NovaTec Kommunikationstechnik GmbH

User Manual

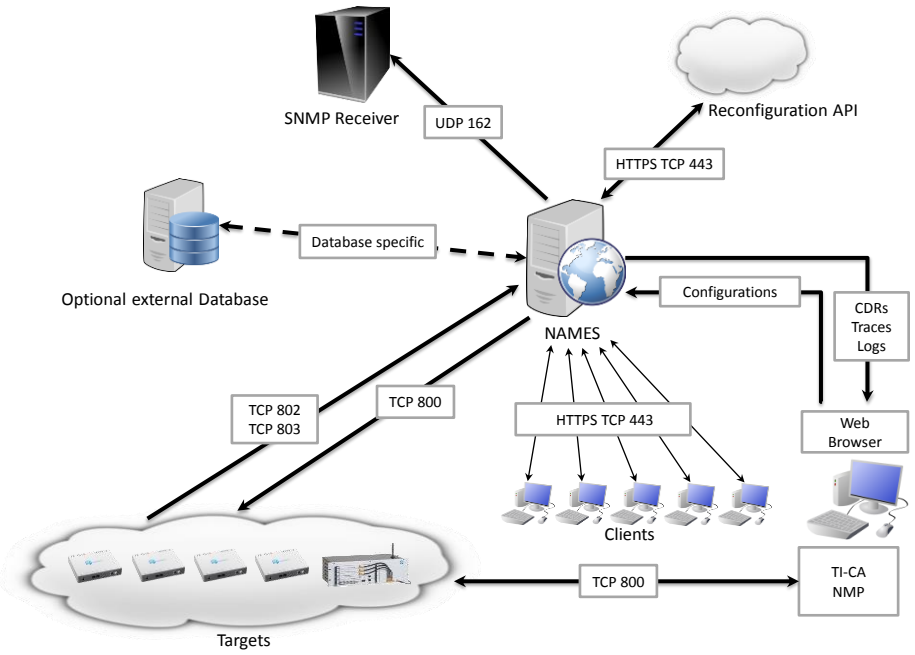
NAMES 2.0

Doc-ID	**DB.NAMESMAN--.NT**
Version	0.1
Datum	02.10.2014
Status	Final

CONTENT

1 Introduction

The NovaTec Administration and Management Element Server (NAMES) allows you to manage all your NovaTec devices through a central service. It contains functions to assist you with deployment, maintenance, configuration and monitoring. The following image shows NAMES in a typical deployment:



NAMES can and should be used as the central administrative element for any non-trivial installation of NovaTec devices. Currently additional tools (the NovaTec Maintenance Package, consisting of the NovaTec Trace Info Client, NovaTec Configuration utility and NovaTec Call Server) are required for certain functionalities and are therefore included in the overview above as installed on the client PCs.

2 System requirements

2.1 NAMES execution environment

NAMES is intended to run on physical or virtual servers under a Windows Server operating system. As NAMES is implemented in Java, a Java Runtime Environment is required.

2.1.1 Minimum specifications

At a minimum, the following specifications are necessary to run NAMES:

- 256 MB of free memory,
- 2 CPU cores,
- 256 MB of disk space,
- Windows Server 2008 R2 Standard Edition SP1,
- Oracle Java SE 7 64-bit Runtime Environment, latest update,
- Oracle Java 7 Unlimited Strength Jurisdiction Policy Files.

With these specifications, only a small number of devices (up to about 10) can be administered. A short deletion interval must be used if automatically retrieving CDRs from the devices, as these can quickly fill up hard drive space, depending on the call volume.

2.1.2 Recommended specifications

The following specifications are recommended for small to medium installations (up to about 50 devices):

- 512 MB of free memory,
- 4 CPU cores,
- 1 GB of disk space,
- NTP time synchronisation.

Larger installations require additional resources and should be sized according to specific requirements.

2.2 Database server

NAMES will use an embedded database by default. However, the use of an external database is possible and may offer advantages with regard to availability and backup planning. NAMES supports the following external databases:

- Oracle DB 11g,
- MySQL 5.5.

If using Oracle, it is recommended to configure a Unicode character set.

2.3 Compatible NovaTec products

NAMES must be used in conjunction with specific versions of NovaTec hardware, firmware and PC utilities. Following versions may be used with NAMES 2.0:

- Hardware: S3, CCU3, CCU4,
- Firmware: 00.08.03.xx,
- NMP: 7.3.x,
- TI-CA: 1.6.0.2.

Please be advised: simultaneous use of the configuration upload capabilities of NAMES and NovaTec Configuration (part of NMP) in the same network is **not** supported. When using NAMES, configurations should be edited in the NovaTec Configuration utility and then transferred to NAMES. The upload of the configuration to the device can be done through NAMES, thereby ensuring that all configurations are managed in NAMES, and that NAMES has correct information about which configuration is currently active on a device.

2.4 Compatible client software

The NAMES web user interface was tested with Microsoft Internet Explorer 9. The web framework in use claims to support all relevant modern desktop browsers and spot checks have shown no contrary evidence; however, extensive testing has not been done. While NovaTec welcomes bug reports for non-Microsoft browsers, fixes will at best be provided on a best-effort basis and support may be unavailable.

2.5 Network configuration

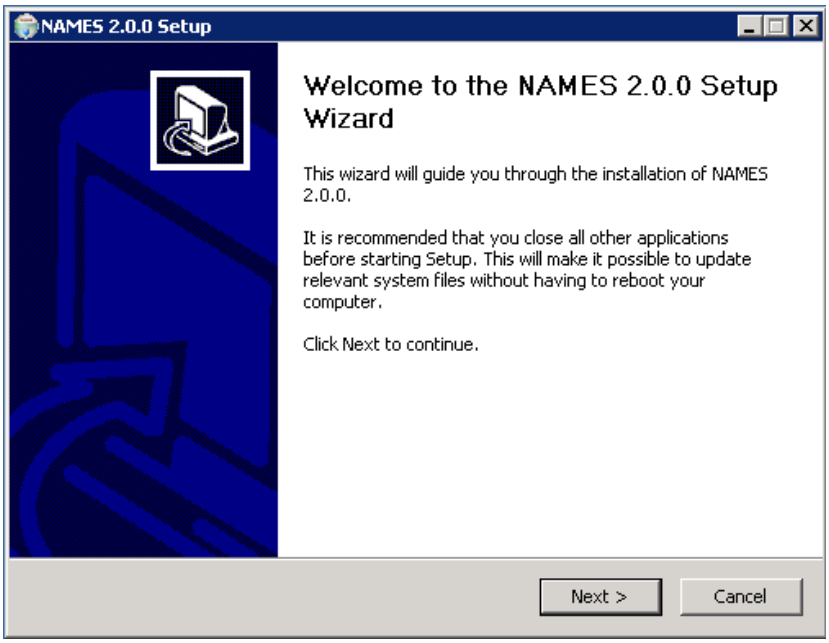
NAMES makes extensive use of network communication. This means that for correct operation, the required connections must be able to be established, and bandwidth may become a limitation, especially in installations with many devices.

All ports can be configured freely, however it is generally recommended to use the default ports, if possible. For details about default port numbers and connections, please see the document "IP Port Matrix" available from the Download section of our homepage (http://www.novatec.de/cms/en/Downloads/Downloadarea.html).

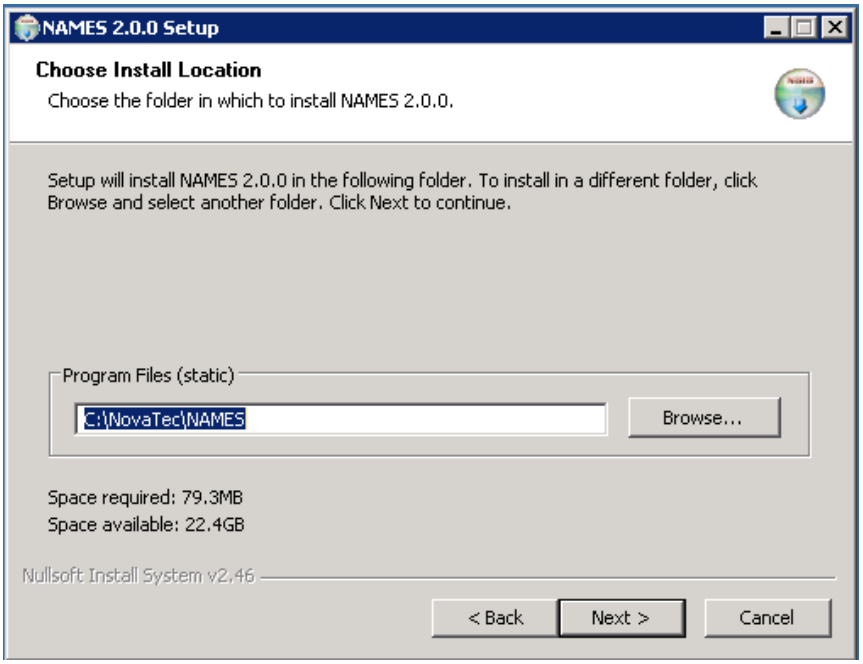
3 Installation

3.1 Running the installer

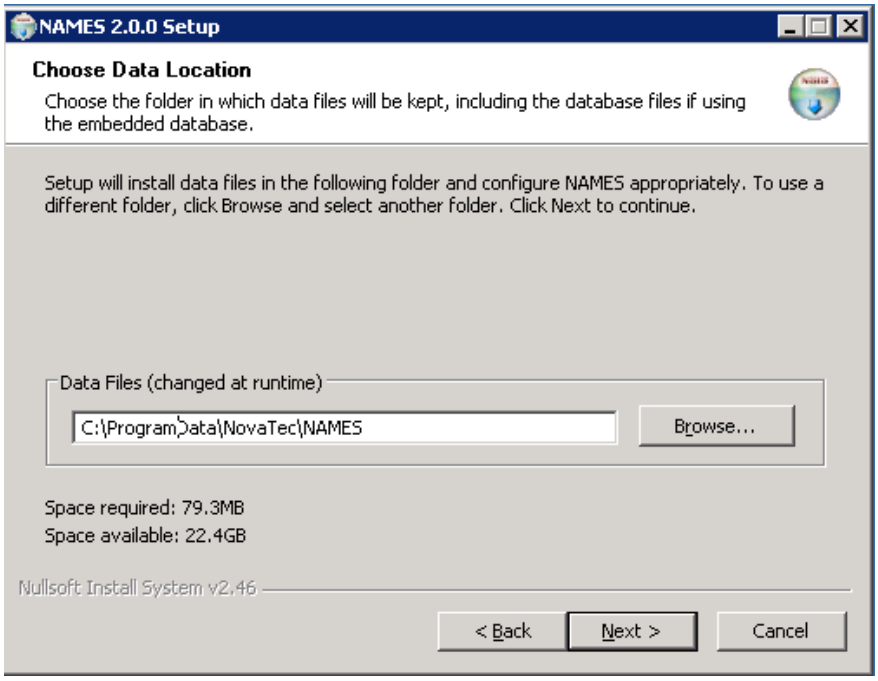
To install NAMES begin by running the provided installer file. The following dialogue box appears:



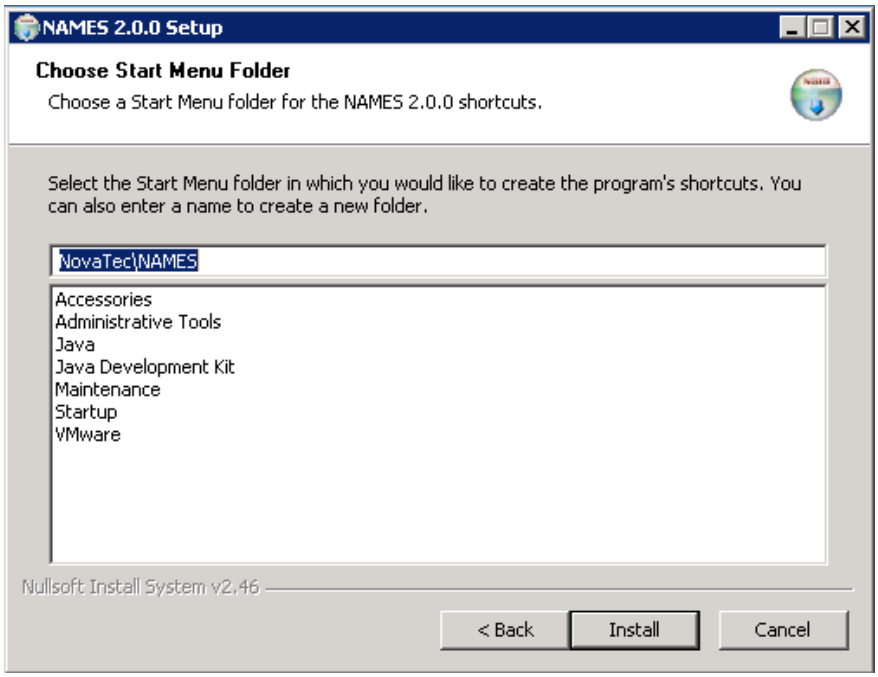
After selecting "Next" choose the installation folder for NAMES.



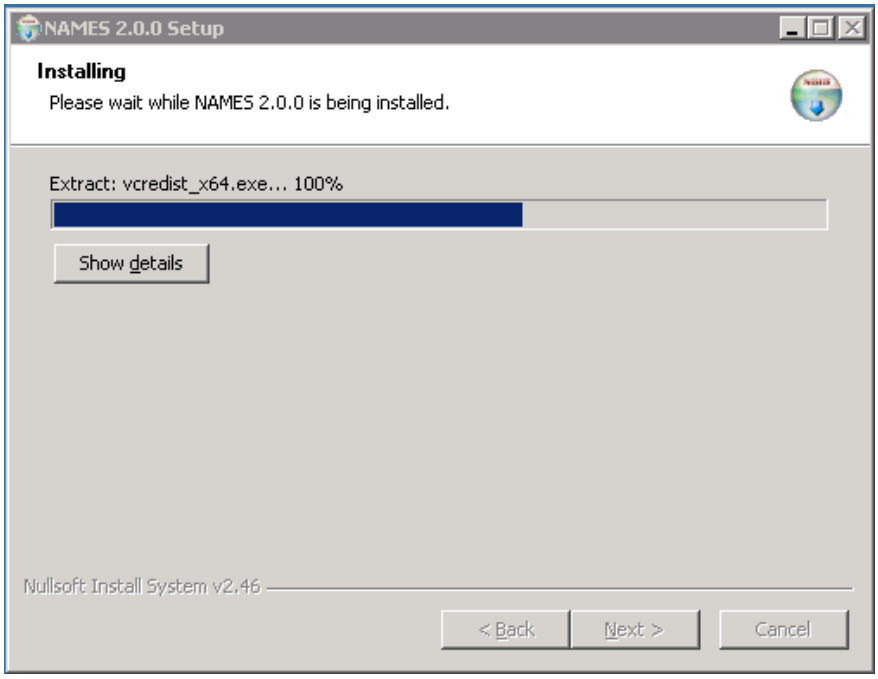
Files that normally don't change during the operation of NAMES are placed into the installation folder, like executables, libraries, resources and configuration files. Files that may change during operation, like the embedded database files and logs, are placed in the data folder, which can be configured on the next page:



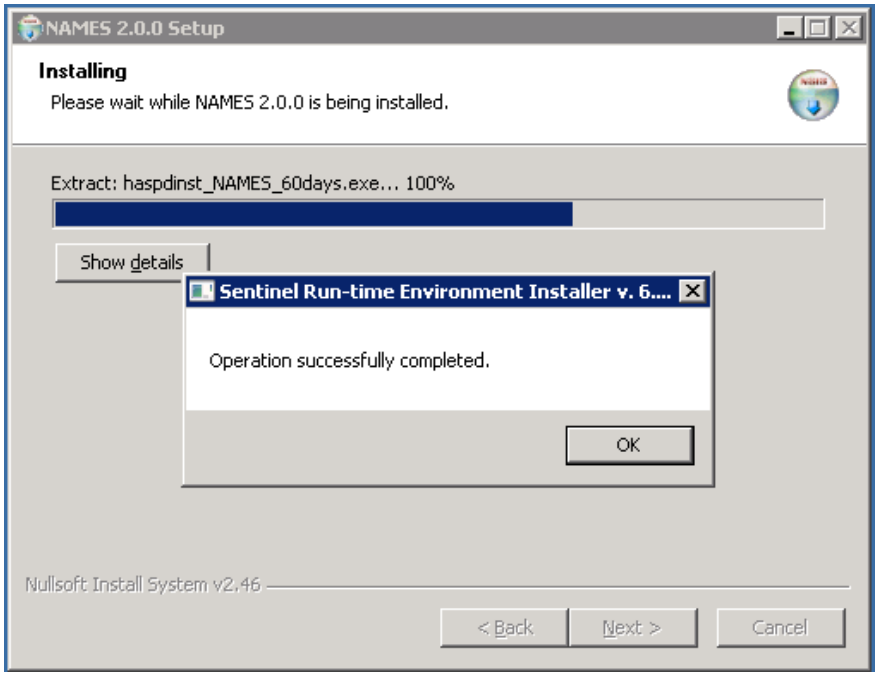
After configuring the folders for program and data files, you choose the start menu folder:



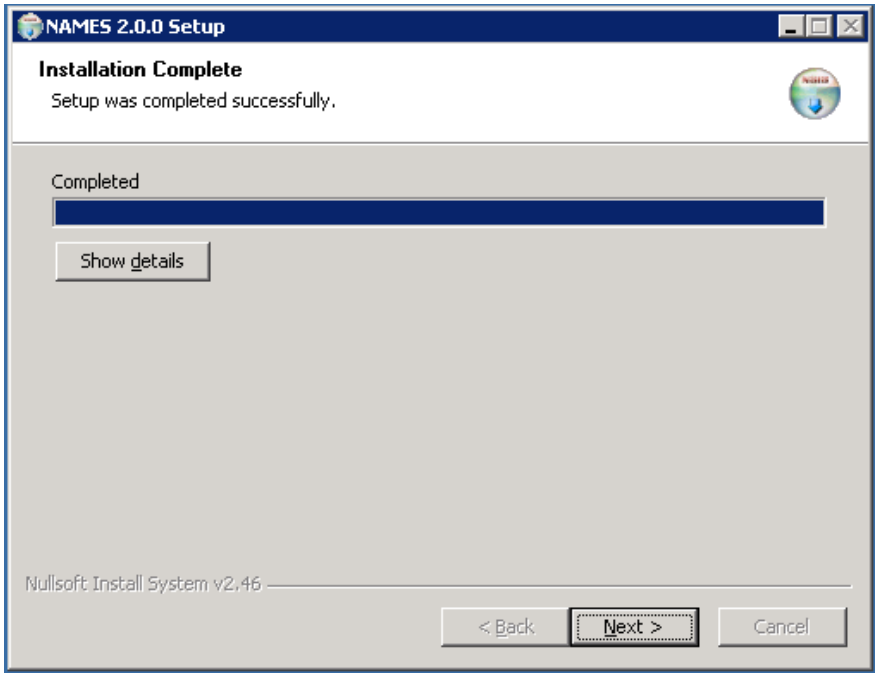
This is the final step before the installation starts, so ensure all settings are correct before clicking "Install". The installer will proceed to complete the necessary installation steps, including installation of a Microsoft Visual C++ Redistributable and the licencing files, including an evaluation licence.



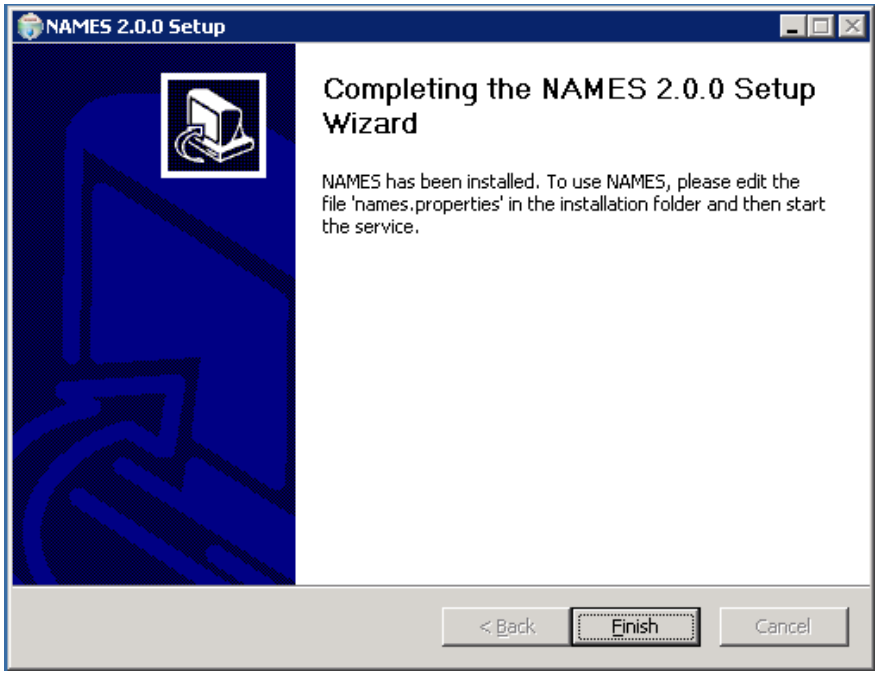
The installation of the licencing mechanism will require a separate acknowledgement:



After clicking "OK" the installation will complete.



Clicking "Next" takes you to the final screen of the installer that describes which steps need to be taken next.



If you wish to use the embedded database and do not want to use HTTPS to access the web UI, NAMES is ready to use. You can manually start the service from the Windows service management UI (see section 5.1) or restart the system. After every system restart, NAMES will start automatically.

3.2 Licence installation

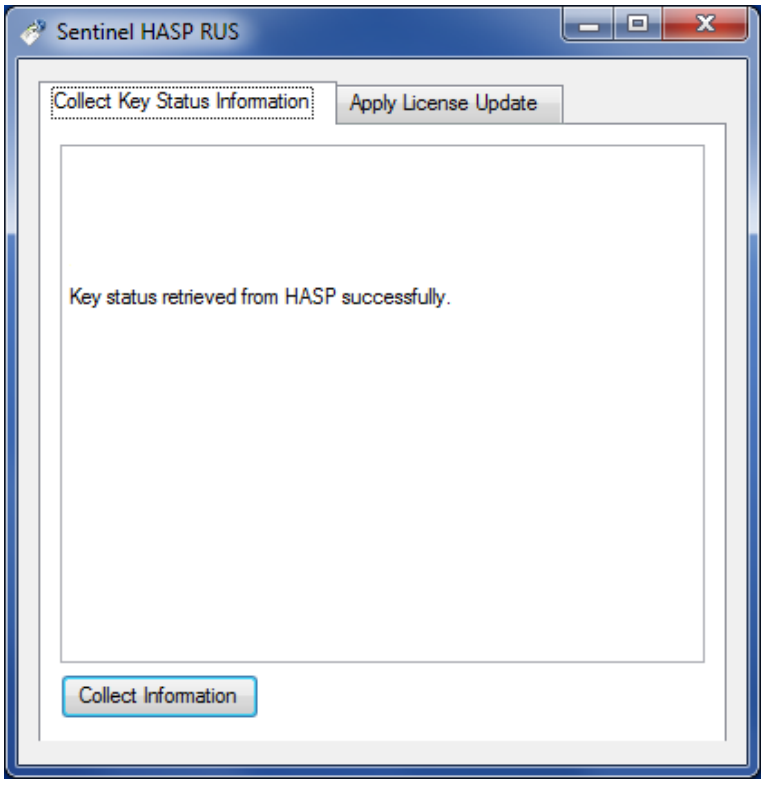
NAMES is installed with a 60-day evaluation licence. Apart from the limited evaluation period, this licence also contains other limitations, such as the number of devices that can be managed. For production use, a perpetual licence has to be installed.

The licencing system in use requires the user to use a licencing tool to collect certain system information into a file, which must then be sent to NovaTec e.g. via email. The information contained in the file is used to create an individualised licence, which is sent back to the client who then has to install it using the same tool.

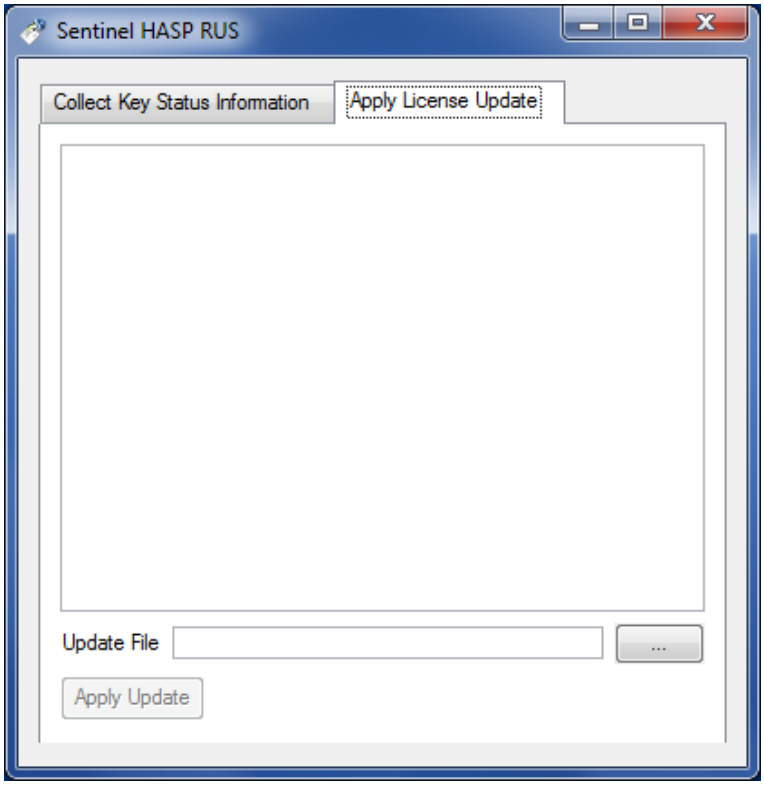
The process is as follows:

1. Run the application "NAMES License Tool" in the NAMES installation folder. A window with two tabs will appear. The first tab, which is selected by default, allows you to collect the licence information.
2. Click the 

button and then select a location and name for the generated system information file. The tool will inform you that the key status was successfully retrieved:



3. Send the generated file (e.g. info.c2v) to your sales contact at NovaTec with the order number for your NAMES licence purchase. If you have not purchased a NAMES licence yet, contact a sales representative for licencing terms.
4. NovaTec will generate a licence file (e.g. customer.v2c) and return it to you.
5. Run the "NAMES License Tool" again. This time, select the second tab which allows you to apply the licence file:



6. Click the ... button. A file selection dialogue will open, allowing you to select the file with the licence information sent to you by NovaTec.
7. Finally, click the Apply Update button. The licence is now installed and ready to be used. If NAMES is running, restart NAMES to load the new licence information.

3.3 Database initialisation

If using an external database, the database structure (tables and some basic database rows) must be imported. If using the embedded database, this step is not required, as the installed database comes prepared with this structure.

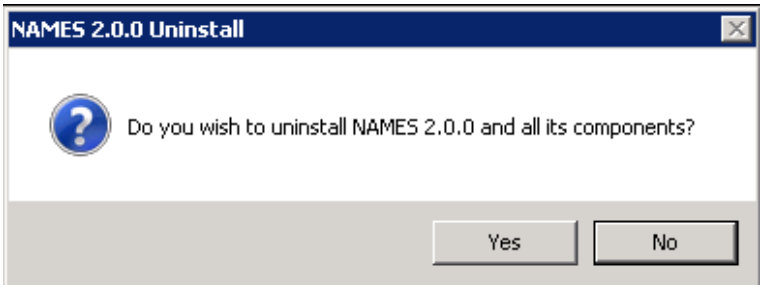
The NAMES installation folder contains two SQL scripts for the two supported external database systems. Select the file appropriate to the database in use (either names-oracle.sql for Oracle DB 11g or names-mysql.sql for MySQL 5.5) and import it into the schema (Oracle) or database (MySQL) that you wish to use for NAMES.

For security reasons, it is recommended to use a separate database user for NAMES. This database user should have all permissions on the corresponding schema/database, except table create/drop privileges, as these are not required for normal operation. Database import operations, and later database upgrades, where necessary when upgrading NAMES, can be carried out with a privileged user that can create, alter and drop tables.

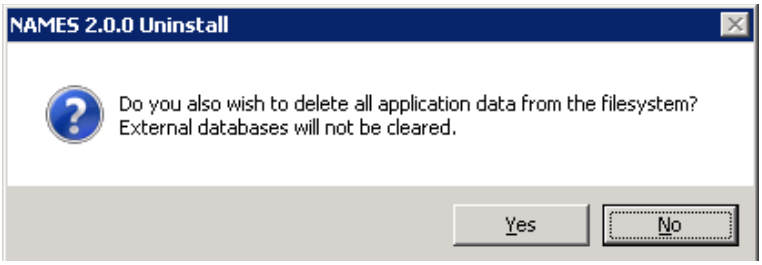
After setting up the database, the correct connection information must be provided to NAMES. See section 4.1.1 for further information about configuring NAMES database connectivity.

3.4 Uninstalling

If required, NAMES can be uninstalled by selecting the "Uninstall" option from the "Start Menu" folder selected or created during installation (default: NovaTec\NAMES). After starting the uninstaller, you are first prompted to confirm that you really wish to uninstall NAMES:



After selecting "Yes", the uninstaller will ask you whether you also wish to remove the data folder, which contains logs, templates and the embedded database, which, if in use, will contain all NAMES runtime data such as configured targets, system configurations etc.. These files will be irrevocably deleted if you select "Yes", so ensure that you have made a backup of these files if you wish to have access to the data at a later point of time:



The uninstaller also reminds you that, should you be using an external database, you will need to drop any data from this database manually. The uninstaller will then proceed to remove the installed files, services, registry settings and shortcuts from the system. Should any files remain in the installation folder (user created files such as Java key stores, backup copies of configuration files etc.) after the uninstallation is completed, the uninstaller will list them and ask you whether you want these files to be removed as well.

After successfully removing NAMES from the system, the uninstaller will show a confirmation screen:

The uninstallation has now been completed.

4 Configuration

4.1 NAMES configuration file

The main configuration file for NAMES is the file `names.properties` in the installation folder (default: C:\Program Files\NovaTec\NAMES). This file contains configuration settings for the NAMES database, for the embedded web server and for the Java Runtime Environment, as well as some other important start up settings.

The configuration file contains extensive commentary, including the default settings for each setting.

4.1.1 Database configuration

If using the embedded database (the default), no further configuration is necessary. To switch back to the embedded database after using an external database, simply comment out all the database configuration directives by prefixing them with a hash mark (#).

To use an external database, the correct connection settings for the database in use must be made. To do this, uncomment the corresponding lines and replace the default setting with the setting you want to change it to.

4.1.1.1 Oracle DB 11g

To configure the Oracle DB 11g connection, make the following configuration settings:

```
database_type = oracle
database_url = jdbc:oracle:thin:@<Hostname/Address>:<Port>:<System Identifier>
database_username = <Username>
database_password = <Password>
database_schema = <Schema>
```

Replace the placeholder text in above example with the corresponding information for your Oracle database. For example, if you are running a database on the server with the hostname `oracle` on the port `1521` with the System Identifier (SID) `ORCL`, and you have prepared a user with the name `names` and password `secret`, using their own schema, configuration should be as follows:

```
database_type = oracle
database_url = jdbc:oracle:thin:@oracle:1521:ORCL
database_username = names
database_password = secret
database_schema = NAMES
```

NAMES will automatically transform the schema name into uppercase internally, as required by Oracle DB 11g. You may therefore also enter the schema name in lowercase, however entering it in uppercase is recommended for consistency.

4.1.1.2 MySQL 5.5

To configure the MySQL 5.5 connection, make the following configuration settings:

```
database_type = mysql
database_url = jdbc:mysql://<Hostname/Address>:<Port>/<Database>
database_username = <Username>
database_password = <Password>
database_schema = <Database>
```

Replace the placeholder text in above example with the corresponding information for your MySQL database. Please note that MySQL uses the terms "database" and "schema" interchangeably. For example, if you are running a database on the server with the hostname `mysql` on the port `3306`, have created a database with the name `namesdb` and prepared a user with name `names` and password `secret` and read/write access to this database, configuration should be as follows:

```
database_type = mysql
database_url = jdbc:mysql://mysql:3306/namesdb
database_username = names
database_password = secret
database_schema = namesdb
```

4.1.2 Web server configuration

The embedded web server need not be configured if you wish to run it in the default unsecured HTTP mode on the default port of `80`. If you wish to enable HTTPS or use a non-standard port, you have to configure the webserver.

4.1.2.1 Changing the listen port

If you simply wish to change the port used for incoming connections from the default `80`, make the following setting:

```
webserver.port = <Port>
```

Replace `<Port>` with the port number you wish to use. Setting the port to `0` will cause NAMES to use the default port, depending on whether HTTPS is configured or not.

NAMES will listen on all available network interfaces.

4.1.2.2 Using secure mode (HTTPS)

In order to secure the web UI of NAMES, you must first generate a pair of keys and acquire a certificate for your webserver. The key and certificate must then be placed in a Java key store with the name `keystore.jks`, while the root certificate of the issuing PKI as well as any other trusted root certificates must be placed in a key store with the name `truststore.jks` in the NAMES installation folder.

How to generate the key and acquire the certificates depends on your PKI and security policies and is beyond the scope of this document. If in doubt, please consult with your resident security expert.

The key stores may be created and populated with any appropriate tool, including the Java key tool contained in the standard JRE distribution and graphical tools such as the free KeyStore Explorer. When importing the private key, ensure that the password for the key and the key store password are identical and that only one key and certificate pair is contained in the key store.

Once the `keystore.jks` and `truststore.jks` files have been placed in the installation folder make the following settings:

```
webserver.secure = 1
webserver.keystore_password = <keystore.jks Password>
webserver.truststore_password = <truststore.jks Password>
```

The NAMES web server will now run on port `443` by default, which is the well-known port for HTTPS. If you wish to use a non-standard port instead, configure a different port as described above.

4.1.3 Miscellaneous configuration

4.1.3.1 Storage path

The storage path is the path to the data folder. During installation, this is automatically set to the path you selected; changing this is only necessary if you decide to move your data folder. To move your data folder, stop the NAMES service, move the data folder to its new location, set the `storage_path` setting to the new location and restart NAMES.

4.1.3.2 Maximum Java heap size

Depending on the size of your installation and how you use NAMES, a large amount of memory may be required. By default, the maximum heap size of NAMES is limited to 512 MB, which is sufficient for most small to medium installations, but may cause out-of-memory conditions for certain memory-intensive operations (mainly XML imports with embedded base64-encoded binaries such as configurations, firmware etc.).

To allow NAMES to use more memory, change the `memsize` setting. For example, to allow NAMES to use up to 1GB of Java heap memory, make the following setting:

```
memsize = 1G
```

Note that the actual Java process size will exceed the configured limit, as memory for other parts of the Java virtual machine is also needed; the heap size is the main determining factor for the Java process size. NAMES will normally start with a lower process size, but will grow, possibly up to the limit, during use.

4.1.3.3 Target monitoring alert time

NAMES monitors the target systems using regular time events sent by the systems. You can configure how many time events a system is allowed to miss before it is considered offline and an SNMP trap is generated. It is recommended to set this to two or even three, as time events may be delayed on occasion. To configure the maximum number of missed time events, make the following setting:

```
max_missed_timeevents = <Number of Max Missed Time Events>
```

4.2 Logging configuration file

Configuration for the logging system (`log4j`) is stored in the file `log4j.properties`. The settings in this file apply to the NAMES error and debugging log as well as the accounting log. It is possible to configure log levels for various NAMES components as well as which appenders (log sinks; anything from a simple file appender through to a remote logging server) these logs should be sent to.

In default post-installation configuration, all modules are set to log level "WARN" and full accounting logs are active. The log files `names-log4j.log` and `accounting.log` in the subfolder `log` of the NAMES data folder, as chosen during installation, are used as output.

For more complex configurations, please refer to `log4j` documentation or consult with NovaTec.

Warning: Setting some modules to `DEBUG` or even `TRACE` log levels will produce very large amounts of log information which may slow execution speed to a point where normal operation is not possible. These log levels should only be set if requested by a NovaTec service technician for troubleshooting purposes.

4.3 Firewall settings

If using a firewall on the host on which NAMES is installed (the Windows Firewall is enabled by default) or on another system between the NAMES server and the client PCs, a firewall exception has to be configured. At the least, an exception allowing incoming connections to the configured NAMES web UI port (80 by default) has to be present. Additional firewall exceptions are required for incoming connections to configured CallHome Servers (see section 5.10).

It might also be necessary to configure firewall exceptions for connections originating from NAMES and going to the target devices.

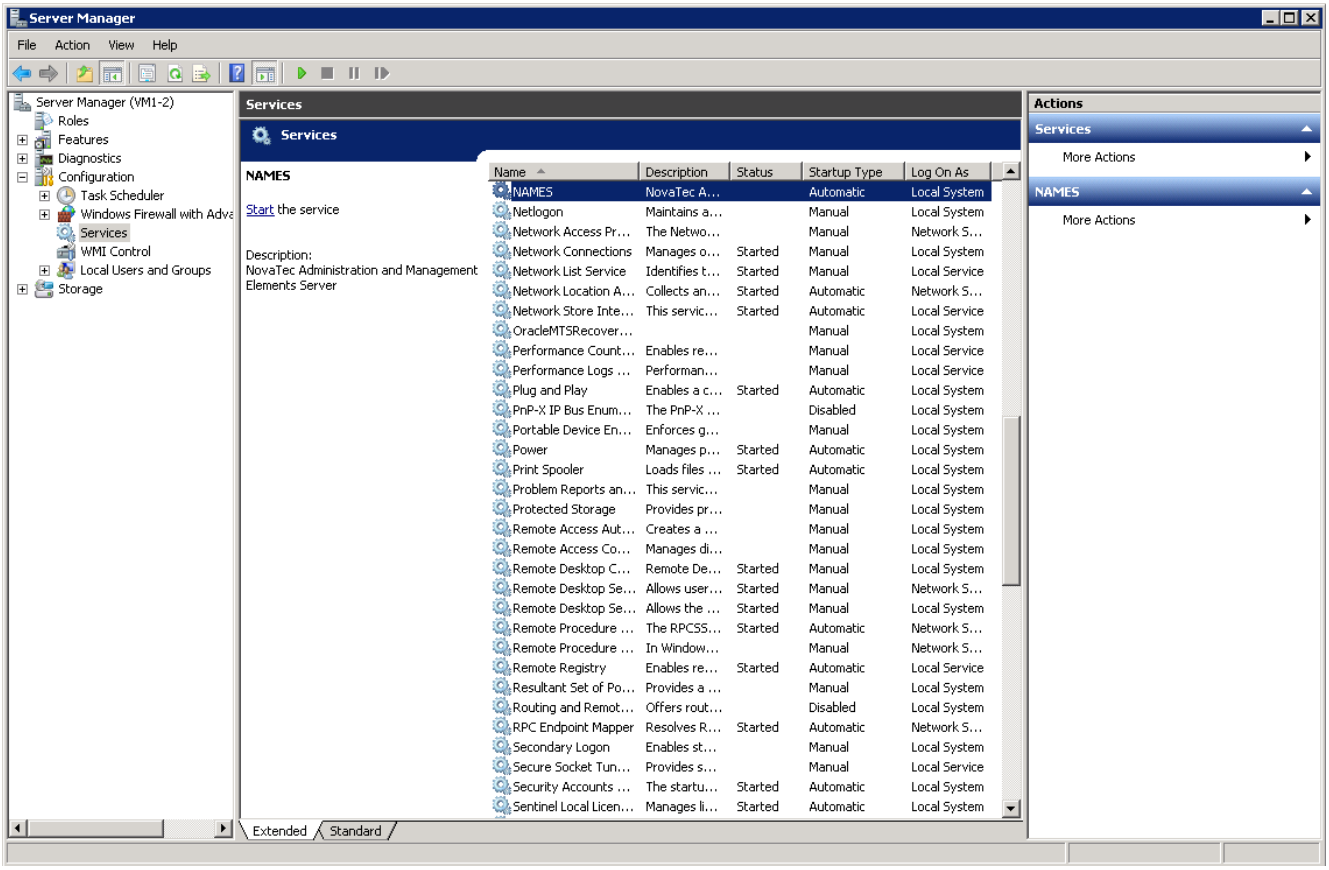
How these exceptions are configured depends on the firewall product(s) you are using and the structure of your network; further explanation is beyond the scope of this document. For default port numbers, please refer to the document "IP Port Matrix", which is available on NovaTec's website under Download/Handbooks (http://www.novatec.de/cms/en/Downloads/Downloadarea.html).

5 Administration

5.1 Starting NAMES

NAMES is installed as a service. This means that it is not started like a normal application, but is managed by the system. During installation, NAMES is configured to run automatically at system start-up, so you will normally not need to explicitly start NAMES. However, if you have just installed NAMES and a condition occurs which prevents NAMES from running (such as the database being unavailable) or you manually shut NAMES down, you will have to start NAMES manually.

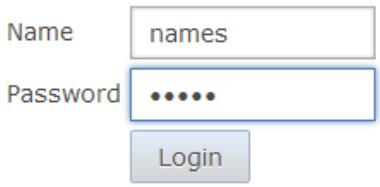
To do this, you should generally use the Server Manager UI, where you can find the item "Services" under "Configuration":



Select the NAMES service from the list and click the "Start" link. Please note that, though the start-up progress window appears only briefly, at that point of time only the Java Virtual Machine has been started, the start-up process of the actual application is still ongoing. It will take a little longer – up to a minute or two – until the NAMES web UI is available.

5.2 First login

To log in to the NAMES web GUI open your browser and navigate to the address where NAMES is installed. You will be asked for your login data:

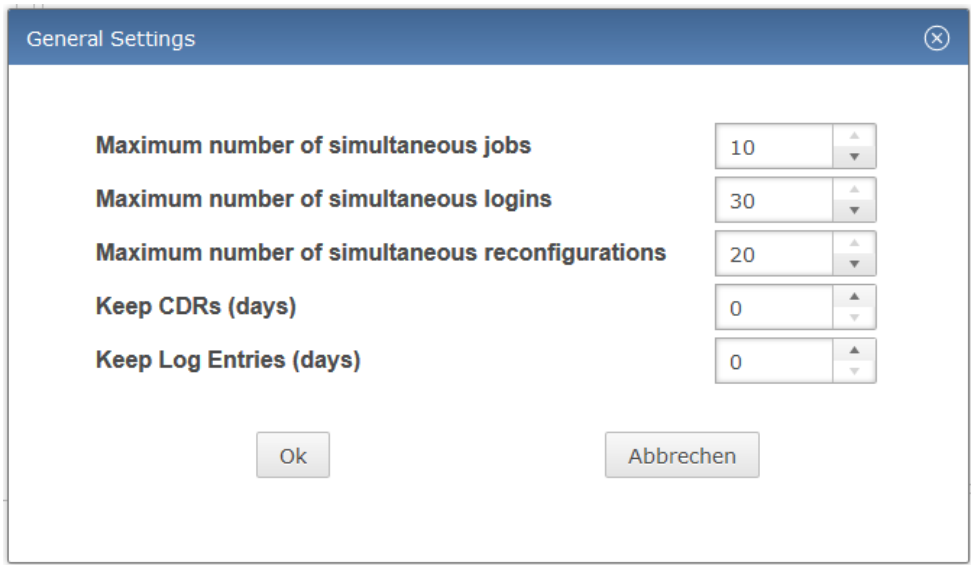


After database installation, a single administrative user with name `names` and password `names` is present. Use this login data when logging in to NAMES for the first time.

After logging in, it is recommended to immediately change the `names` user's password as described in section 6.5 below.

5.3 General settings

In the "General Settings" dialogue, you can set a number of miscellaneous parameters:



5.3.1 Maximum number of simultaneous jobs

This setting specifies how many jobs NAMES may run at the same time. The maximum setting is currently limited to ten simultaneous jobs. You may wish to reduce this if bandwidth limitations lead to poor performance or you want to reduce NAMES bandwidth usage.

5.3.2 Maximum number of simultaneous logins

This setting specifies how many users may use the NAMES web UI at the same time. The default is 30 (the maximum setting available), but it can be reduced if server performance is not sufficient with that number of simultaneous users.

5.3.3 Maximum number of simultaneous reconfigurations

This setting refers to the reconfiguration feature of NAMES, which allows other applications to use NAMES' SOAP interface to reconfigure specific settings on a target. Full documentation on this feature is available by request.

5.3.4 Keep CDRs

This setting controls how long CDRs are kept before being automatically deleted from the database. The default setting is `0`, which means "never delete CDRs". If you are regularly downloading CDRs from your systems, especially if using automated CDR downloads, it is recommended to ensure that CDRs are regularly removed from the database. This may be accomplished through an external mechanism, e.g. if you wish to archive old CDRs, or through NAMES' automated deletion system.

If this setting is set to any number larger than `0`, NAMES will regularly delete any CDRs that are older than this number of days.

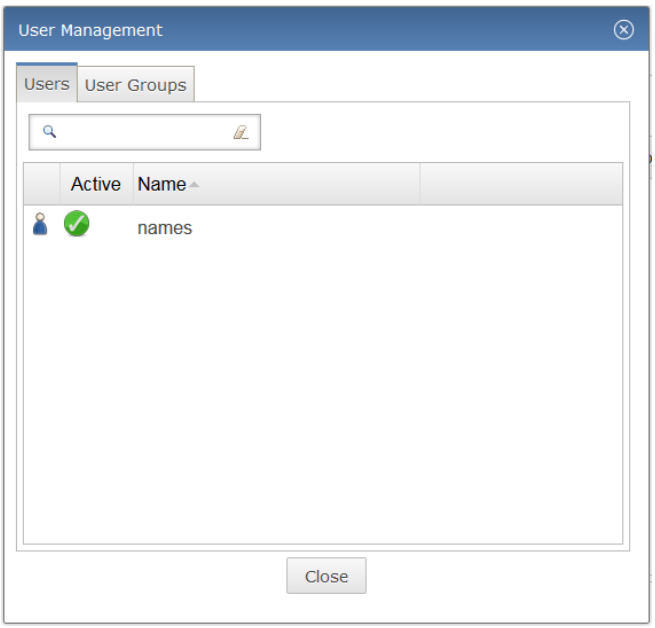
5.3.5 Keep log entries

This setting is the equivalent to "Keep CDRs", except it applies to system logs which have been downloaded from the targets. These logs are saved in the NAMES database and, similarly to CDRs, will need to be deleted on occasion. The default setting is also `0`.

5.4 User management

NAMES has an integrated user management system, which is the base for the AAA (authentication, authorisation and accounting) system. You can create users, assign them to groups, assign roles (more on roles in section 5.5) to users or groups and disable users. Users cannot be deleted or renamed, as this can lead to ambiguity or lack of traceability in the accounting logs.

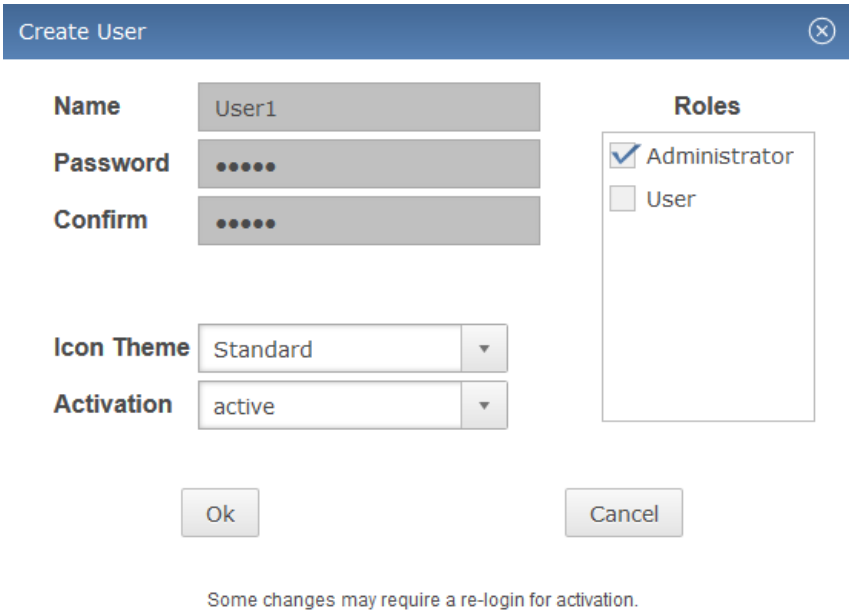
The User Management UI is available from the maintenance menu:



5.4.1 Users

5.4.1.1 Creating a user

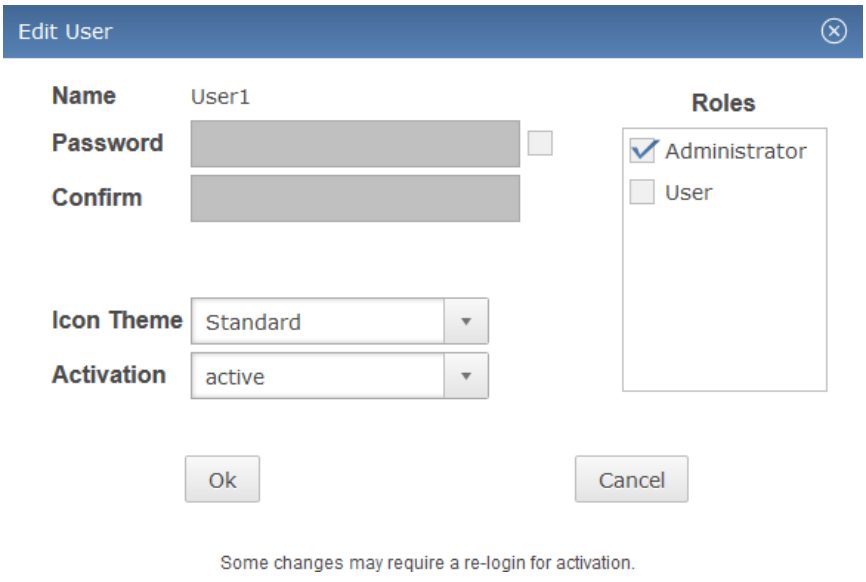
To create a user, right-click in the user table to bring up the context menu, and select “Create”. The user creation dialogue is displayed:



You must enter a user name and initial password for the new user. You can also explicitly assign a role to the user at this stage, though this is not required. Changing the "Activation" setting allows you to create users that are disabled, for example to reserve a certain user name.

5.4.1.2 Editing a user

To edit a user, right-click the user in the User Management UI and select "Edit" from the context menu. The user edit dialogue is displayed:



The user edit dialogue allows an administrator to change all the settings that were previously set in the user creation dialogue. To change a user's password, the checkbox next to the password entry field must be checked. Typing into the password field will automatically check the box. For security reasons, the password field will always be blank when the dialogue loads.

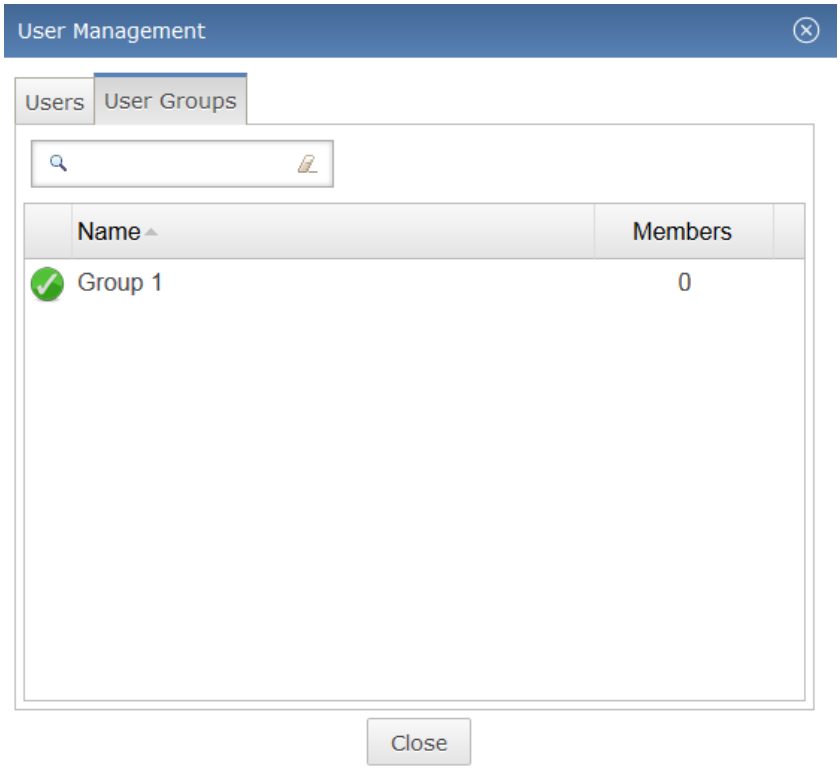
5.4.1.3 Disabling/Enabling a user

Users may be disabled and will then no longer be able to log in to NAMES. This is achieved by editing the user (see 5.4.1.2) and setting the activation status to "inactive". To re-enable the user, set the activation status back to "active".

5.4.2 User groups

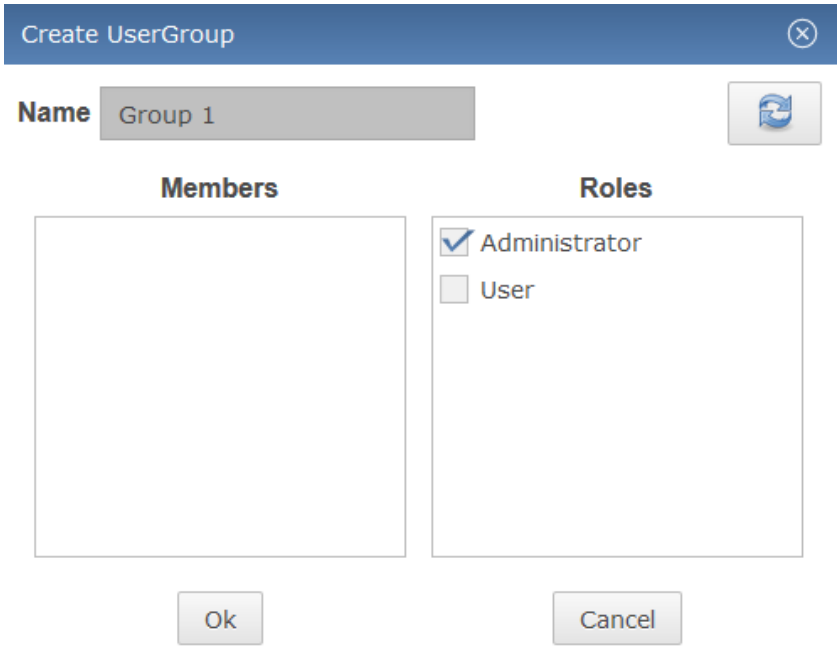
User groups are an entirely optional element of user management. If you wish, you can assign your users to certain user groups. Users will inherit any roles assigned to their groups.

User groups are managed through the User Management UI, which is opened by clicking on "User Management" in the "Maintenance" menu. Switching to the second tab in the User Management UI displays the User Group UI:

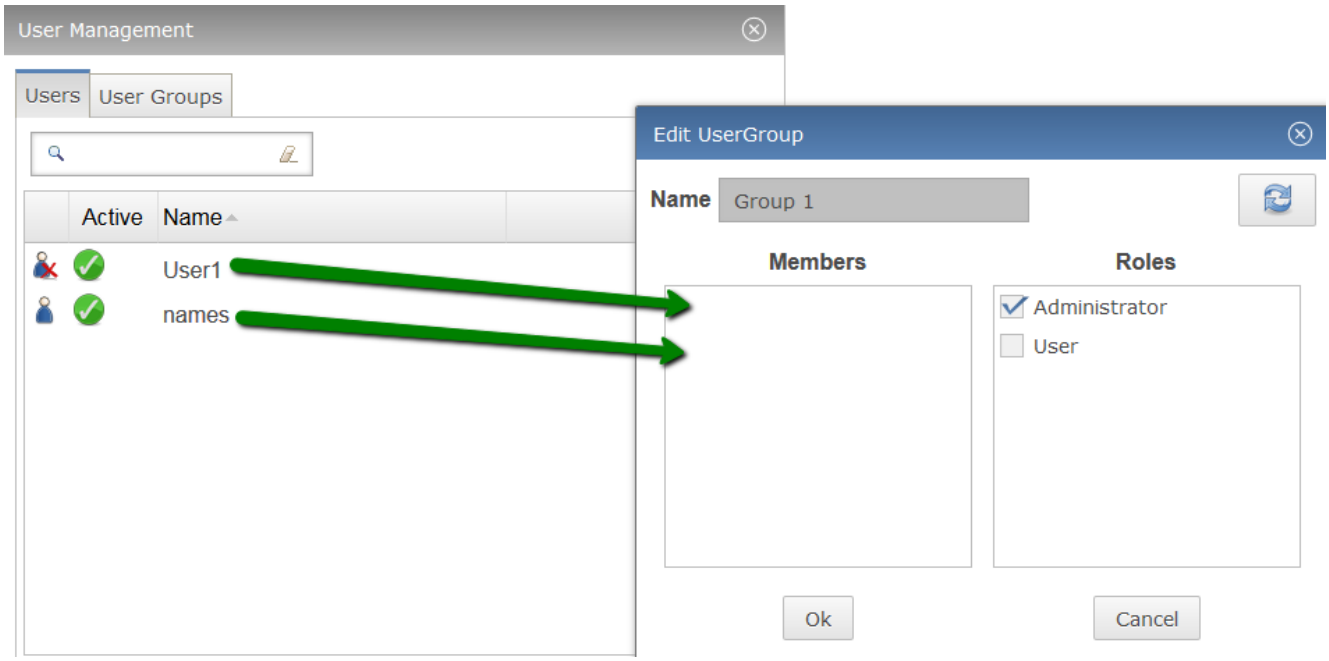


5.4.2.1 Creating a user group

To create a user group, right-click in the user group table and select "Create". The group creation dialogue is displayed:



You must enter a name for the new group. Roles can be assigned as needed. Members can be assigned to the group through drag and drop from the User Management UI:



Click OK to save the group.

5.4.2.2 Editing a user group

The name, members and roles of a user group can be edited by right-clicking the user group in the list and selecting "Edit" from the context menu.

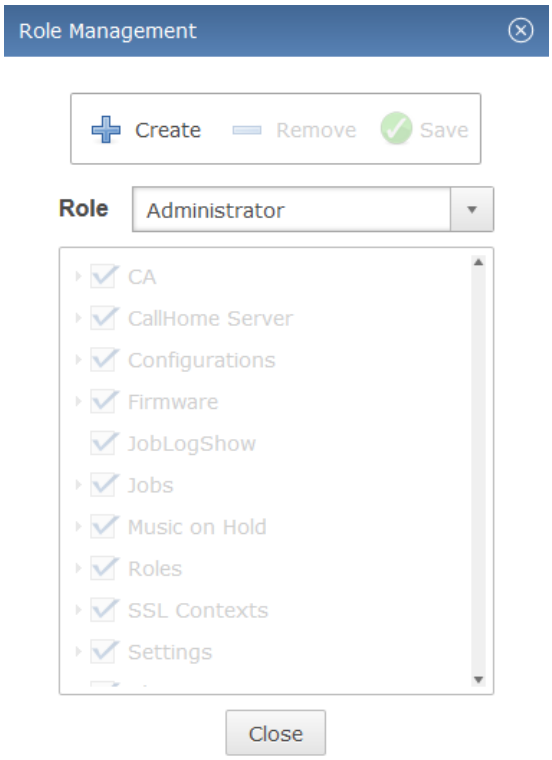
5.4.2.3 Deleting a user group

To delete a user group, right-click the group in the list and select "Delete". You will be prompted to confirm deletion. Once confirmed, any users inheriting roles from the group will lose those roles.

5.5 Role management

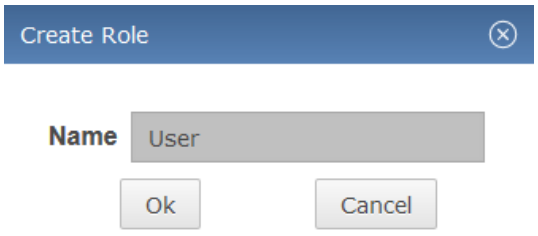
In NAMES, a role is defined as a collection of individual permissions that can be assigned to a user or user group. The default role "Administrator" has all permissions and cannot be deleted. Additional roles with reduced permissions may freely be defined.

To open the Role Management GUI, select "Role Management" from the "Maintenance" menu:



5.5.1 Creating a role

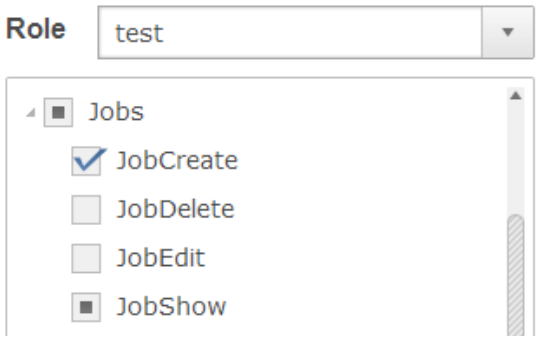
To create a role, click the "Create" button. The role creation dialogue is displayed:



Enter a name for the role and click "OK". The role is created.

5.5.2 Assigning permissions to a role

To assign permissions to a role, select the role you wish to modify from the "Role" combo box. The currently assigned permissions are displayed in a tree structure, with different permissions (create, read, update, delete) for the same object type collected under a common heading:



The checkboxes are tri-state, and the meaning differs slightly between permissions and group headings:

 The permission is not granted / no permissions are granted.

 The permission is granted / all permissions are granted.

 The permission is implicitly granted / some permissions are granted.

Implicit permissions result when a permission that is explicitly granted requires another permission to work properly. In the above example, to be able to create a job, you must also be able to view the job list.

After adjusting the permissions as required, click the "Save" button to persist your changes.

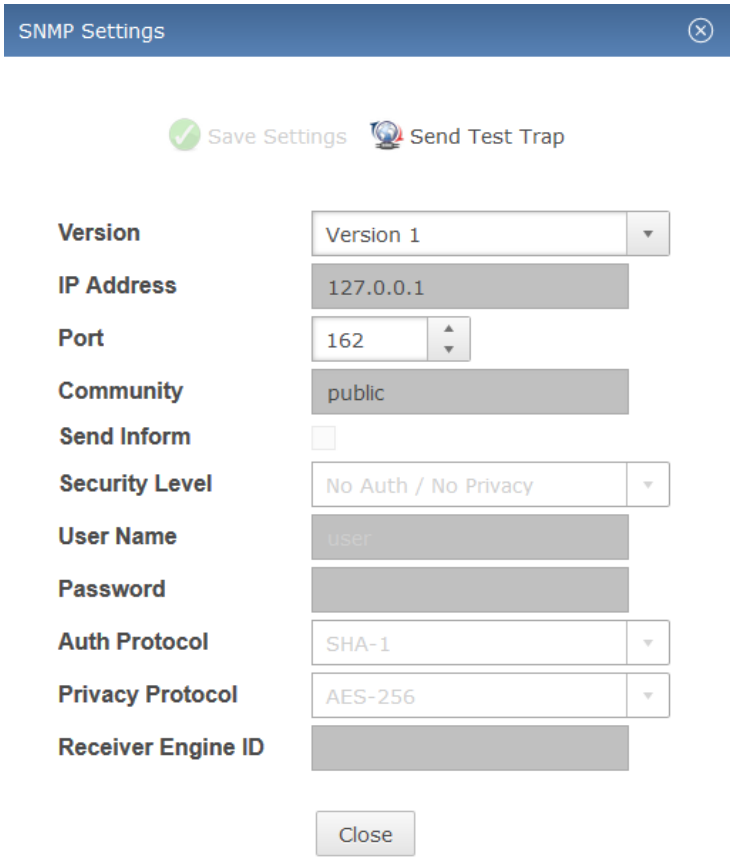
5.5.3 Deleting a role

To delete a role, select the role you wish to remove from the combo box and click the "Remove" button. You will be prompted to confirm the deletion.

5.6 SNMP configuration

NAMES can send SNMP traps/notifications to a network monitoring tool to alert you about various events and conditions, ranging from NAMES start up and shutdown through loss of database connectivity to various target events (CallHome Events) which are mapped to SNMP.

In order to send SNMP traps to your monitoring tool, the correct settings must be configured in the "SNMP Configuration" dialogue available from the "Maintenance" menu:

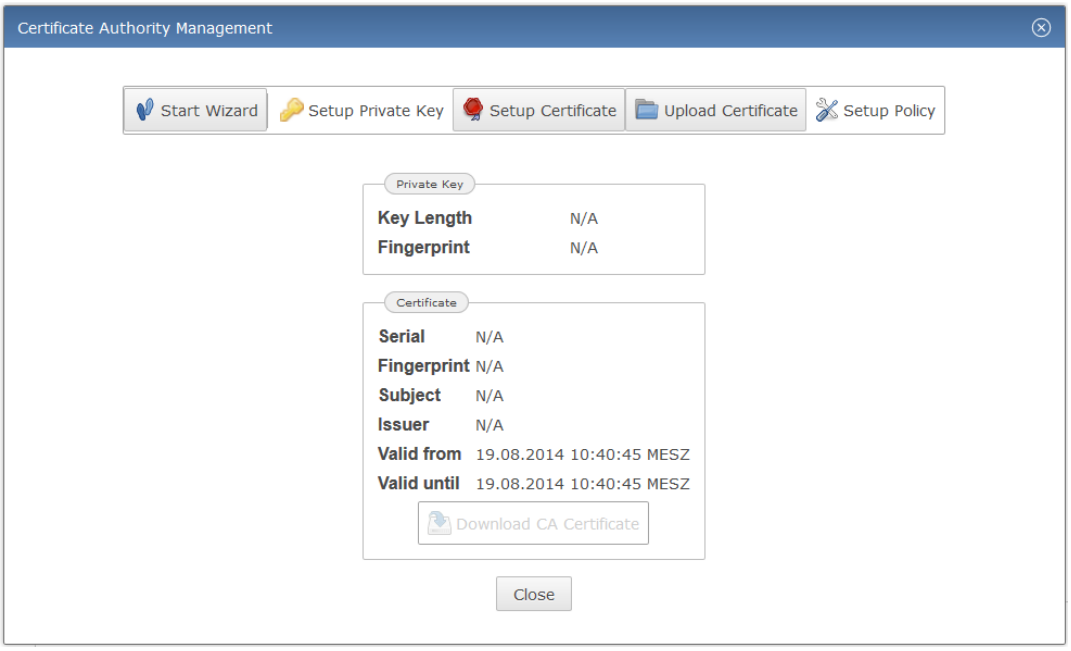


The settings should be configured to match the network monitoring system in use. Some settings are enabled and disabled depending on other settings, primarily the SNMP version, as not all settings are required or supported for all versions.

5.7 Certificate Authority configuration

To use the "Sign Certificates" job to provide a TLS-enabled target with the certificates required for secured operation, the integrated NAMES certificate authority must first be configured properly. Properly configuring both the targets and NAMES for TLS-secured operation requires a working knowledge of asymmetric encryption, PKIs and TLS. Providing this is outside the scope of this document; it is recommended that administrators acquire this knowledge from other sources.

To configure the built-in certificate authority (key, certificate, signing policy) open the "Certificate Authority" dialogue from the "Maintenance" menu:

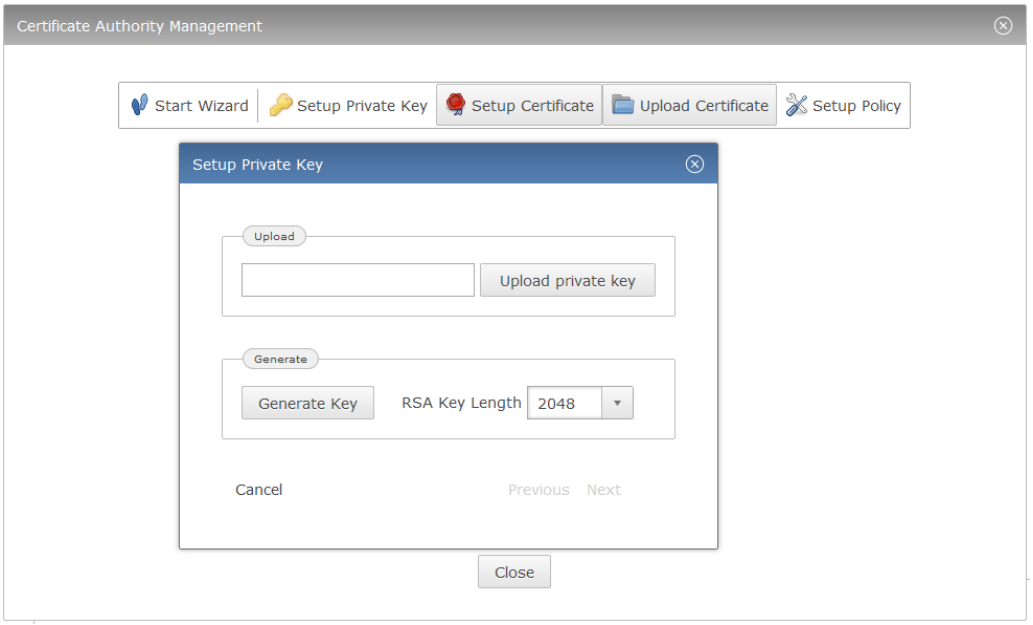


This dialogue shows information about the currently configured RSA key and matching certificate. To begin configuring the certificate authority, either click the "Start Wizard" button to be guided through the configuration, or use the other buttons to directly open the section you wish to configure. In the following description screenshots from the wizard mode will be used, the resulting dialogues are however identical to the individually selected dialogues except for the buttons at the bottom.

There are a number of different ways to configure your certificate authority, both with regards to how key and certificate material is acquired and whether NAMES is integrated into an existing PKI or is configured as a root certificate authority.

5.7.1 General configuration procedure

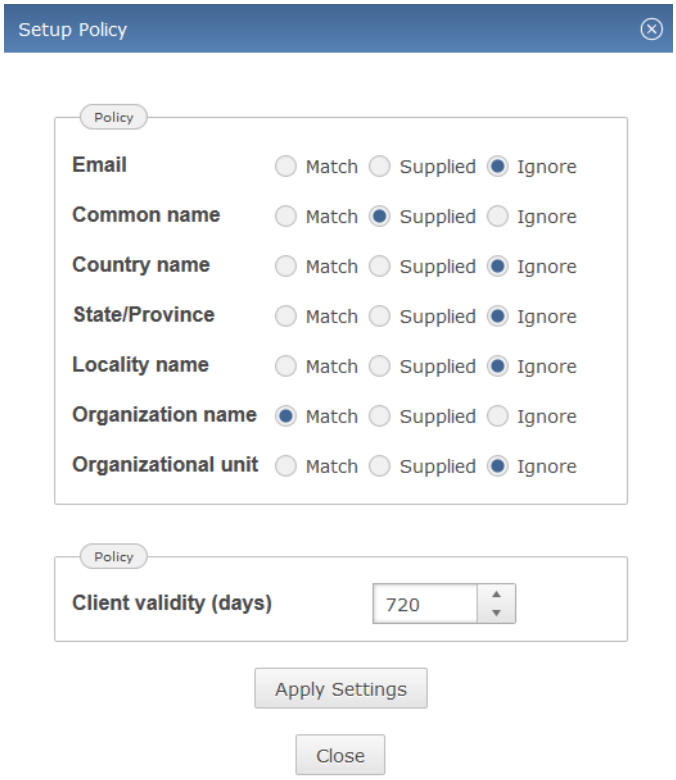
In all scenarios, the certificate authority key and certificate as well as signing policy must be configured. The first step is always to configure the key:



The key can either be uploaded in the form of an unencrypted PEM-encoded RSA key, or generated by NAMES. When generating a key, you can select a key length or 1024, 2048 or 4096 bits. Depending on the selected length of the key and random chance, generation of an appropriate key may take some time.

After configuring the key, a matching certificate has to be configured. For details of how to configure the certificate, see sections 5.7.2 to 5.7.4.

Finally you have to configure the signing policy. The signing policy determines both: Which distinguished names the certificate authority will accept in a Certificate Signing Request and for how many days the issued certificates will be valid.



For each distinguished name component, it can be specified whether the value in the request has to **match** the corresponding value in the certificate authority's certificate, simply be **supplied** but can have any value or is completely **ignored** and thus may also be unset.

5.7.2 Configuring NAMES as a Root CA

The simplest way to configure NAMES is as a Root CA. Begin by generating an RSA key and then generate a self-signed certificate. To do this, you will need to enter the distinguished name of the certificate authority you are setting up in the "Setup Certificate" dialogue. Select how long the self-signed certificate should be valid and finally click the "Generate Self-Signed" button:

The generated certificate will be sent to your browser for use in other applications' trust stores. It can be re-downloaded later from the CA information dialogue. For security reasons, generated RSA keys cannot be downloaded from NAMES.

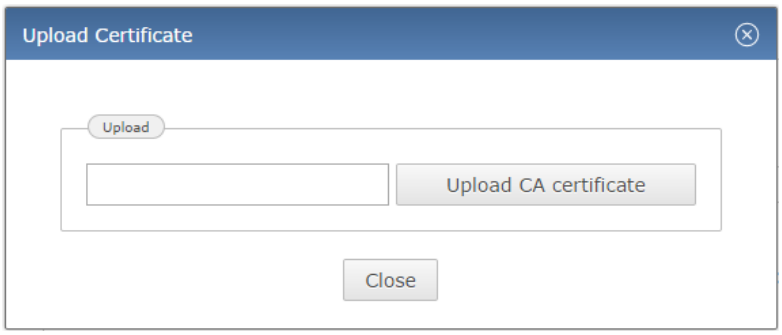
After configuring your policies as described above, your CA is ready to use. Please note that the NAMES CA can only be used to issue certificates to NovaTec devices, not to other devices or software tools (including NMP). You will therefore need another CA to issue certificates to these and will have to configure trust relationships accordingly.

5.7.3 Configuring NAMES as a subordinate CA

When using NAMES with an existing PKI, it may be more convenient to configure it as a subordinate certificate authority under the existing hierarchy. To accomplish this, proceed as in section 5.7.2 above, but do not generate a self-signed certificate. Instead, click the "Download CSR" button in the "Setup Certificate" dialogue to generate a Certificate Signing Request.

This CSR then has to be submitted to the root or intermediate CA, under which the NAMES CA is to be inserted. A corresponding certificate has to be issued, taking care to include correct usage restrictions; appropriate information is contained in the CSR, but CA policy may discard the extension requests. Once the certificate has

been issued, it has to be uploaded to NAMES through the "Upload Certificate" dialogue, reached from the "Certificate Authority Management" dialogue:



The certificate file has to contain the certificate with full verification chain in PEM-encoded format. After configuring signing policy, the certificate authority is ready for use.

5.7.4 Configuring NAMES using an existing key and certificate

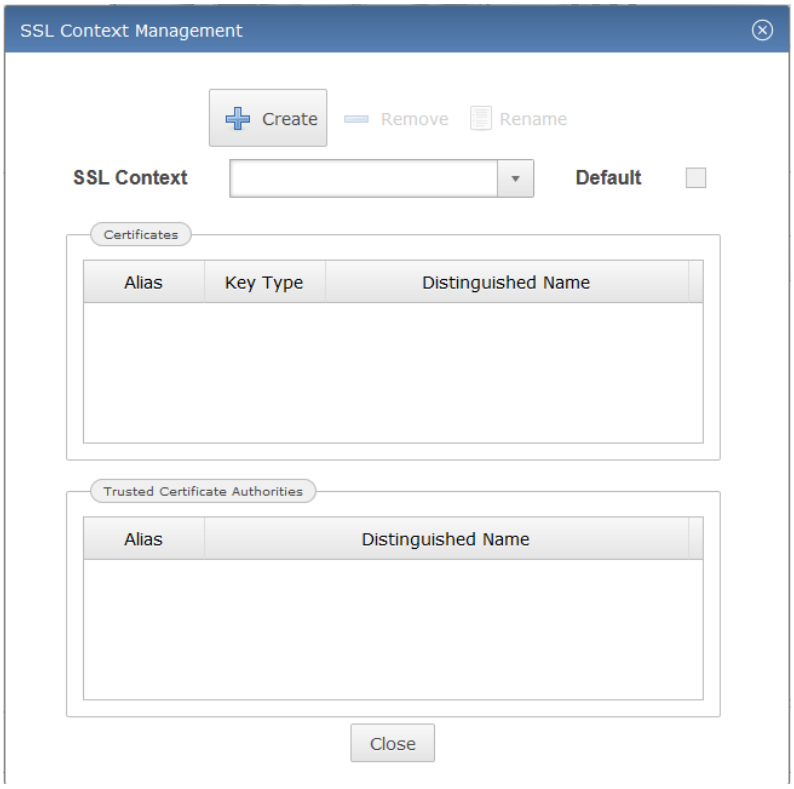
If an existing key and certificate are to be reused for NAMES, or key and certificate are to be generated externally, both can be uploaded to NAMES. First upload the key as explained in section 5.7.1, then upload the certificate as explained in section 5.7.3. You may need to convert existing files into the required formats (PEM-encoded, no encryption). Configure the policy and the certificate authority is ready for use.

5.8 SSL contexts

In order for NAMES to communicate with targets configured for secure maintenance (TLS encrypted/authenticated MNT and/or CH connections), SSL Contexts must be configured. These contexts contain the RSA key used by NAMES, a corresponding certificate and a collection of certificates for all trusted Certificate Authorities. NAMES does not automatically trust its own CA, so you will need to add the certificate for the internal CA even if using NAMES to certify the targets.

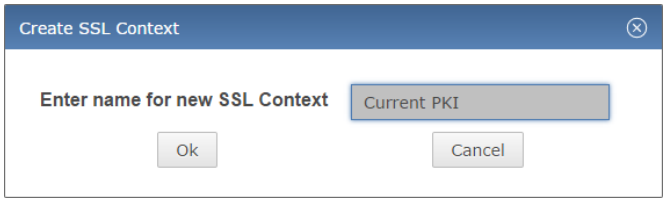
You can have multiple SSL Contexts in use at the same time, for example when migrating from one PKI to another, or when using different PKIs for different network segments or clients. The SSL Contexts will later be assigned to specific targets or CallHome servers; a default SSL Context can also be selected.

To begin configuring SSL Contexts, select "SSL Contexts" from the "Gateway Management" menu:



5.8.1 Creating an SSL context

To create a new SSL Context, click the "Create" button. Specify a descriptive name for the new context and click OK:



The new context will now appear in the "SSL Context" combo box and can be edited as described in section 5.8.2.

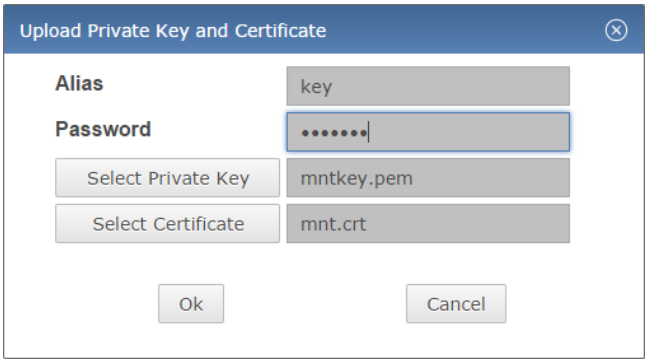
5.8.2 Editing an SSL context

Each SSL Context must contain exactly one entry in the "Certificates" table and at least one entry in the "Trusted Certificate Authorities" table. Multiple own certificates are supported in principle, however, as current firmware versions do not supply a list of trusted CAs during TLS handshake, NAMES cannot select an appropriate certificate. To ensure the correct one is used, only one should be configured at a time.

Warning: editing an existing context which is in use by one or more targets/CallHome servers may cause connections to these targets/servers to fail while changes are being made.

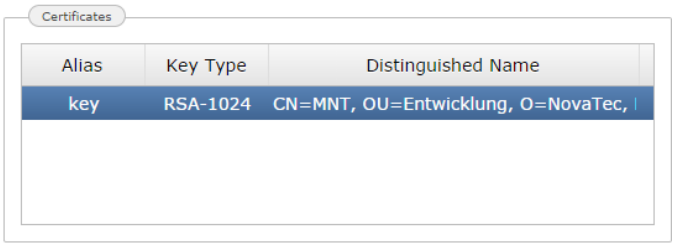
5.8.2.1 Adding a private key and certificate

First, right-click in the "Certificates" table and select "Create" from the context menu. The "Upload Private Key and Certificate" dialogue is displayed:



Fill in a descriptive alias for the key pair and then select a private key file and a certificate file for upload. These files must contain an RSA private key and a corresponding certificate, both in PEM format. The certificate file should contain the entire certificate chain without the Root CA certificate if the signing Certificate Authority is not the Root CA. If the key is encrypted, you must also supply the correct password for decryption. Finally, click "OK" to upload the files.

If the import process was successful an entry containing basic information about key and certificate will be displayed in the "Certificates" table:

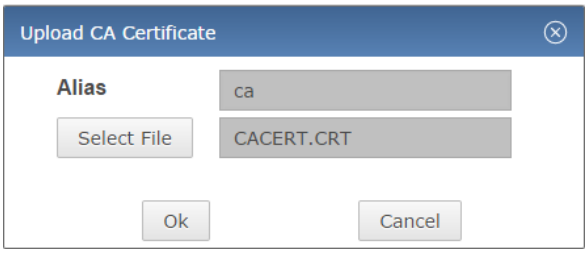


5.8.2.2 Replacing a private key and certificate

To replace a private key and certificate for an SSL Context, you must first remove the current key and certificate. To do this right-click the entry in the "Certificates" table and select "Remove" from the context menu. After removing the current entry proceed as described above.

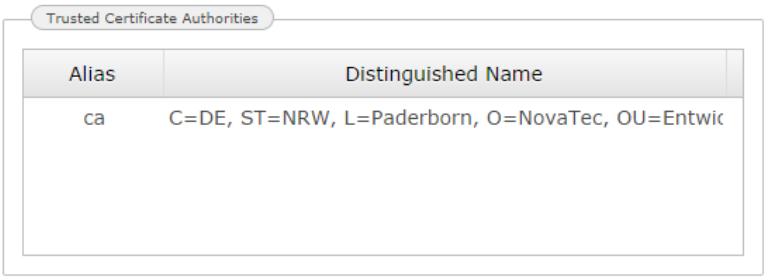
5.8.2.3 Adding a trusted certificate authority

You must add at least one entry to the "Trusted Certificate Authorities" table. Multiple CAs may be added if necessary, for example if targets are signed by different CAs, but trust the same CA. To add a trusted certificate authority, right-click in the "Trusted Certificate Authorities" table and select "Create" from the context menu:



Fill in a descriptive alias (this must differ from any other alias used in the same context, including the alias for the "Certificates" table entry) and select a PEM-encoded certificate for upload, then click OK.

If the import process was successful, an entry containing basic information about the certificate is displayed in the "Trusted Certificate Authorities" table:



5.8.2.4 Removing a trusted certificate authority

To remove a trusted CA from the list, right-click its entry in the table and select "Remove" from the context menu.

5.8.3 Setting an SSL context as default context

You may assign a "Default Context", which means this SSL Context will be assigned as the context for newly created targets or CallHome servers by default. To choose the default context, simply select the context from the combo box and check the "Default" check box.

5.8.4 Removing an SSL context

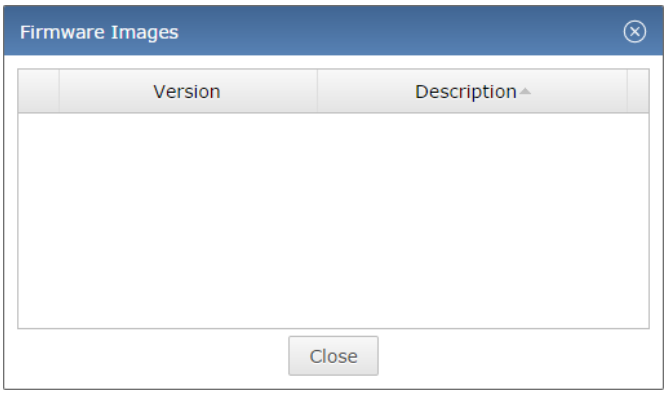
To remove an SSL Context, select the context you wish to remove from the combo box, then click the "Remove" button at the top. If the "Remove" button is greyed out, the context is in use and cannot currently be removed. You must first remove the context from any targets and CallHome servers that may be using it.

5.9 Managing firmware images and music on hold files

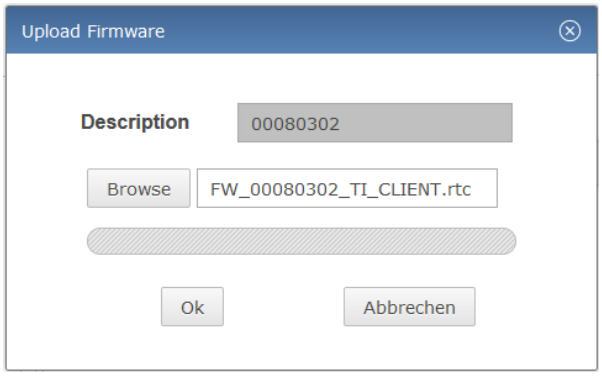
For certain operations binary files need to be uploaded to NAMES first. Specifically, these are Upload Firmware jobs (the firmware image must be uploaded to NAMES) and Upload Configuration if the configuration in question has a Music on Hold configured (the music file must be uploaded to NAMES).

5.9.1 Firmware images

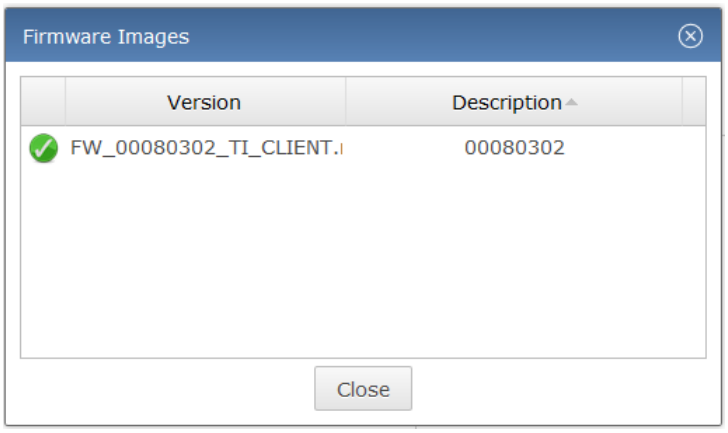
Firmware images are managed through the "Firmware Images" window, which can be opened from the "Gateway Management" menu:



To add a firmware image to NAMES for use in "Upload Firmware" jobs, right-click in the table and select "Upload" from the context menu. The "Upload Firmware" dialogue opens. Specify a description for the firmware (for example, the version of the firmware you are uploading) and select the firmware image you wish to upload:



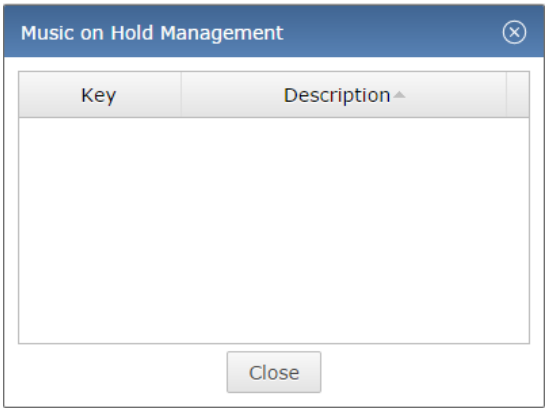
After clicking "OK", the firmware image will be sent to the NAMES server and stored in the database. It is displayed in the table:



To remove a firmware image from NAMES, right-click the entry in the table and select "Delete", then confirm the deletion in the following dialogue.

5.9.2 Music on Hold

Music on Hold files, which are referenced from configurations through the "MoH key", are managed through the "Music on Hold Management" window, accessible from the "Gateway Management" menu:

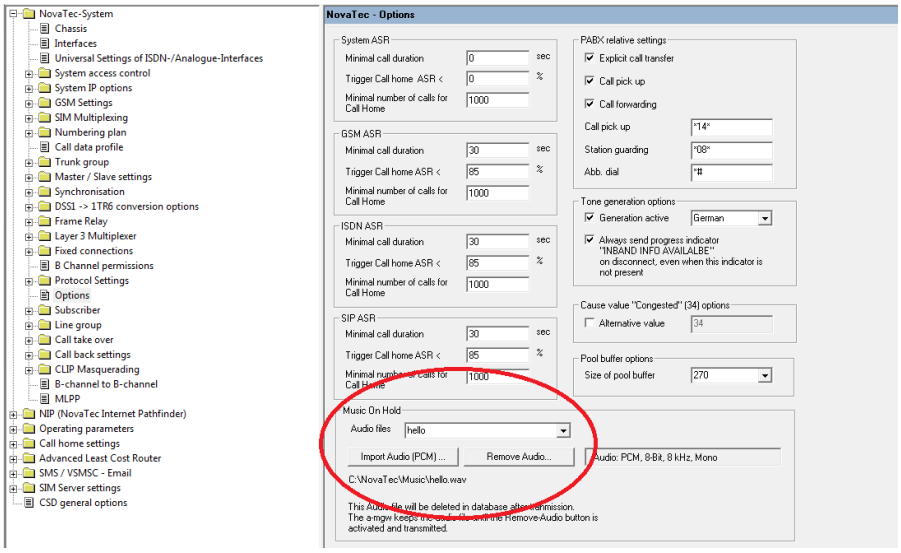


If a system configuration has been configured with Music on Hold, it will contain an MoH key, for which a corresponding music file must be present. Otherwise attempts to upload this configuration to a target will fail, as NAMES will be unable to verify or upload the configured Music on Hold.

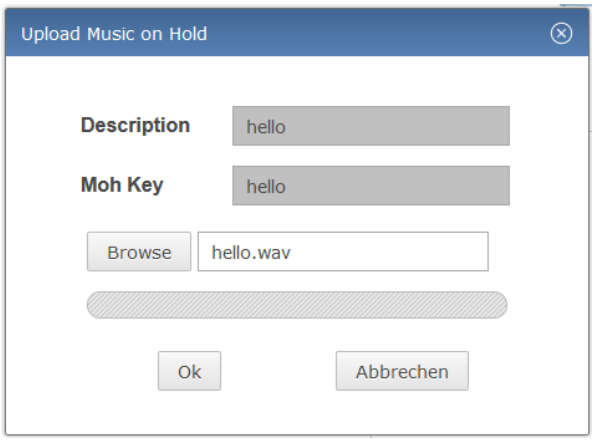
The Music on Hold key is a string of up to ten alphanumeric characters which is configured in the wav.ini file of the NovaTec Configuration utility:

```
[Files]
hello=C:\NovaTec\Music\hello.wav
```

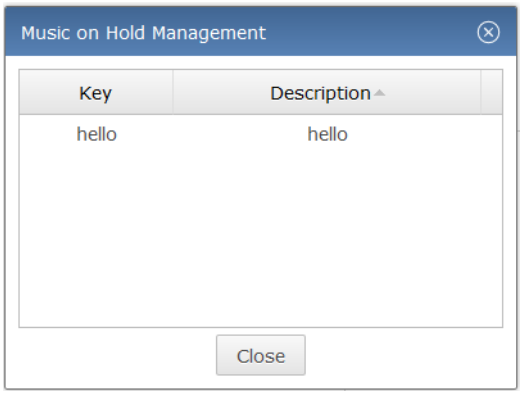
This tells the configuration utility that it can load the file `C:\NovaTec\Music\hello.wav` as Music on Hold with the MoH key `hello`. The music file can then be selected in the NovaTec Configuration utility on the NovaTec-System/Options page:



To correctly upload this configuration to a target device using NAMES, the corresponding music file must be uploaded to NAMES with the same MoH key. To do this, right-click in the table of the "Music on Hold Management" window and select "Upload":



After entering a description, which can be any text, and the correct MoH key and selecting the desired music file, click "OK" to upload the file to NAMES. If the music file is in the correct format (see NovaTec Configuration utility for further details), the file is imported and a new entry appears in the table:



The Music on Hold is now ready for use.

To remove a Music on Hold file from the database, right-click the entry in the table and select "Delete", then confirm deletion in the following dialogue.

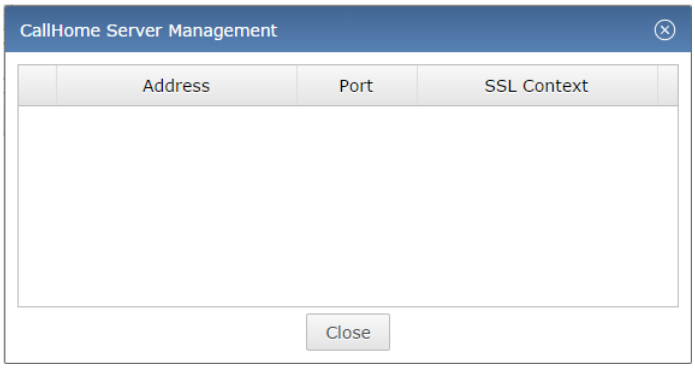
5.10 CallHome servers

NAMES can receive CallHomes – notifications about certain events, referred to as CallHome events – from targets. CallHome Events are mapped to SNMP traps, which are sent to the SNMP management system configured in the SNMP settings (see section 5.6). In addition, some CallHome events may be used to trigger jobs; for example, a notification that the trace file storage is full may be used to trigger a trace file retrieval job.

In order for CallHome reception to work, the targets must be configured to send these notifications to the NAMES server when the corresponding events occur, and the NAMES server must be configured to receive the CallHomes. Configuration of NAMES to receive CallHomes is done in the form of CallHome servers. A CallHome server is a combination of listen IP, port and TLS configuration, which causes NAMES to accept connections on the configured IPport and – optionally – encrypt and authenticate connections using the supplied SSL Context.

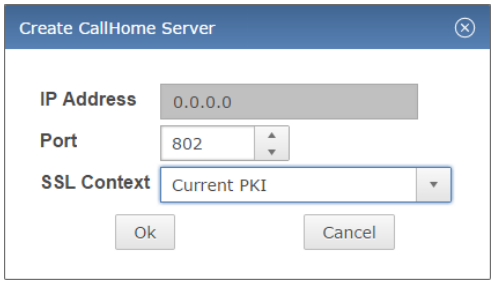
Filtering of incoming connections is done first via TLS authentication – if an SSL Context is assigned to the server –, second through backplane IDs and third through comparison of the source IPs with the IP of the target, which corresponds to the backplane ID. If any of these checks fail, the connection is closed.

To begin managing CallHome Servers, select "CallHome Server Management" from the "Gateway Management" menu. The "CallHome Server Management" window is displayed:

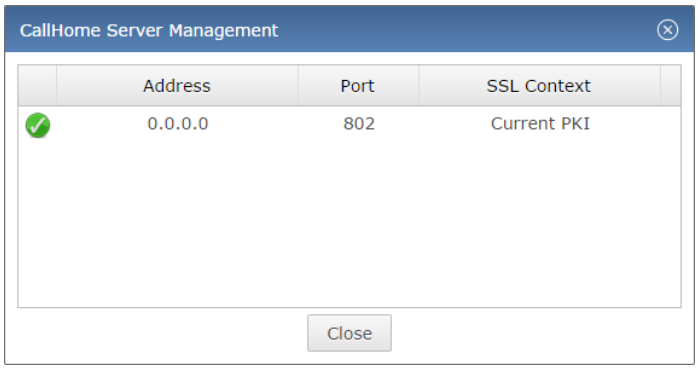


5.10.1 Creating a CallHome server

To create a CallHome server, right-click in the table and select "Create" from the context menu. The "Create CallHome Server" dialogue will appear:



On a system with multiple local IP addresses, you may specify one of thes addresses as the listen address by supplying it in the "IP Address" field, or enter "0.0.0.0" to listen on all IP addresses. Next, select a port for the CallHome server and, if the CallHome Server should use TLS for authentication and encryption, an SSL Context. After clicking "OK", the server will appear in the list:



Multiple CallHome servers may exist, however each IP/port combination must be unique. As specifying "0.0.0.0" for the IP address causes the server to listen on all local IP addresses, no other CallHome servers may be created with the corresponding port. If a CallHome server with the "0.0.0.0" IP address is created on a port that is already in use by another CallHome server with a specific IP, that previously existing server will be removed and subsumed by the newly created entry.

A typical configuration may be e.g. an encrypted CallHome server on port 802 and an unencrypted server on port 803 (gateways with TLS configurations but lacking a certificate will attempt to connect to a port that is one higher than the configured port).

5.10.2 Editing a CallHome server

To edit an existing CallHome server, right-click the entry in the list and select "Edit". The "Edit CallHome Server" dialogue will appear, containing the same options as the "Create CallHome Server" dialogue. After changing the options as desired, click "OK" to save the changes.

Editing a CallHome server will generally cause the listen server to be stopped and restarted with the new settings. This will lead to a brief loss of service; any incoming CallHomes cannot be received during this time, however, targets will retry the transmission for a time.

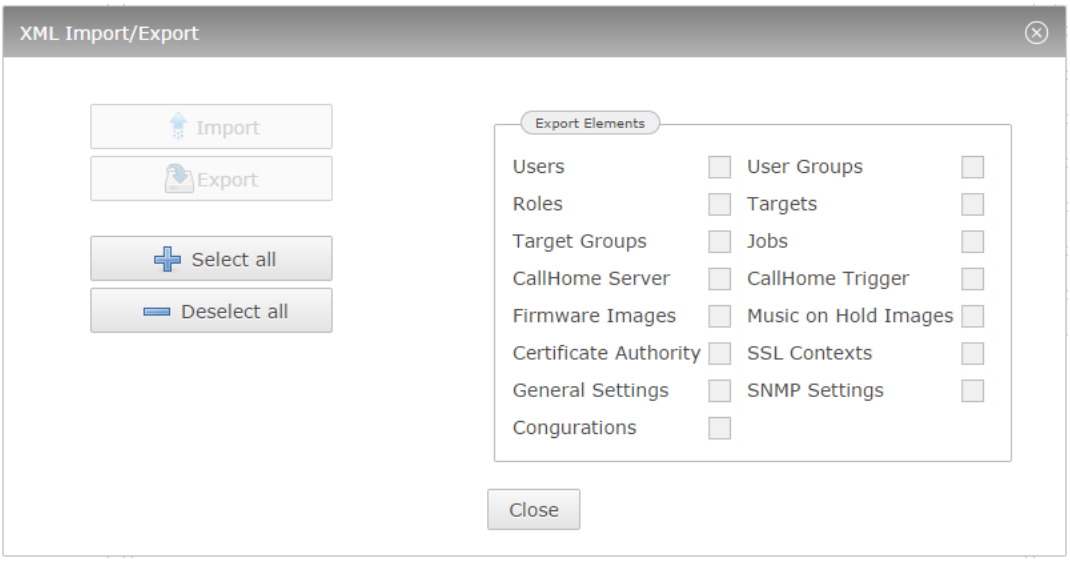
5.10.3 Deleting a CallHome server

To delete a CallHome Server, right-click the entry in the list and select "Delete", then click "Yes" to confirm deletion.

5.11 Data export/import

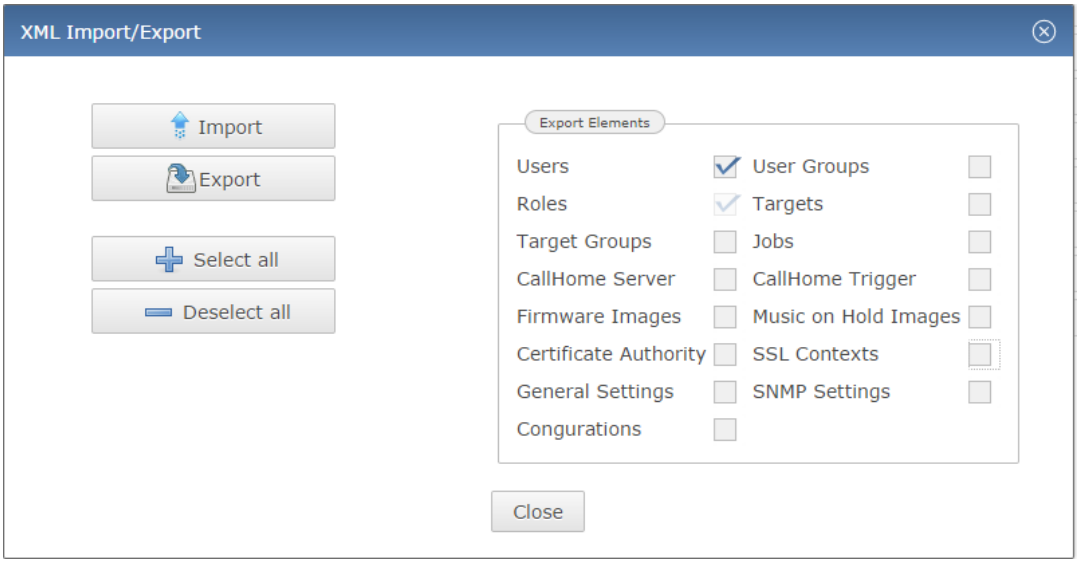
NAMES allows you to export and import data in a database-agnostic XML format that is also upgrade-proof; which means future versions of NAMES will be able to import this data even if the underlying database structure has changed. This function may be used to transfer data from one NAMES instance to another, migrate to a different database type, backup data in an upgrade-proof way or achieve a consistent initial data set in a testing environment.

To export or import NAMES data, select the "Import/Export" item from the "Maintenance" menu to open the dialogue:



Select the elements you wish to export or import in the "Export Elements" group by ticking the appropriate checkboxes. The "Select all" and "Deselect all" buttons can be used to select all or none of the options.

Dependencies will automatically be selected as well; for example, if you select "Users", "Roles" will also be selected:



To export data, select "Export". The data export can be encrypted with AES-256; to do so, specify a password when prompted. To skip encryption, leave the password box empty. The export will then be generated and a download of the export file will start. All exports are GZIP-compressed.

To import existing data, select "Import" and select the file you wish to import from. If the file is password protected, you will be prompted for the password. Importing data currently requires a large amount of free memory, approximately three to four times the size of the uncompressed export.

5.12 Shutting NAMES down

To shut NAMES down, you have several options. From the web UI, you can shut NAMES down "gracefully", which means that no more jobs will be started and the program will exit after all running jobs have been completed, or immediately, which means that any running jobs will be aborted.

To shut down NAMES, select "Server Shutdown" from the "Maintenance" menu. The shutdown dialogue will appear:

The "Graceful shutdown" option is checked by default. To perform an immediate shutdown, aborting all running jobs, deselect the option. After clicking "Yes", NAMES will shut down either immediately or after all running jobs

have finished. As this action also shuts down the embedded web server, no further feedback is provided. The web UI will report that it has lost its connection to the server.

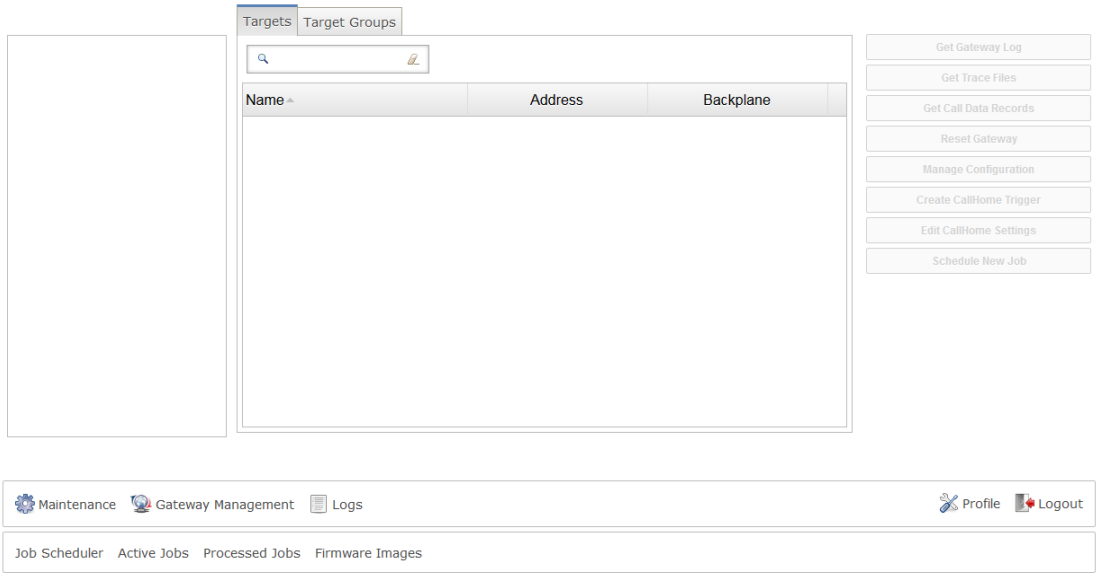
You can also shut down NAMES from the Windows Server Manager UI. This should however only be done as a last resort, if a shutdown through the web UI is not possible.

6 Usage

6.1 Targets

In NAMES, the word "target" signifies a NovaTec device which has been added to the database and is to be administered through the application. It can be a target for the "jobs" that NAMES can perform.

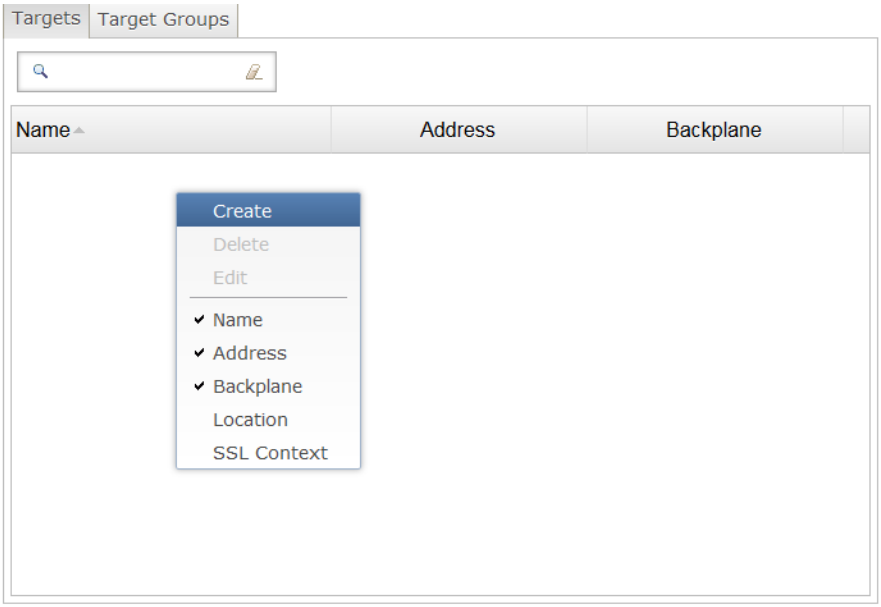
The main application element in NAMES is the target list, which is always displayed centrally in the main window. After NAMES has been installed, the target list is empty and has to be populated by the user:



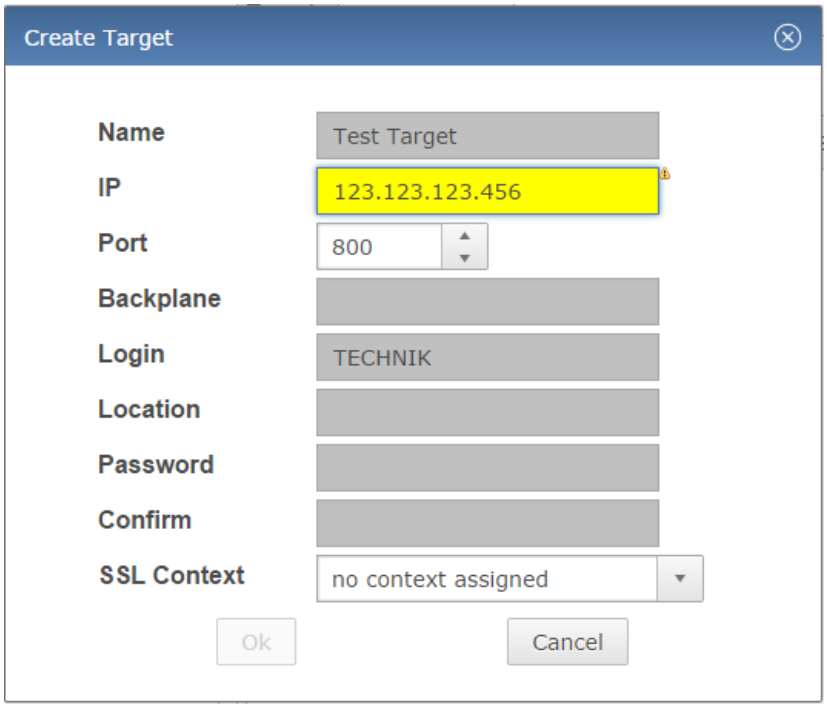
The target list allows you to view, select, create, edit and remove targets.

6.1.1 Creating a target

To create a target, simply right-click in the target list area to bring up the context menu, then select the create option:



This will open the "Create Target" dialogue, which allows you to specify target details. At a minimum, a target name and either an IP address or a backplane ID have to be specified. IPs and backplane IDs are syntax checked and any entry of non-hex characters is suppressed for the backplane ID.



The "Login" field should normally not be changed from the default ("TECHNIK"). If a password has been set on the device using the NMP tools, this password should be entered into the "Password" and "Confirm" boxes. The "Location" field currently only has informational use; any text may be entered here.

The "SSL Context" configuration is necessary for TLS secured maintenance connections and requires an SSL context to be configured. If your device's maintenance connection is TLS-enabled, select the appropriate SSL context after configuring it (see section 5.8).

After entering the necessary information, click "OK" and the target will be created.

6.1.2 Editing a target

To edit a target, right-click the target entry in the list and select "Edit" from the context menu. The "Edit Target" dialogue is identical to the "Create Target" dialogue, except for the checkbox next to the "Password" field. This checkbox specifies whether the password should be changed; if unchecked, no change will be made to the password. To clear the current password, tick the checkbox and leave the password field empty.

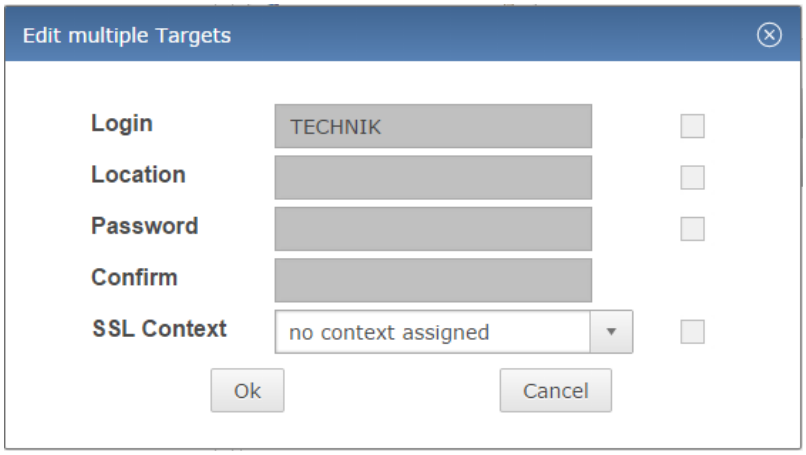
6.1.3 Removing a target

To remove a target, right-click the entry in the list and select "Delete" from the context menu. It may not be possible to remove a target, for example if running or waiting jobs still exist. A confirmation dialogue will be shown before the target is deleted.

6.1.4 Multiple target actions

Both the "Edit" and "Delete" actions may be applied to multiple targets at a time. Simply select multiple targets from the list by holding the `Ctrl` button on your keyboard to select individual targets or the `Shift` button to select a range. Right-click the selection and select "Delete" or "MultiEdit" from the context menu.

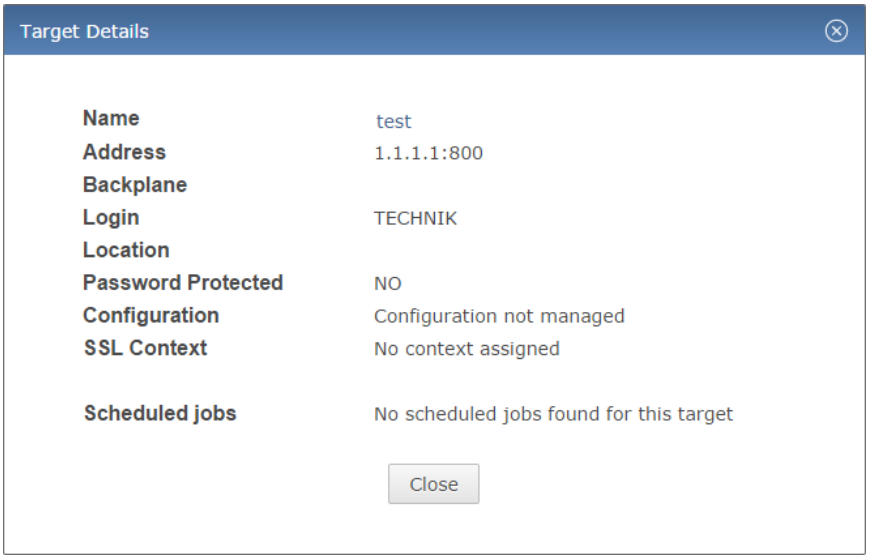
The "Edit multiple targets" dialogue differs from the "Edit Target" dialogue, as it only contains items that can be set for multiple targets at the same time: login name, location, password and SSL context.



As with the password in the regular "Edit Target" dialogue, the checkbox corresponding to a field in the "Edit multiple targets" dialogue must be ticked if changes are to be made. For example, to clear the "Location" value on all selected targets, tick the checkbox next to the "Location" field and leave the input box empty.

6.1.5 Target details

To show the "Target Details" dialogue for a target, double-click its entry in the list. In addition to information that can be configured in the "Target Edit" dialogue, this window also displays whether a password is configured for this device (but not the actual password – that is never sent to the web client), which configuration was last transmitted to the device and whether any jobs are currently scheduled for the target:



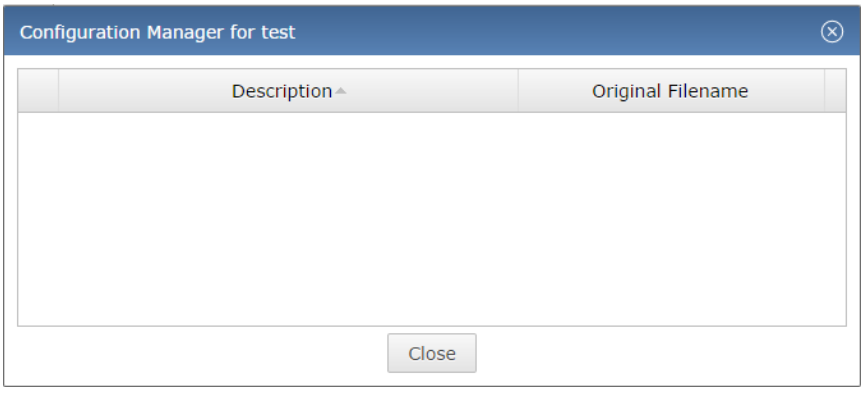
This dialogue does not have any edit functions and is for informational purposes only.

6.1.6 Target configurations

In order to upload a configuration to a target, it must first be uploaded to NAMES. Configurations are created and edited with the NovaTec Configuration utility and saved in MS Access database files (*.mdb). When using NAMES, configurations should not be directly transferred to a gateway using the utility, but through NAMES instead. This ensures that NAMES is the central repository for configurations and that the configuration NAMES shows as active is in fact the target's active configuration.

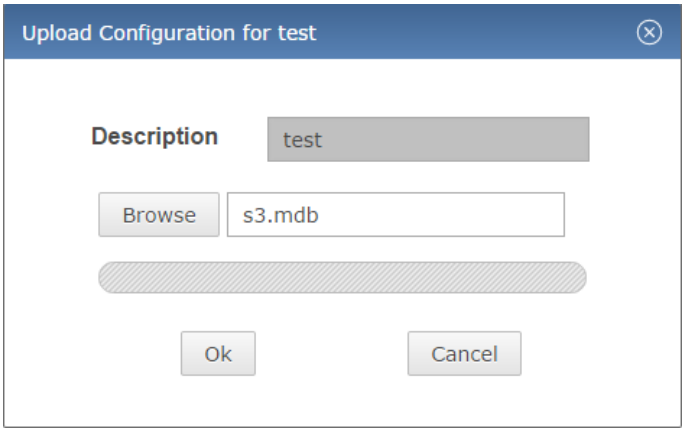
For any target, one or more configurations may be stored in the NAMES database. Whenever one of these configurations is transmitted to the target device, it is marked as active in the database. This is also a requirement for the use of the Reconfiguration API, which will always modify the currently active configuration.

To begin managing a target's configurations, select the target from the target list, then click the "Manage Configuration" button in the action bar to the right. The "Configuration Manager" window is displayed:

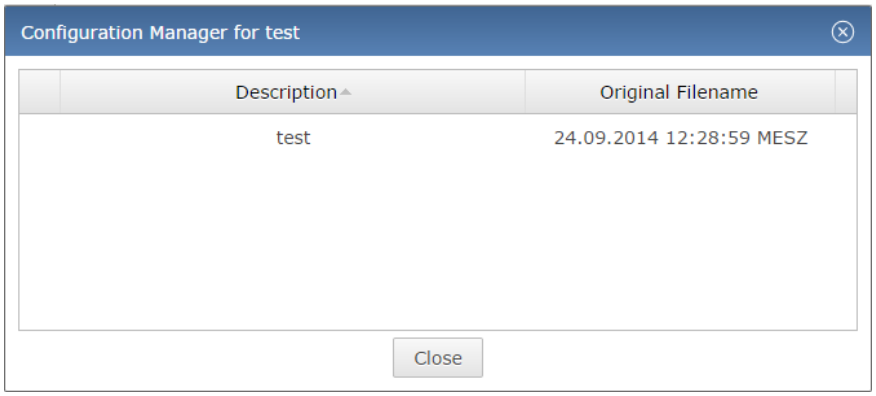


6.1.6.1 Adding a configuration

To add a configuration to a target, right-click in the table and select "Create" from the context menu. The "Upload Configuration" dialogue is displayed:



Enter a description for the configuration and select the configuration database to upload, then click OK. The configuration is imported into the NAMES database, converting from the MS Access format to the internal database format of NAMES. The newly uploaded configuration is displayed in the table and is ready for upload to a target:



6.1.6.2 Deleting a configuration

To delete a configuration from the database, right-click the entry in the table and select "Delete" from the context menu, then click "Yes" to confirm deletion. It is not possible to delete the currently active configuration, which is marked by the  symbol.

6.1.6.3 Downloading a configuration

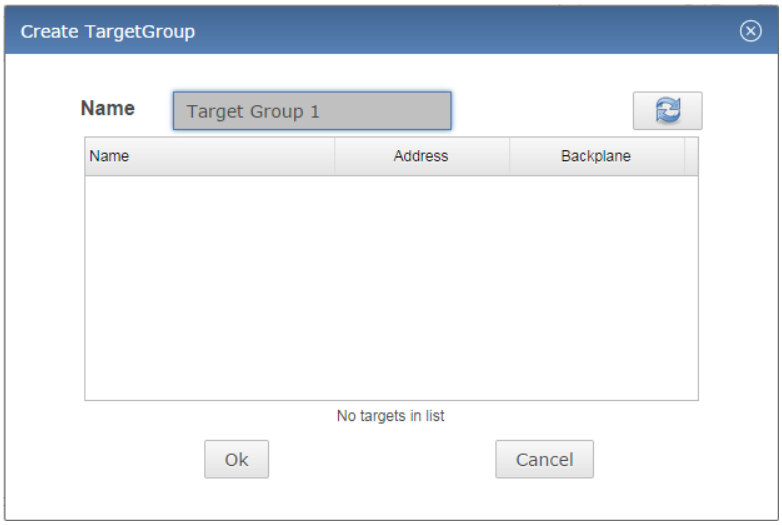
In order to edit a configuration, it must first be downloaded from NAMES. It can then be opened and modified using the NovaTec Configuration utility. To download a configuration from NAMES, right-click the entry in the table and select "Download" from the context menu.

6.2 Target groups

Targets can be collected in target groups. This makes tasks such as creating a job for an entire group of targets much easier. Target groups are administered through the "Target Groups" tab of the main UI window, which will switch the target list to a target group list.

6.2.1 Creating a target group

To create a target group, right-click in the target group list and select "Create" from the context menu. The "Create TargetGroup" dialogue is displayed:



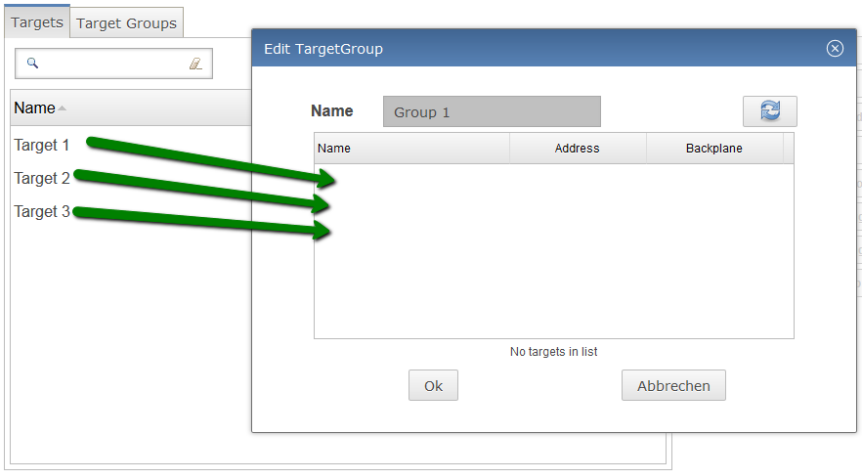
You have to enter a name for the target group. You may add targets to the group (see section 6.2.2) now, or leave it empty and add them later. Click "OK" to finish creating the group.

6.2.2 Editing a target group

Editing a target group allows you to change the group name or which targets are group members. To edit a target group, right-click the target group in the list and select "Edit" from the context menu. The "Edit TargetGroup" dialogue is displayed, which is identical to the "Create TargetGroup" dialogue.

6.2.2.1 Adding Targets

To add targets to a target group, switch back to the "Targets" tab of the main window with the "Edit TargetGroup" window still open. Select the targets you wish to include from the target list and drag them over to the list in the "Edit TargetGroup" dialogue:



6.2.2.2 Removing targets

To remove a target from a target group, right-click it in the list of the "Edit TargetGroup" dialogue and select "Remove from Group" from the context menu.

6.2.3 Removing a target group

In order to remove a target group, right-click it in the list and select "Delete" from the context menu.

6.3 Jobs

In NAMES any changes made to a target are achieved through a "job". Several different types of jobs exist, allowing a number of different administrative and maintenance tasks to be carried out. Jobs may be created by a user – explicitly by using the "Schedule New Job" function, or implicitly by using other functions from the action bar – or in response to a CallHome event (if a corresponding trigger is configured), and may be executed immediately or scheduled for a specific time.

A limited number of jobs can be run at the same time; the maximum number of simultaneous jobs is configured in the NAMES settings (see section 5.3.1) and may be any number in the range of 1 to 10. If all slots are occupied with running jobs, other jobs that are scheduled to run at this time will be added to a waiting queue and executed as slots become available.

6.3.1 Job types

6.3.1.1 Upload Firmware

This job type facilitates a firmware update. Firmware has to be uploaded to NAMES (see section 5.9.1) first, which may require additional privileges. After that, firmware upload jobs may be created, which will upload the firmware to the target. The device will then write the new firmware to its flash and automatically restart once all phone connections have been terminated.

6.3.1.2 Upload Configuration

This job type sends a device configuration to a target. The configuration and any associated Music on Hold file have to be uploaded to NAMES (see section 6.1.6.1 and 5.9.2, respectively) first, which may require additional privileges. When uploading a configuration, the target may tell NAMES that it requires a restart to activate the new configuration. In that case, default behaviour is to tell the target to restart when all phone connections have been terminated. It is however also possible to configure the job to restart the target immediately, or not to restart the target at all.

If the target does not require a restart, the configuration is applied immediately.

6.3.1.3 Reset

This job type sends a reset signal to the device, which will then restart. The device will be unavailable for both phone and maintenance connections whilst restarting. The length of the restart period depends on the device in use.

6.3.1.4 Download Trace Files

This job type downloads all current trace files (error diagnostic information) from the device to NAMES. These trace files are stored in the database and may be downloaded from NAMES for analysis at a later point. Default behaviour is to delete the files on the target after download, but this can be disabled.

6.3.1.5 Download Log File

This job type retrieves the current content of the target device's log and adds it to the database. Log information may later be downloaded from NAMES for analysis by specifying a time range from which logs are to be downloaded. Default behaviour is to clear the targets log after download, but this can be disabled.

6.3.1.6 Download CDRs

This job type retrieves CDRs (Call Data Records) from the target device and saves them in the database. The CDRs may be downloaded from NAMES for analysis later, for a single device or consolidated through target groups.

6.3.1.7 Set Date/Time

This job type sets the UTC time and date of the target device to the UTC time and date of the NAMES server.

6.3.1.8 Sign Certificate

This job type retrieves Certificate Signing Requests (CSRs) from the target device and issues corresponding certificates using the internal Certificate Authority (CA). The certificates are then uploaded to the device and the device is restarted to activate the TLS configuration. For this job type to work, the internal CA has to be correctly configured (see section 5.7) and the device has to be configured with TLS active and at least one of the communication channels (Maintenance, SIP and CallHome) has to be configured to generate a CSR.

6.3.2 Job states

All jobs are in one of a number of states. The possible states and their meanings are as follows:

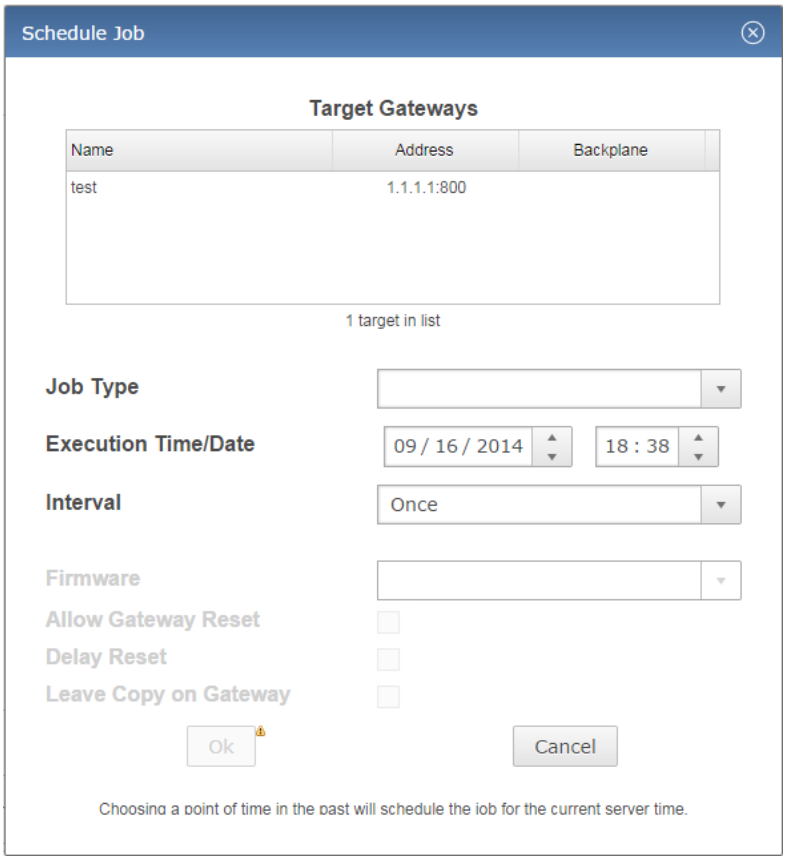
- **Pending:** these jobs have been scheduled for a point of time in the future.
- **Waiting:** these jobs are due to run, but are waiting for slots to become available.
- **Running:** these jobs are currently being run.
- **Done:** these jobs were completed successfully.
- **Failed:** these jobs encountered an error and could not be completed.
- **Obsolete:** these jobs should have been run during NAMES downtime and have been marked obsolete. They may be reactivated from the "Obsolete Jobs" window.

6.3.3 Creating a job

Jobs can be created through various means. They may be created automatically in response to events that have occurred on a target device (see section 6.4), created in response to configuration changes through the "Reconfiguration API", triggered through "refresh" buttons in several UI windows and finally scheduled through the "Schedule Job" dialogue.

This section will address the express scheduling of jobs through the "Schedule Job" dialogue; other ways of creating a job will be addressed at the appropriate point in the manual.

The "Schedule Job" dialogue allows all job types, except for "Upload Configuration", to be scheduled. To open the dialogue, select the target, targets or target group you wish to schedule jobs for and then click the "Schedule New Job" button in the Action Bar on the right:



The target list at the top shows the selected targets and may be further edited by dragging targets from the main window into the list or right-clicking targets and selecting remove.

Select a job type from the drop down menu and select the time you wish the job to be scheduled for. If you select the current time or a time in the past, the job will run immediately. If you wish the job to be repeated periodically, select the appropriate interval from the "Interval" drop down menu.

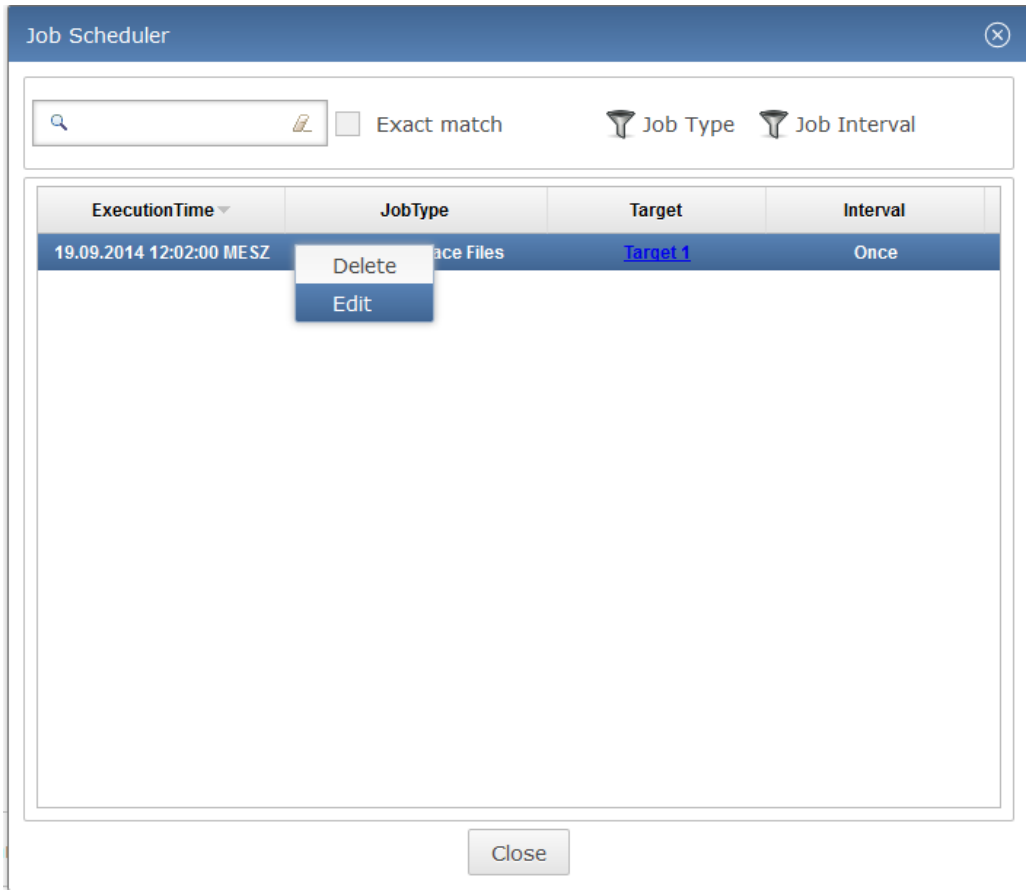
The remaining options depend on the job type you have selected:

- **Firmware:** for an Upload Firmware job, select the firmware you wish to upload to the target.
- **Delay Reset:** for a Reset job, select whether the reset should be delayed until all phone connections have been terminated.
- **Leave Copy on Gateway:** for all download jobs, select whether the job should leave a copy of the data on the target or remove it. Warning: Using this option with log downloads will cause duplicate log entries in the NAMES database if the device log is not otherwise cleared, as NAMES cannot reliably detect duplicate log entries at the moment.

After selecting the options you wish to use, click OK to schedule the job.

6.3.4 Viewing and modifying scheduled jobs

Once a job has been scheduled and is in pending state, it will appear in the "Job Scheduler" window, which can be reached through the "Gateway Management" menu and by default through the quick bar:



Jobs can be deleted or edited by right-clicking on their entry and selecting "Delete" or "Edit" from the context menu as long as they are in the pending state. Once their execution time has arrived and they progress to waiting or running, they can no longer be deleted or edited.

Job types cannot be changed after creation, as this is viewed as an entirely different job. If you wish to do this, simply delete the job and recreate it with the required type.

6.3.5 Active jobs

The currently running jobs may be viewed by opening the "Active Jobs" window, reachable from the "Gateway Management" menu or through the quick bar. The current job activity state (connecting, uploading, downloading, working…) is displayed. If the job is uploading data to the target, a progress bar for the upload is also displayed.

6.3.6 Completed and failed jobs

Completed and failed jobs can be viewed in the "Processed Jobs" window. In addition, a message will be displayed in the notification area to the left of the target list whenever a job fails.

Double-clicking a job in the notification area or the list in the "Processed Jobs" window will open a window showing information about the job, including a failure message that indicates why the job could not be completed.

Jobs may be deleted by right-clicking them in the "Processed Jobs" window and selecting "Delete" from the context menu.

6.4 CallHome jobs

CallHome jobs may be used to automate certain maintenance tasks. CallHome jobs are automatically created and queued by NAMES when a specific event occurs. The association of an event with a job template is referred to as a "CallHome Trigger" in NAMES.

The following event types may be used to trigger a job:

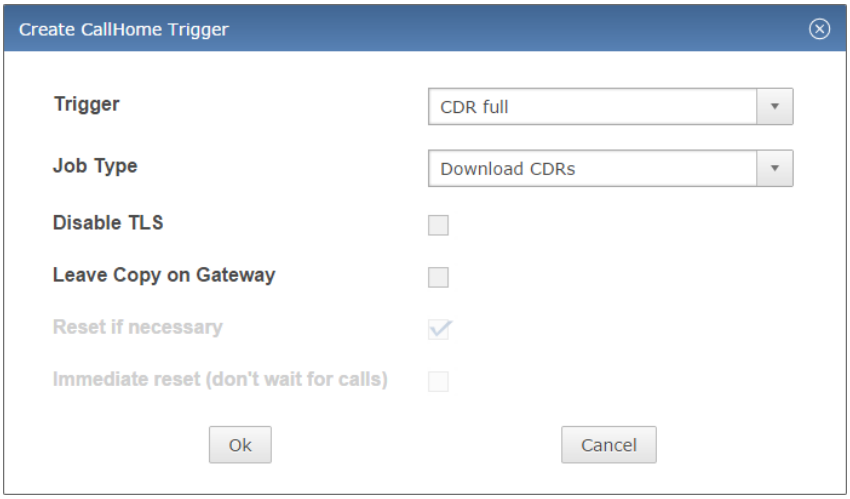
- **CDR full:** target system storage for CDRs has reached 50% fill level.
- **Trace full:** the maximum amount of trace files have been stored on the target system.
- **Log full:** target system storage for logs has reached 100% fill level.
- **System startup:** the target system has finished booting.
- **TLS has default time:** TLS is configured, but system time is not set.
- **Free RAM threshold:** the amount of free RAM has fallen below the configured threshold.
- **DHCP application:** sent by an unconfigured system after retrieving IP and NAMES information from DHCP.

Any of these events may be used to trigger any of the following jobs, although the default job type for each event is usually the only useful combination:

- Download CDRS
- Download trace files
- Download log file
- Reset
- Set date/time
- Sign certificates
- Upload configuration

6.4.1 Creating a CallHome trigger

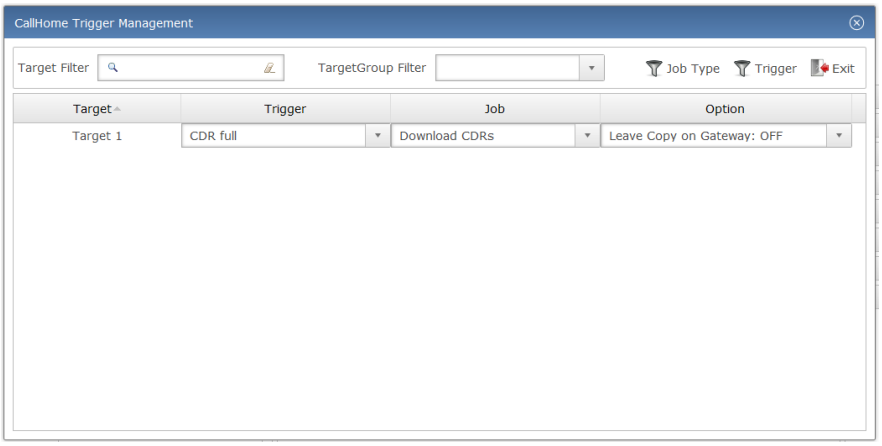
CallHome triggers may be created either for a single target or for a target group. Creating a CallHome trigger for a target group will result in creation of CallHome triggers for each of the targets in the group. Select the target or target group you wish to create a trigger for from the target or target group list, then click the "Create CallHome Trigger" button in the action bar. The "Create CallHome Trigger" dialogue is displayed:



Start by selecting the event type you wish to trigger the job from the "Trigger" combo box. When selecting an event type, the default corresponding job type is automatically selected for you. If you wish a different job type to be triggered, change the selection in the "Job Type" combo box. Finally, configure the job parameters that are available for the selected job type, and click "OK".

6.4.2 Editing CallHome triggers

To edit CallHome triggers, select the target or target group you wish to edit CallHome settings for from the target or target group list and then click the "Edit CallHome Settings" button in the action bar to the right. The "CallHome Trigger Management" window is displayed:



To edit a single entry, select the appropriate settings through the combo boxes.

To remove a trigger, right-click the trigger and select "Delete" from the context menu.

The window also offers a "MultiEdit" function which may be used to alter settings for multiple CallHome triggers at once. This is most useful when editing triggers for a target group. To use this function, select multiple CallHome triggers by holding the `Ctrl` button to add individual entries to your selection or the `Shift` button to add a range of entries to your selection. Right-click the selection and select "MultiEdit" from the context menu. The "MultiEdit CallHome Triggers" dialogue is displayed, which is functionally identical to the "Create CallHome Trigger" dialogue.

6.5 User settings

User settings are available through the "Profile" menu. They allow users to change their password, to select an icon theme that is more appropriate for users suffering from red-green colour blindness or to configure the tool bar located at the bottom of the UI. Currently, icon and tool bar settings are not saved between sessions.

To change the user password, select "My Settings" from the "Profile" menu, then enter a new password into the "Password" input box and confirm it by entering the same password again into the "Confirm" box. Ensure that the checkbox to the right of the "Password" input box is ticked and then click "OK".

The new password must conform to basic password safety rules: it must contain at least five characters, of which at least one must be a lower case letter, one an upper case letter and one a number. If either of these rules are not observed or the password does not match its confirmation, a validation error will be shown and form submission will not be allowed (the "OK" button is disabled).