet Explorer** (MSIE) is the default browser on the PC, you may get blocked.

There are three work-arounds:

- Use manual login as described in Go to Appliance (GTA) using Manual Login (page 87). In addition, you might want to create a **Go to Appliance Service** in your Session **Preferences** for Console (page 12) that will never include credentials; see GTA: http- and https-based Services.
- Update your Windows registry as described here (see "Windows registry changes for GTA with automatic login" page 88), so that automatic presentation of credentials is allowed when using MSIE.
- Select a different Go to Appliance browser, such as Firefox. To do this configure a **Go to Appliance Service** on Session **Preferences** for Console (page 12). See GTA: http- and https-based Services, especially the example "...your default browser is MSIE, and you want to use Firefox for Go to Appliance using the https protocol ... ".

See also Go to Appliance (GTA) Connection blocked (see "Go to Appliance (GTA) Connection doesn't work" page 93).

16. Console display problems

16.1. Special situations

- Some old versions of agents, such as Ping Agents and AKA2xx Agents, may hang on "Get Device Status". Work-around: log out of console if possible; close it; start it again and log in.
- If you connect to the GateManager using a host name registered in a dynamic dns service, and the IP address changes while a Console session is going, the connection may be lost. Work-around: Close the Console. Start it again and log in.
- If you use two monitors, you may run into the following problem: Sometimes when you start the Console, parts of the GUI are not displayed - especially the main menu line. This is a Java issue that will probably be solved in future Java releases. Work-around: try resizing and/or moving the window; if that doesn't work, close the console. Start it again and log in.
- Very long refresh time. See Display doesn't show known changes? Refresh! (see "Console display doesn't show known changes? Refresh!" page 79)

16.2. Console display doesn't show known changes? Refresh!

In order to avoid unnecessary traffic on the GateManager Server, information will not be refreshed on the GateManager Console until a refresh is actively provoked.

A few individual fields are refreshed automatically, for example the response to a request for a Heartbeat and timeout count-down fields.

- But, as a general rule, when you look at something on the GateManager Console, you will start by refreshing.

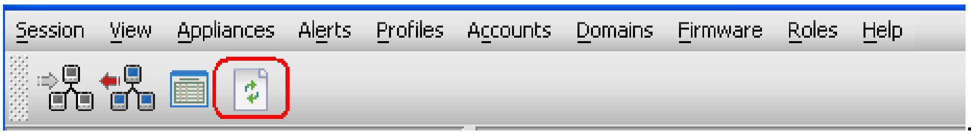
Click on a refresh button to refresh individual objects or multiple objects.

The appliance data you get from the GateManager Server/Database reflects what was received in the last Heartbeat from each appliance. If you want truly real-time information click **Request Heartbeat** on the Appliance’s **Details** tab and then click a refresh button.

Patience please: The more objects there are, of course, the longer it can take for a multiple-object refresh for complete.

16.3. Using AutoRefresh

AutoRefresh is started and stopped by clicking the refresh button on the Main tool bar.



When AutoRefresh is on, it forces a new automatic refresh x [hours:minutes:seconds] after each completed automatic refresh. X is the amount of time set in Session Preferences: Autorefresh interval (see "Preferences for Autorefresh interval" page 14).

The first Refresh occurs x [hours:minutes:seconds] after you click the button.

- **Important**: Remember to turn AutoRefresh off if you do not really need it.

17. Can't find ...

17.1. Online help has no "search" in Firefox

Problem

When I select the **Search** tab in Mozilla Firefox, it is blank. There is no field to enter a search term in.

Solution

Firefox does not support the particular script used in the online help to provide search. If you use Firefox and want to be able to search the online help, you can install the **IE tab** add-on.

Installation

1. Go to https://addons.mozilla.org/en-US/firefox/addon/1419
2. Click the **Install Now** button on the web page.
3. When **Install now** appears on the screen, click it.
4. Click **Restart Firefox**.

Use

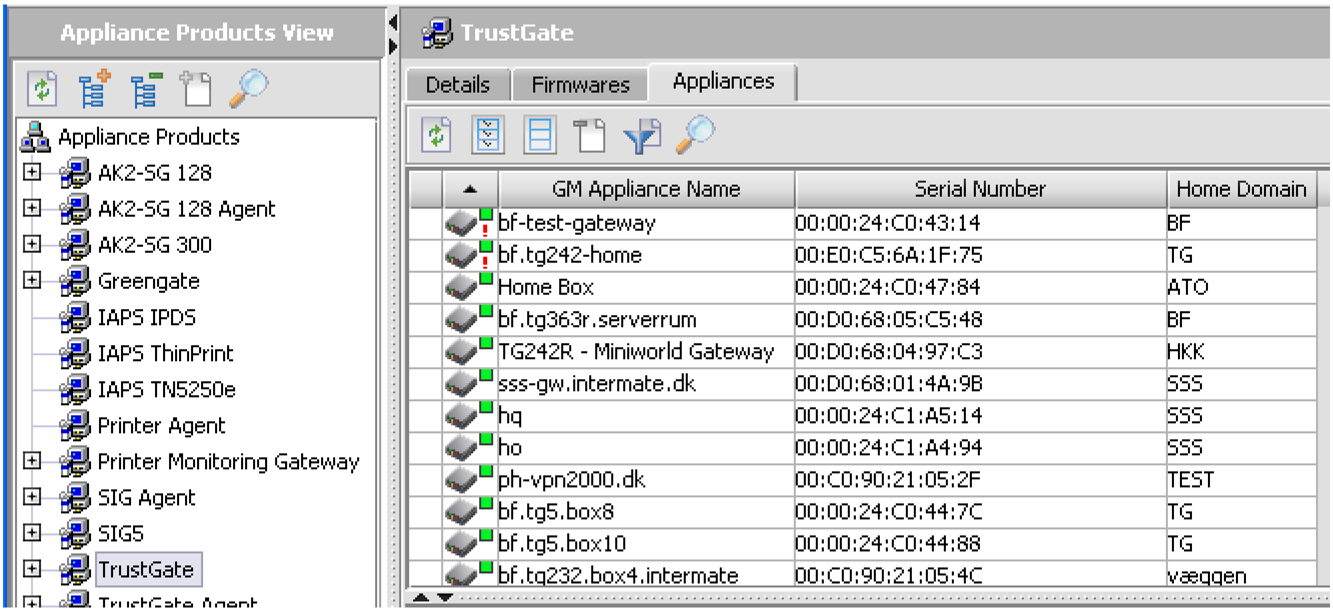
When you have **IE tab** installed, you can switch between Firefox and Microsoft Internet Explorer (MSIE) with a single click. This process is called switching "rendering engines".

Usually the button is placed in the lower right hand corner. There is a tool tip (mouse-over) that explains how to use the button. If you like, you can have one tab running MSIE while your other tabs are running Firefox.

17.2. Where are Appliances of a given type?

Highlight the **Appliance Product** of interest, for example TrustGate, as shown here.

Select the **Appliances** tab to see a table of all Appliances of this type that are in your home domain or a non-private subdomain to your home domain.



	▲	GM Appliance Name	Serial Number	Home Domain
		bf-test-gateway	00:00:24:C0:43:14	BF
		bf.tg242-home	00:E0:C5:6A:1F:75	TG
		Home Box	00:00:24:C0:47:84	ATO
		bf.tg363r.serverrum	00:D0:68:05:C5:48	BF
		TG242R - Miniworld Gateway	00:D0:68:04:97:C3	HKK
		sss-gw.intermate.dk	00:D0:68:01:4A:9B	SSS
		hq	00:00:24:C1:A5:14	SSS
		ho	00:00:24:C1:A4:94	SSS
		ph-vpn2000.dk	00:C0:90:21:05:2F	TEST
		bf.tg5.box8	00:00:24:C0:44:7C	TG
		bf.tg5.box10	00:00:24:C0:44:88	TG
		bf.tg232.box4.intermate	00:C0:90:21:05:4C	væggen

Using the table

If you select an entry in the table, e.g. with a single left click, the **Appliance Details** are shown below the table.

If you right click on the entry, the **Command** menu will be displayed.

If **Go to Appliance** is supported, you can do it either from the **Appliance Details** tab or the **Command** menu.

17.3. Attach Tentative Appliance Dialog has missing domains

When you select an Appliance and start the **Attach Tentative Appliance Dialog**, the first screen displays a product-aware tree that includes only the domains you can choose among. So, you will only see the domains which have a product binding for that particular Appliance.

See Domain doesn't have the necessary product binding (see "Domain does not have the necessary product binding" page 81).

17.4. An enrolled Appliance hasn't shown up where you expect it

When you configure an appliance for first-time enrollment, you include a Domain Token. This tells the GateManager where to tentatively place it in the domain hierarchy.

The appliance will be placed incorrectly if

- the Domain doesn't have the necessary product binding (see "Domain does not have the necessary product binding" page 81); this should be your first suspicion.
- the Domain Token is not recognized (see "Domain Token not recognized" page 81).

For most products, if the Domain Token is blank, the Appliance will not even show up on the GateManager; for a few, a blank Domain Token will be treated as not recognized.

See also *Appliances that are hidden* (page 83).

17.4.1. Domain does not have the necessary product binding

1. Select the **Domain Name** in the **Domains View**.
   - **Tip**: You are probably in the **Appliances View** looking for the Appliance. Right-click on the **Domain Name** and select **Go to Domains View**.
2. Click the **Product Bindings** tab.
3. Look for the relevant **Appliance Product** on the table.
4. If the Appliance Product is on the table, go to Domain Token not recognized (page 81).

   If the Appliance Product is *not* on the table, click on the Add button.
5. A **Bind Appliance Products** dialog will open.
6. Do one of the following:
   - If the Appliance Product you are looking for is on the list, click on the selection column to select it; then click **OK**.
   - If the Appliance Product is not on the list, go up the domain hierarchy until you find it. The Appliance Product will be made available for binding in a domain once it is available in the parent domain. You may need to bind several levels in the hierarchy, and you may need to get help from a higher-level administrator.

17.4.2. Domain Token not recognized

The GateManager reads the Domain Token from left to right, element by element, moving down the hierarchy domain by domain. When it reaches an unrecognized element, it will stop looking and tentatively place the Appliance at the last recognized level.

Example

You are the administrator of a domain hierarchy that looks like this with domain tokens as shown.

Hierarchy	Domain Tokens
Company B	Root.Company B
B1	Root.Company B.B1
B11	Root.Company B.B1.B11
B12	Root.Company B.B1.B12
B2	Root.Company B

You have enrolled an appliance that you simply cannot find anywhere. You contact the top administrator who finds the appliance in ROOT, marked as Unrecognized ?.

The Domain token entered was	- what was wrong?
Blank	(Missing. A blank domain token in some products places the Appliance in ROOT. In most products, the Appliance won't even show up there).
Cmpany B.B1	Typographical error: the o in Company is missing.
ROOT.COMPANY-B.B1.B11	The second element in the Domain Token is written as "COMPANY-B" (with a hyphen), but should have been written "COMPANY B" (with a space).

Tell the administrator where the appliance should be, and he or she will attach it to the correct domain.

17.5. Which Appliances in a given Domain are ... e.g. Failed?

- **Note**: The Appliances **Report** function was first introduced in GateManager release 3.3. If you are blocked from activating the **Reports** tab for a domain in the Appliances View, your role has no privileges in the **Appliance Reports** group. Contact the GateManager Owner.

17.5.1. Appliance Report Definition

1. In the **Appliances** View, select the domain of interest.
2. Select the **Reports** tab.
3. On the top part of the tab, click the 📄 button to create a report definition.
4. On the **Select Appliance Product** screen that results, select **Generic** or a specific **Appliance Product**.
5. Click **Next**.
6. Give the report definition a meaningful **Name**.
7. Click the **Edit** button to start the Expression editor.
8. Select parameters and values in the expression editor, which works exactly as the Alert Rules editor does.
9. Save changes and close the dialog by clicking **OK**.
10. Save changes and close the dialog by clicking **OK**.

You can delete a Report Definition if your role includes the Delete Appliance Report Definition privilege (Appliance Reports group (see "Appliance Reports" page 42)). There is no limit to the number of definitions that can be stored.

17.5.2. Appliance Report Generation

Pre-requisite: You have a Report Definition (see "Appliance Report Definition" page 82).

1. In the **Appliances** View, select the domain of interest.
2. Select the **Reports** tab.

3. Do one of the following:
   - On the table on the top half of the Reports tab, right-click the **Report Definition** of interest and select **Generate Report** from the context menu.
   - Click the Generate Report icon on the table for the Report Definition of interest; this table is on the bottom half of the Reports tab.
4. Answer **Yes** or **No** to the Question "Would you like to include subdomains in the report?"

The report will be added to a table on the bottom half of the tab.

You can delete a report if your role includes the Delete Appliance Report privilege (Appliance Reports group (see "Appliance Reports" page 42)). There is no limit to the number of reports that can be stored.

17.5.3. Accounts

1. In the **Appliances** View, select the domain of interest.
2. Select the **Reports** tab.
3. To view a generated report, do one of the following on the bottom part of the tab:
   - Highlight the report and click on the Eye icon .
   - Double-click on the report.

The report opens in a separate window. You can use the table headings to sort the entries.

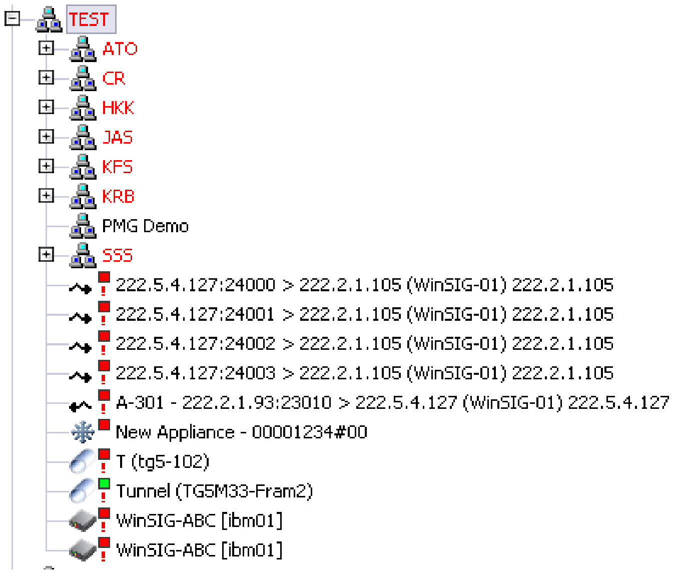
17.6. Hidden objects

17.6.1. Appliances that are hidden

If you don't find an Appliance where you expect it, make sure you are in the **Appliances View** and try one of the following actions:

Simple unhiding

- Expand the domain node + in the Tree pane.
- Be sure to look at the bottom of the domain, as the individual Appliances are shown *after* any subdomains.



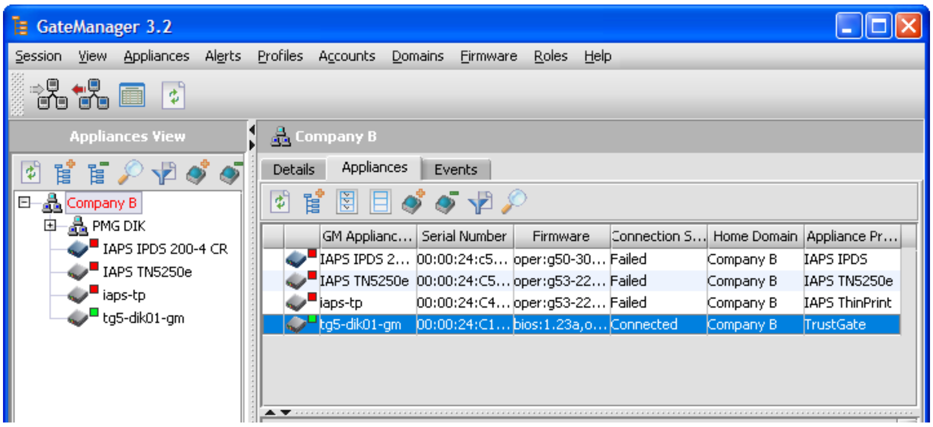
```
TEST
  ATO
  CR
  HKK
  JAS
  KFS
  KRB
  PMG Demo
  SSS
  222.5.4.127:24000 > 222.2.1.105 (WinSIG-01) 222.2.1.105
  222.5.4.127:24001 > 222.2.1.105 (WinSIG-01) 222.2.1.105
  222.5.4.127:24002 > 222.2.1.105 (WinSIG-01) 222.2.1.105
  222.5.4.127:24003 > 222.2.1.105 (WinSIG-01) 222.2.1.105
  A-301 - 222.2.1.93:23010 > 222.5.4.127 (WinSIG-01) 222.5.4.127
  New Appliance - 00001234#00
  T (tg5-102)
  Tunnel (TG5M33-Fram2)
  WinSIG-ABC [ibm01]
  WinSIG-ABC [ibm01]
```

Getting a look at subdomains from a single place

The general rule is that when you select a given domain, you only see the individual objects in it. But there are three ways around this:

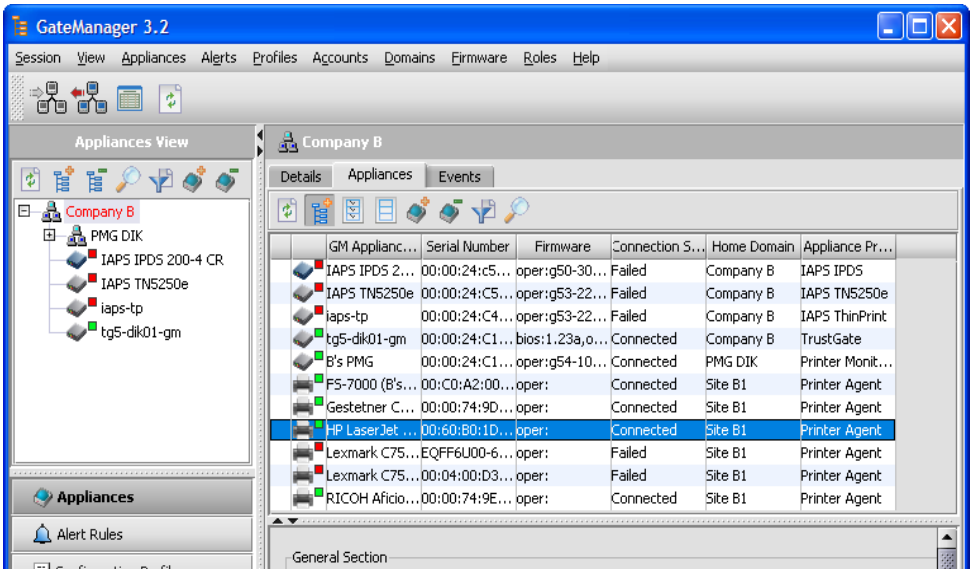
- Expand the entire tree with the icon on the View tool bar .
- Work with the relevant table for the domain.

  For example, if you are using the **Appliances View**, and have selected any domain, there will be an **Appliances** tab in the Information pane. The top half of the pane is a table of Appliances.



GM Applianc...	Serial Number	Firmware	Connection S...	Home Domain	Appliance Pr...
IAPS IPDS 2...	00:00:24:c5...	oper:g50-30...	Failed	Company B	IAPS IPDS
IAPS TN5250e	00:00:24:C5...	oper:g53-22...	Failed	Company B	IAPS TN5250e
iaps-tp	00:00:24:C4...	oper:g53-22...	Failed	Company B	IAPS ThinPrint
tg5-dik01-gm	00:00:24:C1...	bios:1.23a,o...	Connected	Company B	TrustGate

Recourse the table using the icon on the tab tool bar. Result:



GM Applianc...	Serial Number	Firmware	Connection S...	Home Domain	Appliance Pr...
IAPS IPDS 2...	00:00:24:c5...	oper:g50-30...	Failed	Company B	IAPS IPDS
IAPS TN5250e	00:00:24:C5...	oper:g53-22...	Failed	Company B	IAPS TN5250e
iaps-tp	00:00:24:C4...	oper:g53-22...	Failed	Company B	IAPS ThinPrint
tg5-dik01-gm	00:00:24:C1...	bios:1.23a,o...	Connected	Company B	TrustGate
B's PMG	00:00:24:C1...	oper:g54-10...	Connected	PMG DIK	Printer Monit...
FS-7000 (B's...	00:C0:A2:00...	oper:	Connected	Site B1	Printer Agent
Gestetner C...	00:00:74:9D...	oper:	Connected	Site B1	Printer Agent
HP LaserJet ...	00:60:B0:1D...	oper:	Connected	Site B1	Printer Agent
Lexmark C75...	EQFF6U00-6...	oper:	Failed	Site B1	Printer Agent
Lexmark C75...	00:04:00:D3...	oper:	Failed	Site B1	Printer Agent
RICOH Aficio...	00:00:74:9E...	oper:	Connected	Site B1	Printer Agent

- Generate a Report for Appliances that fulfill specified conditions and include subdomains in the report as shown in Which Appliances are ... e.g. Failed? (see "Which Appliances in a given Domain are ... e.g. Failed?" page 82)

17.6.2. Accounts that are hidden

If you don't find an account where you expect it, make sure you are in the **Accounts** View and try one of the following actions:

Simple unhiding

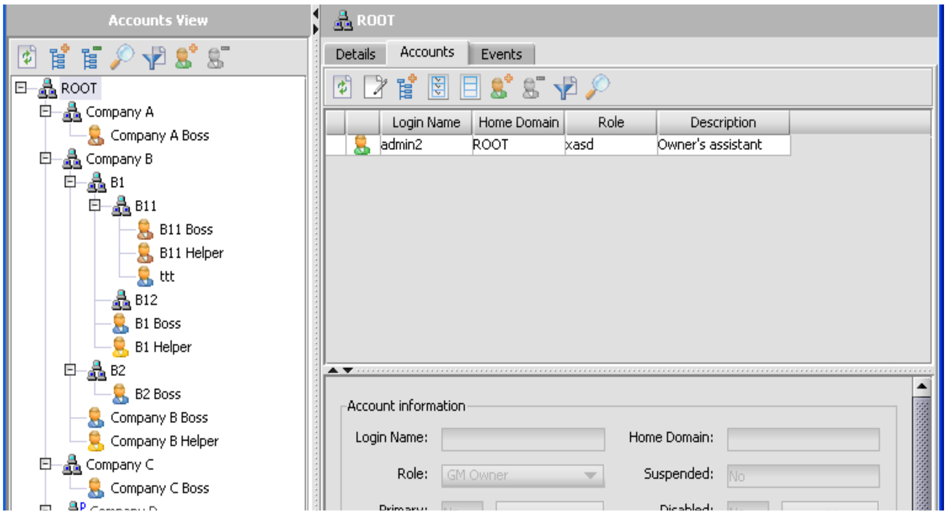
1. Expand the domain node + in the Tree pane.
2. Be sure to look at the bottom of the domain, as the individual accounts are shown *after* any subdomains.

Getting a look at subdomains from a single place

The general rule is that when you select a given domain, you only see the individual objects in it, not in its subdomains. But there are two ways around this:

- Expand the entire tree with the icon on the tool bar .
- Work with the relevant table for the domain.

  For example, when you have selected any domain, there will be an **Accounts** tab in the Information pane. The top half of the pane is a table of accounts.



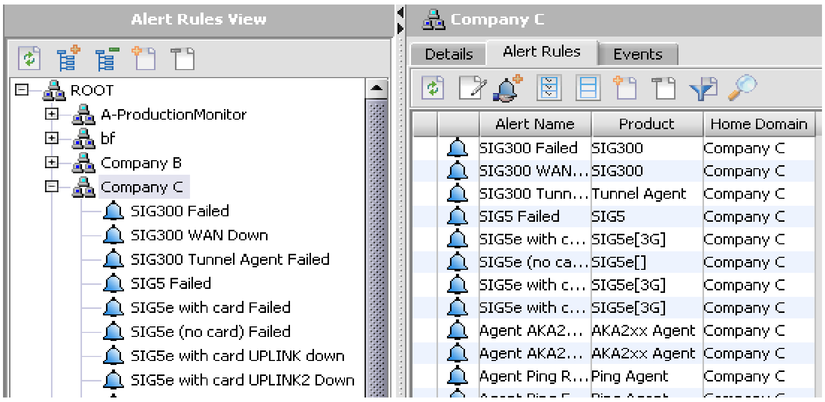
Login Name	Home Domain	Role	Description
admin2	ROOT	xasd	Owner's assistant

Login Name:
Home Domain:
Role: GM Owner
Suspended: No

Recourse the table using the icon on the tab's tool bar.

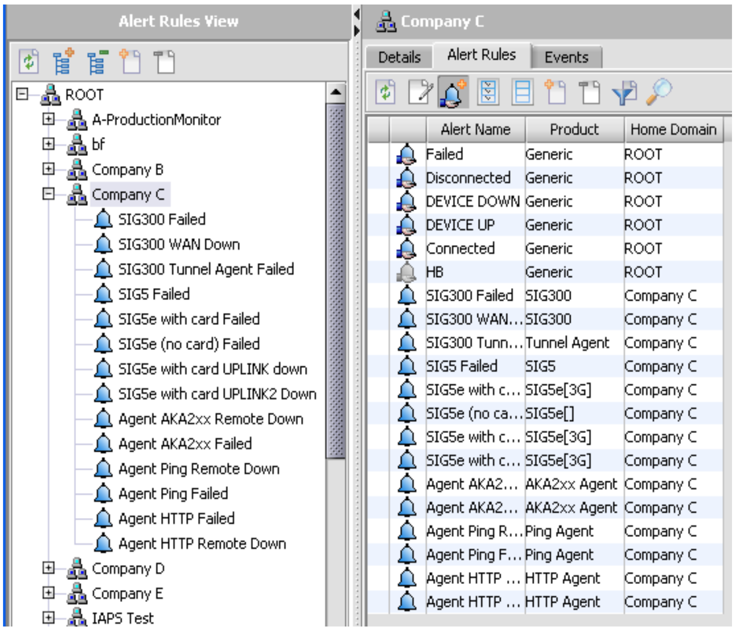
17.6.3. Alert rules that are hidden

If an alert rule is not actively shared downward, it is supposed to be hidden. If you want to see the rules that have been shared to a domain from a higher domain, you will not see them listed in the Tree pane even after you expand the tree or the domain node.



Alert Name	Product	Home Domain
SIG300 Failed	SIG300	Company C
SIG300 WAN...	SIG300	Company C
SIG300 Tunn...	Tunnel Agent	Company C
SIG5 Failed	SIG5	Company C
SIG5e with c...	SIG5e[3G]	Company C
SIG5e (no ca...	SIG5e[]	Company C
SIG5e with c...	SIG5e[3G]	Company C
SIG5e with c...	SIG5e[3G]	Company C
Agent AKA2...	AKA2xx Agent	Company C
Agent AKA2...	AKA2xx Agent	Company C
Agent Ping R...	Ping Agent	Company C

Click the Show Shared button on the tab tool bar. The rules that have been shared from a higher domain are now visible on the table - and only there.



- ROOT
  - A-ProductionMonitor
  - bf
  - Company B
  - Company C
    - SIG300 Failed
    - SIG300 WAN Down
    - SIG300 Tunnel Agent Failed
    - SIG5 Failed
    - SIG5e with card Failed
    - SIG5e (no card) Failed
    - SIG5e with card UPLINK down
    - SIG5e with card UPLINK2 Down
    - Agent AKA2xx Remote Down
    - Agent AKA2xx Failed
    - Agent Ping Remote Down
    - Agent Ping Failed
    - Agent HTTP Failed
    - Agent HTTP Remote Down
  - Company D
  - Company E
  - IAPS Test

Alert Name	Product	Home Domain
Failed	Generic	ROOT
Disconnected	Generic	ROOT
DEVICE DOWN	Generic	ROOT
DEVICE UP	Generic	ROOT
Connected	Generic	ROOT
HB	Generic	ROOT
SIG300 Failed	SIG300	Company C
SIG300 WAN...	SIG300	Company C
SIG300 Tunn...	Tunnel Agent	Company C
SIG5 Failed	SIG5	Company C
SIG5e with c...	SIG5e[3G]	Company C
SIG5e (no ca...	SIG5e[]	Company C
SIG5e with c...	SIG5e[3G]	Company C
SIG5e with c...	SIG5e[3G]	Company C
Agent AKA2...	AKA2xx Agent	Company C
Agent AKA2...	AKA2xx Agent	Company C
Agent Ping R...	Ping Agent	Company C
Agent Ping F...	Ping Agent	Company C
Agent HTTP ...	HTTP Agent	Company C
Agent HTTP ...	HTTP Agent	Company C

17.6.4. Configuration profiles that are hidden

If a configuration profile (CP) is not actively shared downward, it is supposed to be hidden.

What may take a little getting used to is that if you want to see the profiles that have been shared downwards, you can not see them in the Tree pane of the Configuration Profiles View, even after you expand the tree. Instead

1. Select the domain of interest in the Configuration Profiles View.
2. Select the Configuration Profiles tab.
3. Click the Show Shared button on the tab tool bar.

17.6.5. Domains that are hidden

Domains View: You cannot recourse the table of domains on the Domains tab in the Information pane. If you need to see domains lower than one level down, use the Tree pane, and expand a node ⊞ or expand the tree .

Appliance View: When you attach an Appliance to a domain, you will only see domains that have the necessary product binding.

18. Go to Appliance (GTA)

18.1. GTA Connection broken

There are two predictable situations where the GTA connection gets broken.

- **Timeout**

  The connection times out after 15 minutes of activity. This is done for security reasons. Click **Go to Appliance** again.

- **Reboot**

  Rebooting the appliance usually breaks the connection. Wait for about three minutes after the reboot, then click **Go to Appliance**.

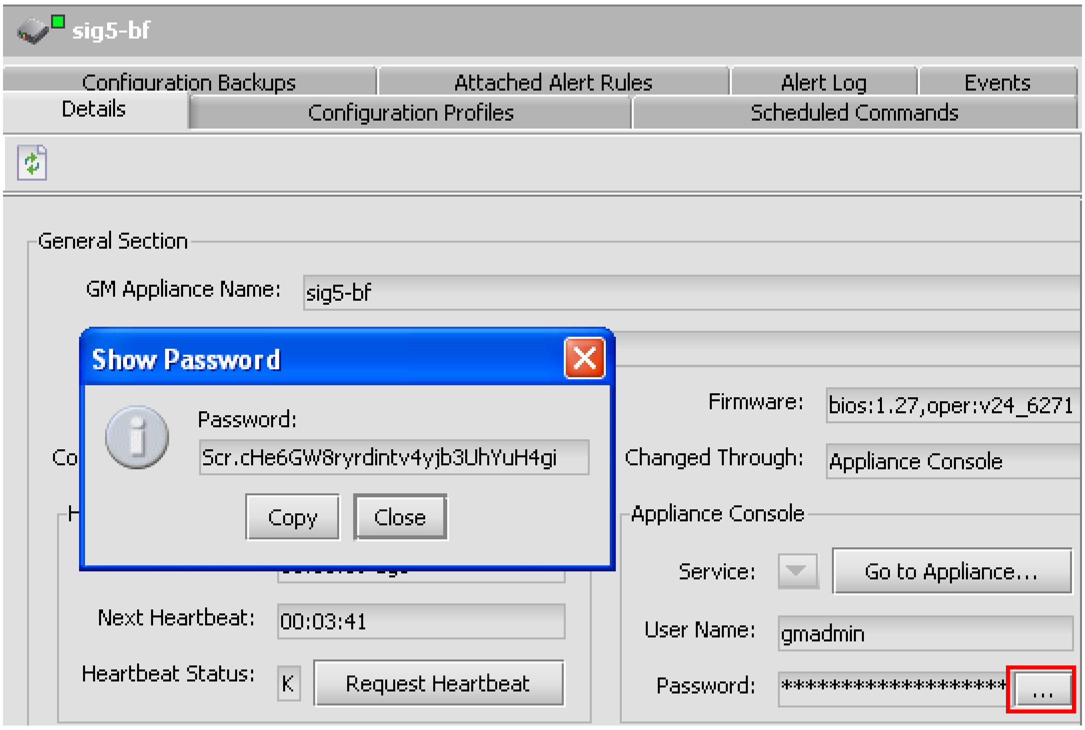
18.2. Go to Appliance (GTA) using Manual Login

If you do not want to automatically present credentials when you log on with a browser to a GateManager-enabled appliance that generates GateManager-session passwords (TrustGate, SIG, etc), you have two possibilities:

- Present the normal user name and password for the appliance
- Use the gmadmin account and paste the session password in.

How to manually login using the GateManager session password

1. In the Appliances View, use a single left click to highlight the Appliance you want to "go to".
2. On the **Appliances Details** tab, below the **Go to Appliance** button and session user name is an ellipsis (…) button to Show Password. Click it



GM Appliance Name: sig5-bf

Password: Scr.cHe6GW8ryrdintv4yjb3UhYuH4gi

Firmware: bios:1.27,oper:v24_6271

Changed Through: Appliance Console

Service:

Next Heartbeat: 00:03:41

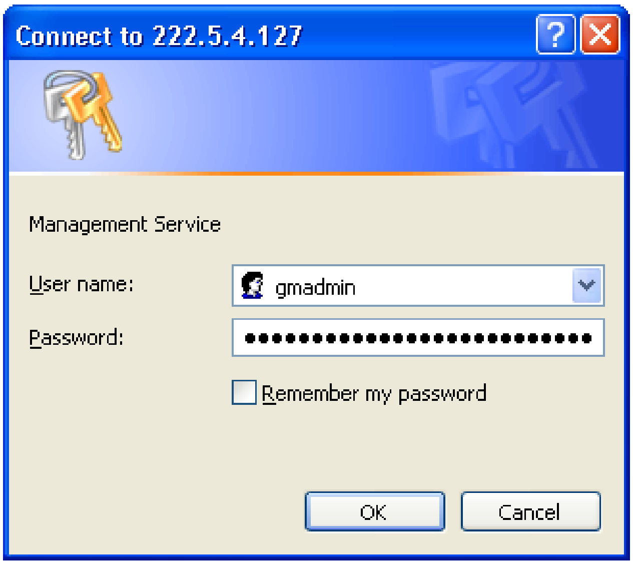
User Name: gmadmin

Heartbeat Status: K

Password: ******************

3. Click **Copy** on the popup. This will automatically copy the password to your clipboard.
4. Click the **Go to Appliance** button.

5. When asked to log in to the appliance, type in the special user ID **gmadmin** and paste (Ctrl+v) the session password from your clipboard in to the password field.



Connect to 222.5.4.127

Management Service

User name: gmadmin

Password: ••••••••••••••••••••••••••

□ Remember my password

18.3. Windows registry changes for GTA with automatic login

In the beginning of February 2004, Microsoft issued a security update (832894) for Microsoft Internet Explorer (MSIE), which helps to protect against spoofing. Windows Explorer and Internet Explorer will not open HTTP or HTTPS sites by using a URL that includes user information. Cf. http://support.microsoft.com/default.aspx?scid=kb;en-us;834489 (http://support.microsoft.com/default.aspx?scid=kb;en-us;834489)

So, by default, if user information is included in an HTTP or an HTTPS URL, the resulting web page shows an error (page cannot be displayed or invalid syntax error). If you have installed this security update, you cannot let the GateManager automatically present credentials to Microsoft Internet Explorer.

If you don't want to log on manually or use a different browser (see "Go to Appliance Browser" page 78), and you determine that "Go to Appliance" gives you a page cannot be displayed or invalid syntax error, you can adjust your Windows registry as shown here.

Do not attempt this unless you have experience working with the registry or can find an experienced registry user to do it for you.

18.3.1. What the result looks like in the registry

Create iexplore.exe and explorer.exe DWORD values in *one* of the following registry keys. Set the value data to 0.

For *all users of the program*, set the value in the following registry key:
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

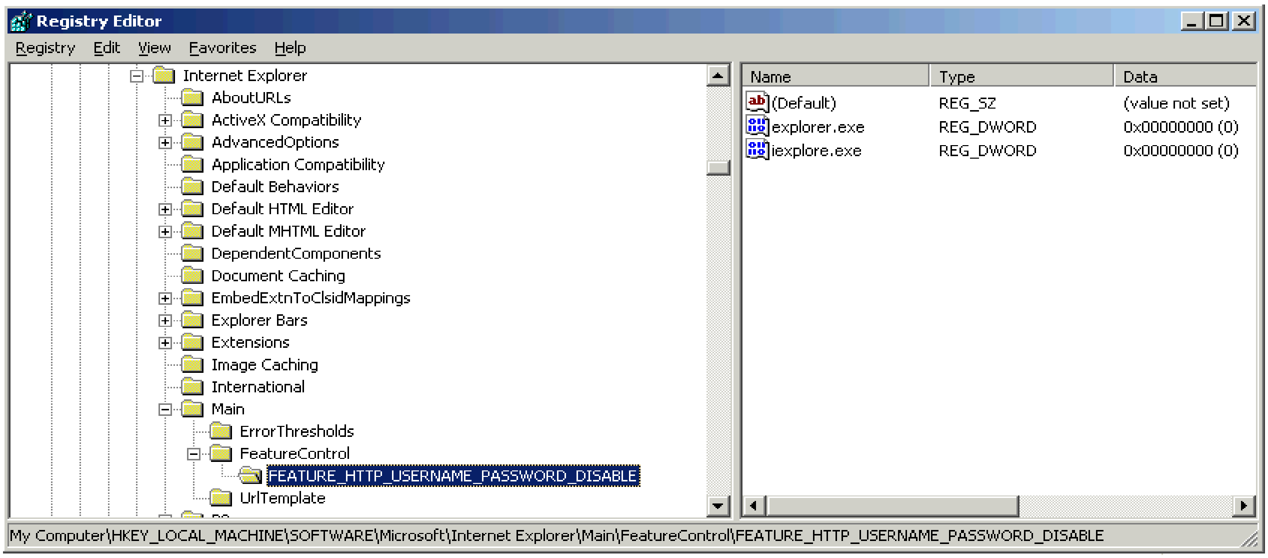
"explorer.exe"=dword:00000000
"iexplore.exe"=dword:00000000

OR

For *the current user of the program only*, set the value in the following registry key:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

"explorer.exe"=dword:00000000
"iexplore.exe"=dword:00000000

The result should look like this:



- Internet Explorer
  - AboutURLs
  - ActiveX Compatibility
  - AdvancedOptions
  - Application Compatibility
  - Default Behaviors
  - Default HTML Editor
  - Default MHTML Editor
  - DependentComponents
  - Document Caching
  - EmbedExtnToClsidMappings
  - Explorer Bars
  - Extensions
  - Image Caching
  - International
  - Main
    - ErrorThresholds
    - FeatureControl
      - FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
    - UrlTemplate

Name	Type	Data
(Default)	REG_SZ	(value not set)
explorer.exe	REG_DWORD	0x00000000 (0)
iexplore.exe	REG_DWORD	0x00000000 (0)

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

Regedit: How to proceed (see "Regedit: how to adjust the registry step by step" page 89)

18.3.2. Regedit: how to adjust the registry step by step

- **IMPORTANT:** These instructions are known to work for Windows 2003 using an English user interface. Consult your Windows documentation if you are running a different operating system.
- **NOTE:** All the entries you make are case-sensitive. To avoid typographical errors, it could be a good idea to copy/paste text from here into the text fields when renaming.

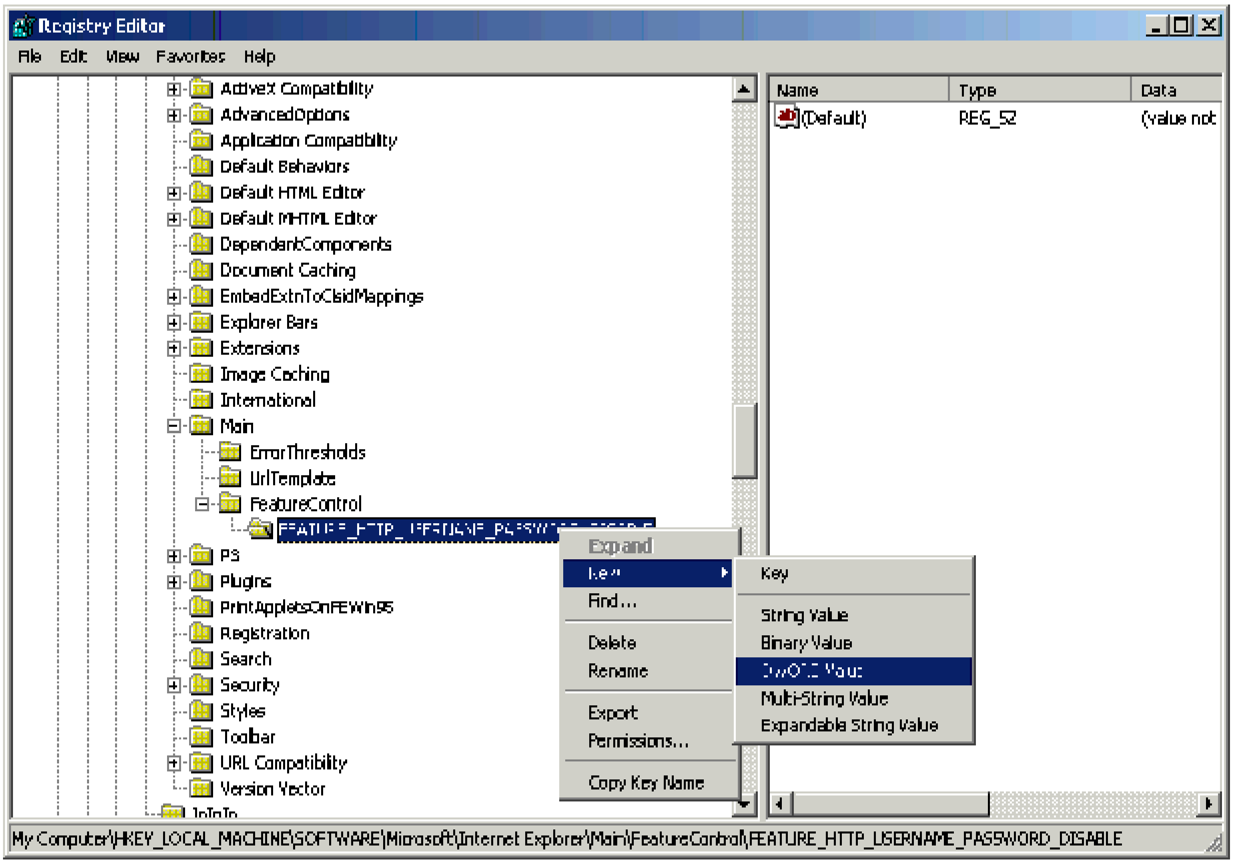
1. Start the Registry editor like this: In Windows click **Start** and **Run**, enter **regedit** and click **OK**.
2. Decide whether you want any user of the PC to able to present credentials in an Internet Explorer URL - or limit this feature to the specific user currently logged in.
   - To give any and all users this feature, unfold the registry tree down to the folder

     HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\
   - To restrict this feature to the specific user currently logged in, unfold the registry tree down to the folder **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\**
3. If the folder **FeatureControl** exists in the **Main** folder, go to the next step. If it does not exist, it must be created like this.
   a. Right-click on the **Main** folder.
   b. Select **New** and **Key**
   c. The new key is named **New Key #1** by default. Rename it to **FeatureControl**.
4. If the folder **FEATURE_HTTP_USERNAME_PASSWORD_DISABLE** does not exist in the **FeatureControl** folder, create it like this.
   a. Right-click on the **FeatureControl** folder.
   b. Select **New** and **Key**
   c. The new key is named **New Key #1** by default. Rename it to **FEATURE_HTTP_USERNAME_PASSWORD_DISABLE**.
5. Now you will add two DWORD values to the key: iexplore.exe and explore.exe. Follow these instructions.

Follow these instructions to add two DWORD values to the key: iexplore.exe and explore.exe.

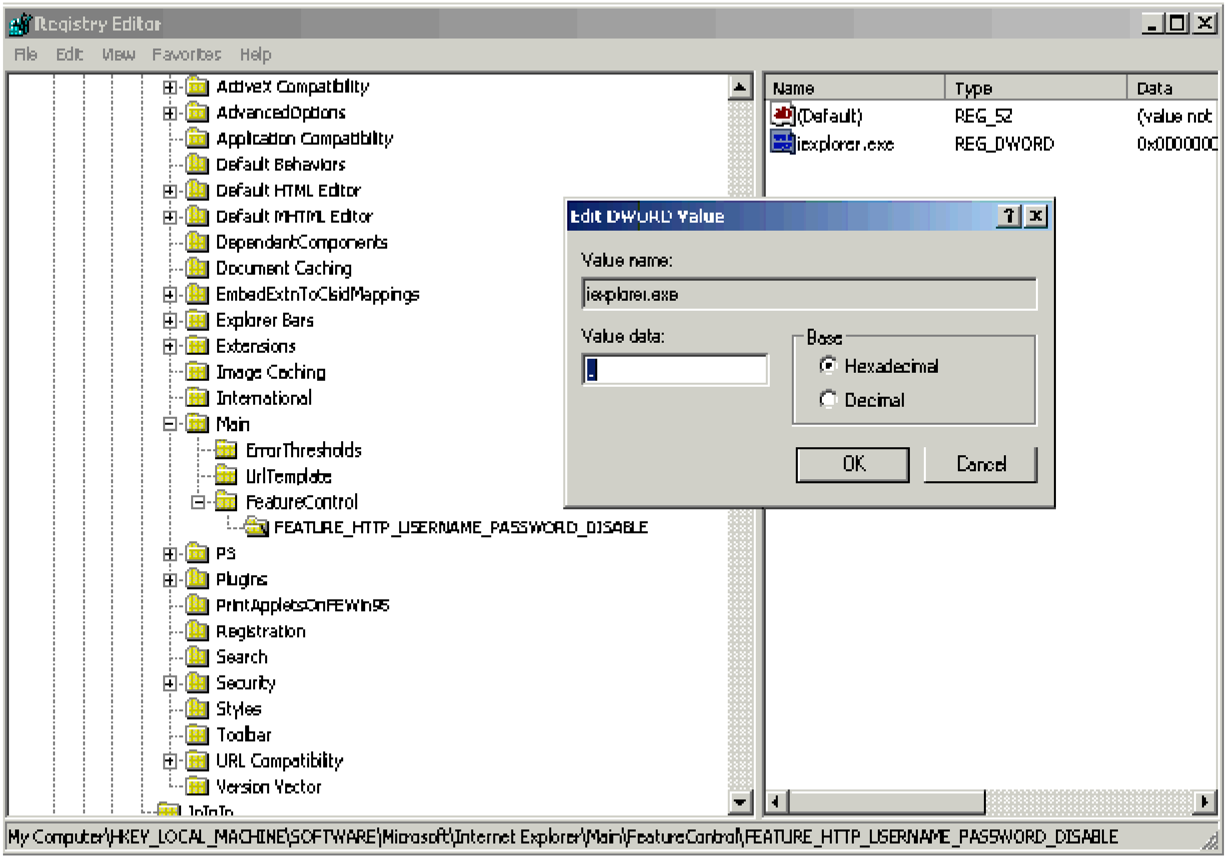
   a. Right-click the **FEATURE_HTTP_USERNAME_PASSWORD_DISABLE** key (folder).

b. Select **New**, select **DWORD Value**.



c. The new value is added to the list of DWORD values for FEATURE_HTTP_USERNAME_PASSWORD_DISABLE and is automatically named **New Value #1**. Rename it to **iexplore.exe**, for example by right-clicking it and selecting **Rename**.

d. Double click on **iexplore.exe**, and ensure that value data is set to **0**.



Name	Type	Data
(Default)	REG_SZ	(value not
iexplorer.exe	REG_DWORD	0x0000000

Edit DWORD Value

Value name: iexplorer.exe

Value data:

Base: ● Hexadecimal ○ Decimal

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

Repeat steps a-d to create a new DWORD value called **explorer.exe**.

6. Close down the registry editor.

Result: You will be able to use "Go to Appliance" with automatic presentation of the special user name gmadmin and the session password.

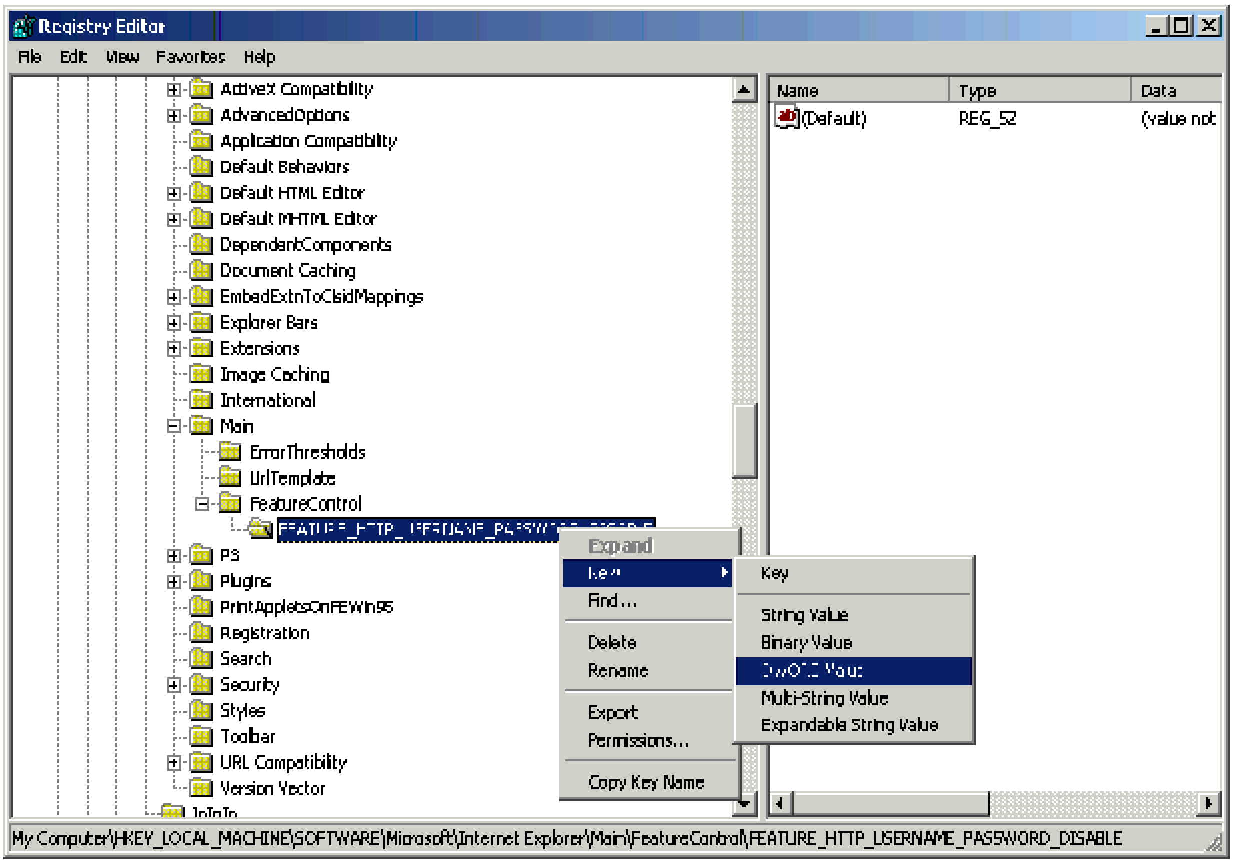
- **NOTE:** The DWORDs should not be placed in both LOCAL MACHINE and CURRENT USER. If you want to change the settings from one to the other, be sure to go back and delete them in your first setup.

DWORD values

Follow these instructions to add two DWORD values to the key: iexplore.exe and explore.exe.

a. Right-click the **FEATURE_HTTP_USERNAME_PASSWORD_DISABLE** key (folder).

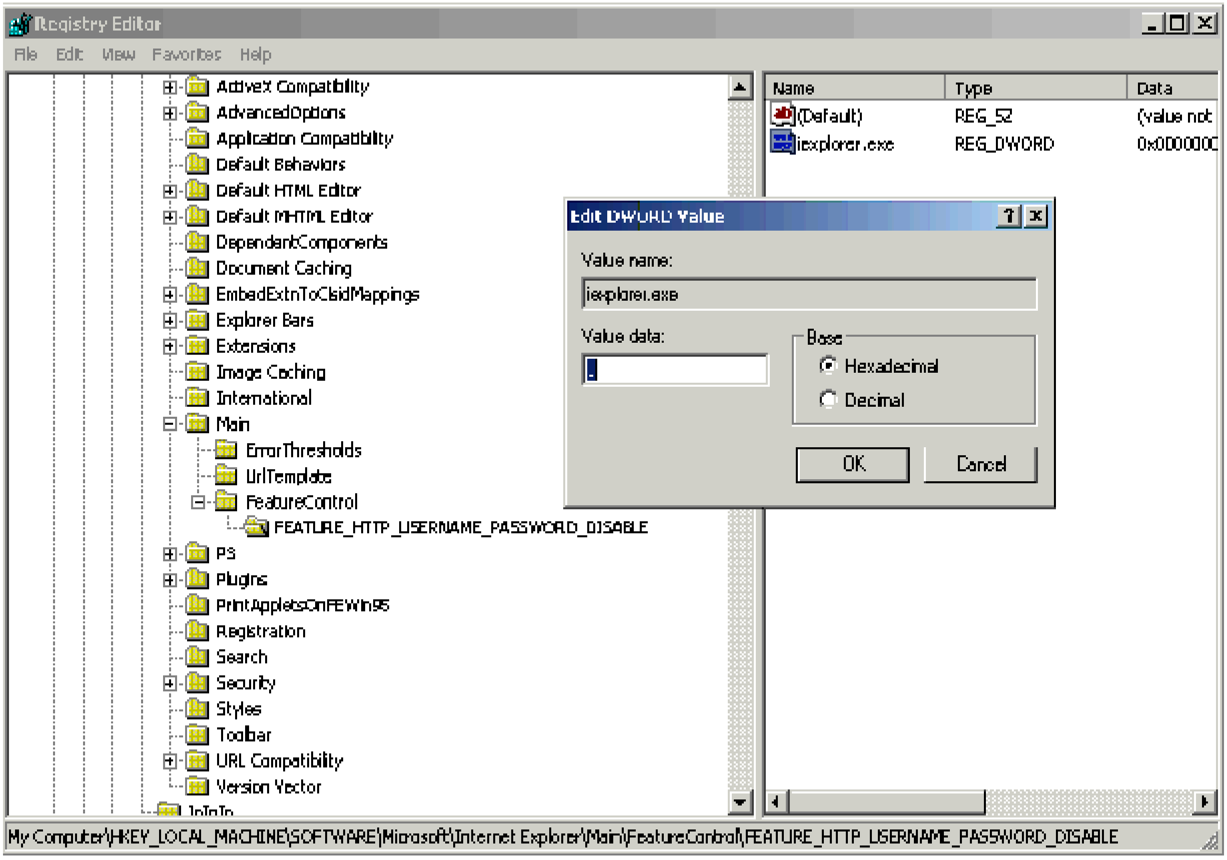
b. Select **New**, select **DWORD Value**.



My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

c. The new value is added to the list of DWORD values for FEATURE_HTTP_USERNAME_PASSWORD_DISABLE and is automatically named **New Value #1**. Rename it to **iexplore.exe**, for example by right-clicking it and selecting **Rename**.

d. Double click on **iexplore.exe**, and ensure that value data is set to **0**.



Name	Type	Data
(Default)	REG_SZ	(value not
iexplorer.exe	REG_DWORD	0x0000000

Value name: iexplorer.exe

Value data: 0

Base: ● Hexadecimal ○ Decimal

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE

Repeat steps a-d to create a new DWORD value called **explorer.exe**.

18.4. Go to Appliance (GTA) Connection doesn't work

Appliance configuration blocks GTA

In many products, the appliance administrator can block GTA completely. Contact the appliance administrator if you believe that the configuration should be changed or if you simply need more information.

You are asked for a native user name and password - but didn't expect this

Some products always require native user name and password - for example the PMG (Printer Monitoring Gateway) and the various types of IAPS (Intermate Advanced Print Server).

Some products allow GTA with automatic presentation of GateManager session credentials - but can be configured to limit access. Limited access requires you to give the native user name and password for the appliance - even if your GateManager Console preferences define the particular GTA Service as one that includes credentials. Contact the appliance administrator if you believe that the configuration should be changed or if you simply need more information.

"Page cannot be displayed"

If you use **Microsoft Intermate Explorer** (MSIE) and try to include GateManager session credentials in the GTA URL, you may be blocked. For further information and work-arounds, see Go to Appliance Browser (page 78).

"Page cannot be displayed"

If your PC is behind a very restrictive firewall, you may need to get some adjustments done (see Network and firewall configurations for Console use (page 8)).

"Unable to connect to private interface: http: //xxx.xxx.xxx.xxx:55908"

(the x's stand for an IP address, and the port number is an example of a port number assigned for temporary access to the appliance.)

The firewall your PC is behind has not opened for the GTA ports (usually 55000-59999). Contact your system administrator.

No response at all

Your role may not include the GTA privilege. You can see this by Viewing Account privileges (see "Viewing your account privileges" page 18).

Contact your GateManager administrator if you think your role needs to be changed.

19. Logging

19.1. Where does the GateManager log events?

Audit

Each GateManager object has an **Audit**. It is accessed via the Audit tab when an object is selected.

(Before GateManager 3.4, this was called the Events log.)

Appliance Log

Starting with GateManager 3.4, an **Appliance Log** has been added (not available on all GateManager-enabled devices). It is accessed via the Appliance Log tab when an Appliance is selected.

Events are logged regardless of whether the event was initiated by the GateManager or by/on the device itself. Depending on the Appliance Product, the Appliance Log tracks the following:

- GateManager Connect, GateManager Disconnect.
- User Logged In, User Logged Off, User Login Failed;
- Network Interface Up, Network Interface Down;
- Log Overflow; Power On, Shut Down, Reboot.
- Configuration Export, Configuration Import/Update, Firmware Upgrade.
  The configuration- and firmware-related events show what the device has actually experienced and reported; the "same" events in the Audit show commands submitted.

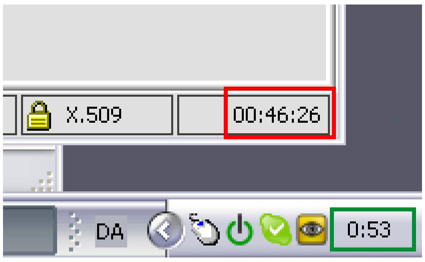
Alert Log

Each Appliance has an **Alert Log** which is accessed via the Alert Log tab when the Appliance is selected. This keeps track of Alerts triggered. The maximum number of retained Alert Log Entries is set as a Domain Preference.

19.2. Time stamps

On login, the Console synchronizes time with the GateManager Server so that all time-stamps reflect Server time, and not the time of the PC running the Console.

The current **server time** is shown in the lower right corner of the GateManager Console:



Here, the red box marks the server time, while the green box marks the PC local time.

20. Glossary of Terms

A

agent

An agent is the representation of a device on the GateManager.

All types of agents are known as **Appliances** on the GateManager Console.

Agents can be grouped into two basic types: **native** and **hosted**.

- **Native agents** represent GateManager-enabled devices such as SiteManager, SiteManager Soft, PMG, WinPMG, IAPS IPDS, and so on. Native agents are sometimes called GateManager Clients - or simply managed appliances.
- **Hosted agents**: Some GateManager-enabled products can also host agents for devices that do not have their own "Agent Control Modules".
  - For example, Printer Agents configured on a PMG or WinPMG make it possible to use the GateManager to monitor or access just about any type of printer imaginable.
  - For example, PC/VNC Agents configured on a SiteManager (or SiteManager Soft) make it possible to use the GateManager to access a PC that is running a remote control server such as UltraVNC.

Unless otherwise stated, the way you work with a hosted agent is exactly the same as the way you work with a native agent.

alert

Alert notifications push information on Appliance status to an e-mail address (which, depending on your telephony service provider, can be sent to your telephone as an instant message / SMS).

The basis for an alert is the alert rule, which you configure in the **Alerts** view. Appliances without Alert Rules attached will not send alerts.

Appliance - with capital A

An Appliance is the representation on a GateManager Console of a GateManager-enabled physical appliance (device gateway or other device), a GateManager-enabled virtual appliance (device gateway or other device), a hosted agent, or a relay service.

Examples

GateManager-enabled device gateway	SiteManager, PMG
GateManager-enabled device	IAPS TN5250e
GateManager-enabled virtual device gateway	SiteManager Soft, WinPMG
GateManager-enabled virtual device	WinIAPS TN5250e
hosted agent	printer agent, serial agent, PC agent, TCP agent
relay service	(SiteManager and SiteManager Soft only) device relay, server relay, web proxy relay

Hosted agents and relay services are GateManager-enabled and can also be seen as virtual appliances. However, the key feature about hosted agents and relay services is that they "live" on another GateManager-enabled entity and make it possible for the GateManager to work with network devices that are not in themselves GateManager-enabled - e.g. printers, equipment connected via an ethernet or serial interface and PCs.

Billing for the use of a GateManager is usually based on the number of enrolled Appliances. In connection with billing, different GateManager Owners may use different terminology, such as enabled agents, activated agents, or enabled devices.

See also Appliance status, Appliance state and connection state.

appliance product

In GateManager this term describes a supported *type* of physical appliance, virtual appliance, agent or relay service.

Appliance products are visible in the **Appliance Products View**, which also serves as a firmware repository. Each folder in the Appliance Products View is created by a so-called plugin for the given appliance product.

With very few exceptions, the term **Product** in the GateManager Console means the same as **Appliance Product**.

Appliance state

In GateManager, this refers to an enrolled Appliance's relationship to the domain in which it is placed:

Tentative

! **New**: An Appliance has presented itself in a recognized domain.

Under the square connection state icon is a red exclamation mark.

? **Unrecognized**: An Appliance has presented itself in a domain that is unrecognized by the GateManager, or in a domain that does not have the necessary product binding for the type of Appliance.

Under the square connection state icon is a red question mark.

Attached

Both New and Unrecognized Appliances need to have their domain placement confirmed. You can drag the Appliance to the desired domain or right-click on the Appliance and select **Attach Appliance to Domain** from the context menu.

There is no exclamation mark or question mark under the square connection state icon.

- **IMPORTANT**:

  When a tentative Appliance becomes attached, its domain placement is confirmed and unchangeable. If you need to move the Appliance, you must first delete it from the Console. Then configure the device, agent or relay with a new domain token, and activate the GateManager connection.

See also connection state.

Appliance status

In GateManager, this is shown for each Appliance in the **General Section** on the **Details** tab. It includes Appliance state, connection state, and a timeout/countdown for how long a controlled disconnection is expected to last before the GateManager considers the connection to be failed.

It also shows whether or not the Appliance has been disabled on the GateManager and includes a button you can use for disabling and enabling an Appliance.

attached

Primary meaning: An attached Appliance has a confirmed, unchangeable placement in a domain. See Appliance state.

Additional meanings

1. Configuration profiles are attached to an Appliance before being applied.
2. Alert rules are attached to individual Appliances.

audit

The **Audit** tab for any given GateManager object is a log of actions taken on the object.

As of GateManager 3.4:

- This **Audit** tabs replaces the old **Events** tabs.
- The **Enrollment Report** tab for any given domain replaces the old **Audit** tab for that domain.

B

backend (GateManager)

The GateManager backend consists of the Server, including application and database, and the Proxy.

C

connection state

In GateManager, once an Appliance has been enrolled, the GateManager Console keeps tracks of the connection. The icons used to identify the connection state were changed in GateManager version 3.7.

The icons are defined on the GateManager server, so if you connect to an older server version, you may still see the old square icons even with a GateManager Console version 3.7 or newer.

Version 3.6 and older	**Version 3.7 and newer**	**Conntion state**
🟩	✓	Connected "green"
🟥	✖	Failed "red"
🟨	▬	Unknown "yellow"
■	▬	Disconnected / controlled disconnect – for devices supposed to be "always online"
■	*None*	Disconnected – for devices that are only connected *on demand*, such as LinkManagers, TrustGate Softclients, etc. the appliance icon itself is "grayed out".
X	✕	Disabled. The GateManager will refuse connection attempts (The Appliance name is greyed out and a big red X is super-imposed)

Console

The GateManager Console is the frontend application used for managing the whole solution (see "The GateManager Console" page 7). Other tools for accessing GateManager include the LinkManager and web services (web services are described in the *Developer's Guide*).

context menu

This is a menu that is tailored to a specific object. The usual way of invoking it is to right-click the object.

D

DNS

DNS stands for Domain Name Server, but it is common to say "DNS server".

A DNS Server is used to convert between a host name and the IP address of the host bearing that host name.

DNS naming restrictions for host names

Naming requirements are dependent on where the particular DNS Server looks up a host name in order to find the current IP address. A host name must be unambiguous in a given environment.

For example, on the Internet, the host name must be an FQDN (Fully Qualified Domain Name), containing at a minimum a hostname, such as **www**, and a two-level domain name, such as **secomea.com**.

In a closed environment, the hostname, or a two-label host name, is usually enough.

Because a host name may need to function in many different types of name spaces, if you are responsible for creating a DNS host name, follow these guidelines as a way of preventing problems:

- Minimum 2 characters.
- Maximum 256 characters unless otherwise specified for a specific configuration.

- The first character in the name must be a letter (preferred) or a digit (allowable in most modern environments).
- Valid characters: letters a-z. DNS servers do not treat a name as case-sensitive, but the name may end up being treated as case-sensitive in another environment. Sticking to lower case letters is safest.
- Valid characters: digits 0-9, and the hyphen/dash (-).
- Period / full stop / dot . can be used - but only as a separator for the labels using the DNS naming rules, for example **www.secomea.com** .
- Some environments may permit underscore (_). The Appliance Launcher utility used for a number of GateManager-enabled products can read a name with _ but you cannot create a new name that includes _.
- Not allowed: any thing else. People are most tempted by spaces, special symbols or extended (international) characters (i.e. above Hex 7E / decimal 126). Don't use them!

domain

Domains are the all-important administrative groupings in GateManager, not only of accounts and of Appliances, but also of alert rules and configuration profiles, which are created in domains before they can be associated with Appliances.

Furthermore, firmware managed in the Appliance Product View can only be used in a domain which includes the appliance product in its Product Bindings.

Domains are grouped into hierarchies. The domain in which an object is created is known as the object's **home domain**.

E

enrollment report

This is the report for any given domain that lists all enrolled Appliances as of the report date, usually used for billing purposes.

Enrolled Appliances are sometimes called activated devices or activated agents in connection with commercial contracts.

The enrollment report was called audit before GateManager 3.4.

F

FQDN

The Fully Qualified DNS Name is an unambiguous host name given to a network device which can be looked up on a DNS Server.

Usually, the term is reserved for names that can be found in the open Internet environment.

Thus, the name must include three labels: a hostname, a second-level domain name, and a top-level domain. such as **com** or **net**.

An FQDN starts with a hostname and continues all the way up to the top-level domain. So there may be more than three labels. For example **www.parc.xerox.com**

Sometimes an FQDN ends with a dot (period) in order to indicate that no suffixes are to be added.

The DNS naming restrictions for host names should be used.

G

GateManager Server

Depending on the context, this phrase has two meanings:

1. The entire GateManager backend, consisting of Server and Proxy.
2. The GateManager Server as opposed to the Proxy.

GTA

Abbreviation for the GateManager function Go to Appliance (sometimes also written as Go To Appliance, Go-to-Appliance, Go-To-Appliance, GoToAppliance).

This function forwards ("proxies") a connection between the GateManager Console and the native management interface of a managed Appliance.

H

heartbeat

The heartbeat is a package of information about Appliance identity and status. (Appliance - with capital A stands for what is in the GateManager database).

When a heartbeat is sent	**Comments**
Appliance initiates connection	The initial heartbeat from an Appliance finds the GateManager and establishes or renews the connection, or establishes a new connection e.g. after having been turned off and powered on again.
Normal automatic heartbeat	The GateManager is configured to periodically request a heartbeat from each Appliance.The heartbeat interval is set in **Domain Preferences** on the **Details** tab for the Appliance's home domain.
State change	Sending a heartbeat can be triggered by an Appliance state change.
On request	You can **request** a heartbeat manually from the **Details** tab for a selected Appliance in the **Heartbeat** block.
After you delete an Appliance from the database	If you delete an Appliance from the database and do not want it to keep re-enrolling itself, you must de-activate GateManager in the product.
See also Fallback heartbeat.	

When a heartbeat is *not* sent	**Comments**
Appliance is disabled from Console	The effect of disabling an Appliance from the Console is that no more heartbeats are responded to. The Appliance will still keep sending heartbeats every 3 to 30 minutes, depending on the product. After the Appliance is enabled on the Console, if you don't want to wait for the automatic connection, you can usually do something to provoke a new connection. Some products require a reboot, others require that you deactivate GateManager and save, then activate GateManager and save - see the product documentation for details.

host name

This is a term that can be ambiguous. We try to use it in the following way:

A host name has at least two labels.

- hostname (the single host)
- information about the domain the host is placed in

Examples:

mypc.ourdomain

www.ourdomain.org

In order to save space, our field texts read hostname; your network environment may require a full host name.

See also FQDN.

hostname

The name of a single computer (a host) on a network.

See also host name; FQDN; DNS naming restrictions for host names.

J

joined account

An account is said to be joined to a domain when the user of that account is able to access the appliances in that specific domain, which is located outside the normal tree-based domain structure accessible to that user.

Notice that only specific domains are joined - the access rights do not recurse to deeper levels in the tree.

joined domain

A domain is said to be joined to an account – when the account is joined to the domain; this is simply two different views on the same association between an account and a domain.

O

object

The system is built up so that you can create and manage seven major objects.

The GateManager GUI is organized with a View for each type of object:

The primary objects are: **Domains**, **Accounts** (users), and **Appliances**.

Domains create the hierarchy for grouping and managing Appliances and accounts. Each Appliance and each account must be attached to a domain.

Two secondary objects, **Alert Rules** and **Configuration Profiles**, must be created in a home domain. Then they are attached to individual Appliances in the domain.

These five objects are **domain-centric**.

Two secondary objects, **Appliance Products** and **Roles**, are **system-wide**, and are usually only managed by the highest level administrator for the GateManager.

- **Appliance Products** are the various types ofGateManager-enabled products. In order to be visible within a domain, an appliance product must be attached to the domain as a product binding.
- **Roles** are collections of privileges – access rights – for accounts.

Owner

This term refers to the person or authority with the highest legal responsibility for a GateManager installation. Many Owner tasks can be delegated.

For example, an Owner might not install the GateManager on the server (operations), set the server up, or design a network (infrastructure). However, he or she *is* responsible for ensuring that others coordinate these activities across the entire remote device management solution.

For example, an Owner might not be a top level (ROOT) administrator on the system (with the access role "Owner"), but he or she *is* responsible for making sure that a properly trained and authorized ROOT administrator is able to administrate roles and accounts in a secure manner.

P

product

In the GateManager GUI, the term **Product** means **Appliance Product**.

The only exception is in the Specific Section describing an individual TrustGate VPN/firewall appliance: here, the Product refers to specific types of TrustGates, such as the TrustGate 5 and the TrustGate 363R.

R

red domain

Red domain / failed domain: In the **Appliances View**, Tree pane, if the domain name is red, the domain houses one or more *failed* Appliances. The Details tab for the Domain will show Domain Status as Failed, with Failed in red letters. This information is not affected by the possible failure of Appliances in subdomains.

S

superior administrator

The domain hierarchy controls access rights. Sometimes you will need to consult **an administrator higher up in the hierarchy** to help you find "lost" objects or to determine if you need changes to the role given to your account.

21. Notices

Publication and copyright

GateManager - Administrator's Guide Version 4.0, 2009-04-21

You may download and print a copy for your own use. As a high-level administrator, you may use whatever you like from the contents of this document to create your own instructions for deploying our products. Otherwise, no part of this document may be copied or reproduced in any way, without the written consent of Secomea A/S. We would appreciate getting a copy of the material you produce in order to make our own material better and – if you give us permission – to inspire other users.

Trademarks

GateManager™, SiteManager™, PlantManager™ and LinkManager™ are trademarks of Secomea A/S. Other product names may be trademarks of their respective owners.

Disclaimer

Secomea A/S reserves the right to make changes to this document and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S.

Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we can not guarantee that there are none.

The following paragraphs do not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S

www.secomea.com