A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant/Manager

Access Management V11

Administrator Documentation
09/2025

A31003-H34B0-M121-05-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 Access Management-Overview

This section covers the following topics:

See Also

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

1.1 Introduction

Access Management is the access control component for OpenScape 4000 servers. It controls which users are allowed to access a specific server, and which applications and access rights these users may use. Possible users are customer administrators and service technicians that manage OpenScape systems.

For those users, Access Management creates user accounts, manages their passwords, password attributes and other account-related data, and controls their access via a web browser.

Further features of Access Management are:

- **Web Session Management**
  - Control of users that are currently logged on.
  - Web sessions time out after a configurable amount of time the user is inactive.
  - Web sessions can also be terminated explicitly by using the **Logoff** button, or the Web Session Manager.
- **Network Single Logon (NSL)**
  - Users can log on only once to a OpenScape 4000 network server, being able to access connected OpenScape 4000 systems without further authentication.
  - Security and access control is managed via the NSL password configuration and appropriate access right configuration on the OpenScape 4000 systems.
- **Integration of Windows(TM) Client and Server programs**
  - Windows(TM) programs are also integrated into the OpenScape 4000 authentication and session concept.

  Two ways are offered:
  - Integration into the Start Page of OpenScape 4000 Assistant/Manager: execution of the Windows(TM) client after web-based authentication via the Start Page of OpenScape 4000 Assistant/Manager.
  - Using an authentication library provided by Access Management that avoids the need to use a browser for log on.

- **Emergency Password Reset (EPR)**
  - Emergency Password Reset (EPR) provides a means to reset the administrator (user "engr") password in case the password was lost or the system was corrupted.
- **Password History Configuration**
  - Password History Configuration provides a means to set additional password rules.
- **Control of system accounts**
  - For technical reasons, OpenScape 4000 servers generate a predefined set of Linux accounts used internally by different applications, e.g. for accessing the Database with specific permissions, or to allow attached systems to connect.
  - Access to these system accounts can also be controlled via Access Management. For a detailed list of system accounts please refer to Access Management Security Levels and User Accounts.
- **Managing Web Server certificates (starting with Version 2.0**)
  - Creating Certificate Signing Requests (CSRs) for SSL Security Certificates.
  - Generating, Activating and Importing SSL Security Certificates for the current server.
  - Generating, Activating and Importing SSL Security Certificates for network management.

1.2 Access Management Security Levels and User Accounts

Topics covered in this section:

Security Levels and Predefined User Accounts

System Accounts and Accounts for Network Single Logon (NSL)

See Also

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

1.2.1 Security Levels and Predefined User Accounts

Access Management provides five different **Security Levels**.

Every user that logs on to a OpenScape 4000 server belongs to exactly one of these levels.

For four of them, predefined user accounts with initial passwords are created to grant immediate access to the OpenScape 4000 server.

For security reasons, the initial password must be changed when the user logs on for the first time.

The table below provides a detailed overview of the Access Management security levels and predefined user accounts.

Security Levels

Security Level	Predefined User Account	Initial Password	Linux Shell Access	Owner	Remarks
engr 	engr(1)	4K-admin	yes	Service	Engineer (full system administration privileges). To be used in emergency cases only. Includes all other security levels Assistant only: access to Linux Shell is with superuser rights (uid 0).
rsta 	rsta	4K-admin	yes	Service	Remote Service Technical Assistance (restricted system administration privileges). To be used by upper level service technicians. Includes security level rsca.
rsca 	rsca	4K-admin	yes	Service	Remote Service Customer Assistance (restricted system administration privileges). To be used by lower level service technicians.
cusa 	cusa	c.u.s.a	no	Customer	CUstomer Security Adminstrator (restricted system administration privileges). To be used by the customer's "master" administrator(s). Includes security level cust.
cust 	--	--	no	Customer	CUSTomer level (standard user). Individual accounts can be created at runtime to fit into the customer-specific environment.

(1) Assistant only: by default, logon to root is locked and can be unlocked only via engr.

Related Topics

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts

Accounts for Network Single Logon (NSL)

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

1.2.2 System Accounts and Accounts for Network Single Logon (NSL)

In addition, Access Management manages two other types of accounts that are not used for interactive logon:

- System Accounts

and

- Accounts for Network Single Logon (NSL)

These account types are shown and explained in the tables below.

System Accounts

Account /Category	Icon	Description
System accounts		
syst		Linux accounts created for different purposes to assure proper operation of OpenScape 4000 features and communication to their partner systems. These accounts are not used for interactive logon.

Accounts for Network Single Logon (NSL)

Account /Category	Icon	Description
Network single logon (NSL) accounts		Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.
nsl-syst		System level - used for internal server-server communication of OpenScape 4000 components like System Management, Expert Access/MPCID, Logging Management.
nsl-engr		Network single logon for remote access of service technicians at expert level for emergency cases (engr).
nsl-rsta		Network single logon for remote access of service technicians at upper service level (rsta).
nsl-rsca		Network single logon for remote access of service technician at lower service level (rsca).
nsl-cusa		Network single logon for remote access of customer security administrator (cusa).
nsl-cust		Network single logon for remote access of standard (cust-level) users.

Related Topics

System Accounts

Accounts for Network Single Logon (NSL)

2 Functionality

The following topics are covered in this section:

2.1 Server and Application Access Control

Access Management ensures that every user has to authenticate against a OpenScape 4000 server with a valid account name and password. In case of successful logon, a session is created. Within this session, the user is allowed to access OpenScape 4000 applications according to his/her user profile only. The **Access Management** application itself is also included in this access control. For example, **User Account Administration** tasks are granted to users belonging to the security levels **rsca, cusa** or higher.

Session Management area

The **Session Management** area comprises the following features:

- Change Password

  By default, every user can change his/her password using Change Password. This privilege can be withdrawn by a higher-level user to keep passwords for certain accounts unchanged.
- Password Distribution (OpenScape 4000 Manager only)

  The new Manager-only version of the **Change Password** dialog facilitates administration and distribution of passwords for individual users. Using this feature, you can not only change the password for the current user on the Manager application but also on all selected Assistants.

- Web Session Manager

  The Web Session Manager is used to view and kill running sessions on the server. Depending on the security level of the logged-on user, sessions of other, lower-level users may also be listed. The main purpose of the Web Session Manager is to kill orphaned sessions that have not yet timed out. A session is orphaned if for example a user closes all browser windows without logging off explicitly.
- Emergency Password Reset (EPR)

  Emergency Password Reset (EPR) provides a means to reset the administrator (user "engr") password in case the password was lost or the system was corrupted.

  The Account and Password Policy dialog is used to activate and configure advanced password rules.

Account Management area

The Account Management area is only accessible for users belonging to **rsca, cusa** or higher security levels. This section includes:

- User Account Administration

  Create or delete individual user accounts, and manage their password properties.
- System Account Administration

  Change the password properties of OpenScape 4000 server system accounts, predefined administrator accounts, and Network Security Levels (NSLs).
- Access Right Configuration

  Assign or withdraw access right groups to/from these users, creating individual profiles.
- Access Right Group Configuration

  Create and manage access right groups by sorting application access rights into them.
- Export User Reports

  Display the current user and access right configration data from the server in an HTML file. Export the data into a text file. Import the data into a spread sheet program for further editing or evaluation.

Manage Web Server Certificates area

- Generate Certificate Sign Requestes (CSRs) for SSL security certificates.
- Generate, activate and import SSL security certificates for the current server.
- Generate, activate and import SSL security certificates for network management.

For a summary of **Access Management** features please refer to Access Management-Overview on page 6.

Related Topics

Access Management User Interface page 16

Introduction page 7

Access Management Security Levels and User Accounts page 9

Access Management tab sheet in System Management page 183

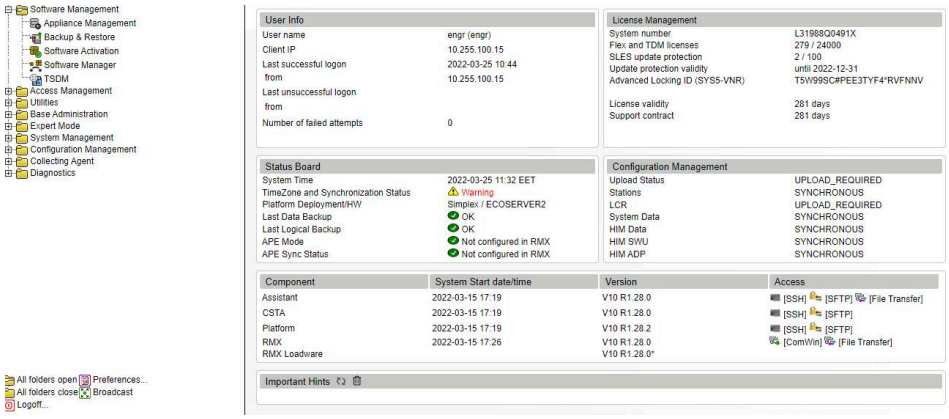
See Also

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.2 Access Management User Interface

After logging on to the Web server, the main functional areas of Access Management are displayed in the form of an application tree in on the **OpenScape 4000 Assistant/Manager Start Page** (referred to as **Start Page** in this publication). Clicking on one of the Access Management links displayed in the application tree launches the corresponding functional dialog in Acess Management. The Start Pages of **OpenScape 4000 Assistant** and **OpenScape 4000 Manager** have slightly different contents in their application trees, but their functionality is the same. On the Start Page you will see only those applications that you are entitled to use based on the license you acquired and based on the rights of the logged-on user.

OpenScape 4000 Assistant Start Page



User Interface Description

Please find the descriptions of icons, controls and other elements of the **Access Management** user interface under the following links:

Content of the Start Page of OpenScape 4000 Assistant/Manager

Toolbar

Menu Bar

Context Menu

Web Session Manager

Change Password

Password Distribution (OpenScape 4000 Manager only)

Emergency Password Reset (EPR)

Account and Password Policy

User Account Administration dialog - User Interface Description

Toolbar Icons - User Account Administration dialog

System Account Administration dialog - User Interface Description

Toolbar Icons - System Account Administration dialog

Access Right Configuration dialog - User Interface Description

Toolbar Icons - Access Right Configuration dialog

Access Right Group Configuration dialog - User Interface Description

Toolbar Icons - Access Right Group Configuration dialog

Related Topics

User Account Administration

System Account Administration

Access Right Configuration

Access Right Group Configuration

Export User Reports

Manage Web Server Certificates Area

Access Management tab sheet in System Management

Introduction

Access Management Security Levels and User Accounts

Server and Application Access Control

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.2.1 Content of the Start Page of OpenScape 4000 Assistant/Manager

The application tree on the **Start Page** contains all licensed applications (user purchased applications) which the current user is authorized to use. To enforce license check, a license ID is stored with every application (which must be registered before the user can use it). For some applications like the applications in the **Direct Access** component (in OpenScape 4000 Manager) or in the **Expert Mode** component (in OpenScape 4000 Assistant), respectively, no registration is required.

The **Start Page** gets all registered applications from License Management, and all applications the user is authorized for from Access Management. Using this information, only applications which are licensed and the user is authorized for are visible in the application tree. If an application requires a network object, at least one instance of the required network object type must be present in the system.

The following functional areas are displayed in the Access Management application tree on the OpenScape 4000 Assistant/Manager Start Page:

Account Management area

Session Management area

License Management

Manage Web Server Certificates Area

2.2.1.1 License Management

License Management is a separate software component which has its own online help.

Related Topics

Content of the Start Page of OpenScape 4000 Assistant/Manager

Toolbar

Menu Bar

Access Management User Interface

2.2.1.2 Session Management area

Session Management covers the following functional components:

- Change Password
- Password Distribution (OpenScape 4000 Manager only)
- Web Session Manager
- Emergency Password Reset (EPR)
- Account and Password Policy

2.2.1.3 Account Management area

The **Account Management** area is divided into the following functional components:

- User Account Administration
- System Account Administration
- Access Right Configuration
- Access Right Group Configuration
- Export User Reports

2.2.1.4 Manage Web Server Certificates Area

The **Manage Web Server Certificates** area comprises the following features:

- Certificates for this Web Server
  - Activate - HG35xx Board NOT Installed
  - Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only
  - Generate
  - Import
  - Generate via CSR

- Certificate Network Management
  - Root Certificate
  - Sign CSR

2.2.2 Toolbar

The icons in the **Toolbar** have the same functions as the corresponding menu entries. For descriptions of the individual toolbar icons please refer to the individual components, as follows:

Toolbar Icons - User Account Administration dialog,

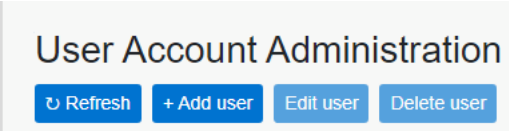
Toolbar Icons - System Account Administration dialog,

Toolbar Icons - Access Right Configuration dialog,

Toolbar Icons - Access Right Group Configuration dialog.

2.2.3 Menu Bar

The **Menu Bar** is displayed with all components of the **Account Management** section, except for the **Export User Reports** feature, which has no menu bar.



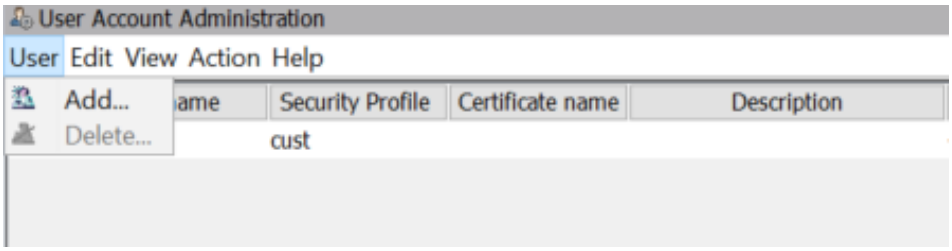
The content of the **Menu Bar** may vary. Depending on the component and functionality selected, different menus will be displayed.

The **Edit**, **View**, **Action** and **Help** menus are displayed with all main components of the **Account Management** area, except for **Export User Reports**, which has no menu bar.

The components of the **Session Management** area do not have a menu bar.

User menu

The User menu menu is only displayed in the User Account Administration dialog.



Edit menu

The options in the Edit menu may vary, depending on the software component selected. For further details, please refer to the descriptions of the individual components:

Edit menu - User Account Administration

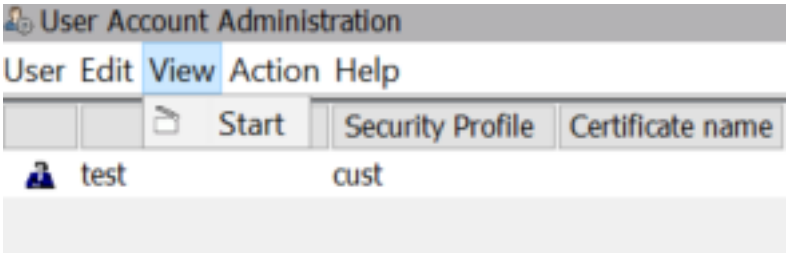
Edit menu - System Account Administration

Edit menu - Access Right Configuration

Edit menu - Access Right Group Configuration

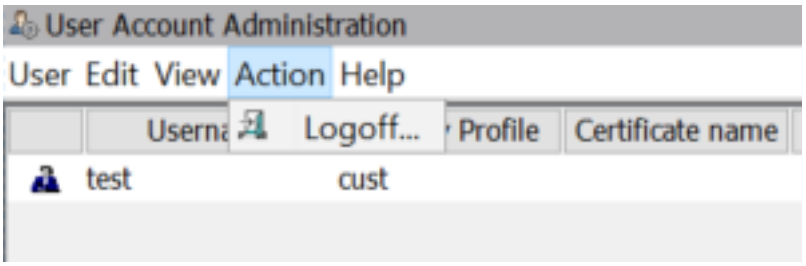
View menu

The options displayed in the **View** menu may vary, depending on the software component selected. In the User Account Administration and System Account Administration components, the **View** menu only contains the **Start** option which brings you back to the OpenScape 4000 Assistant/Manager Homepage. In the Access Right Configuration and Access Right Group Configuration components the View menu contains component-specific options. For details, please refer to the corresponding sections. As an example, the **View** menu of the Access Right Group Configuration is shown below.

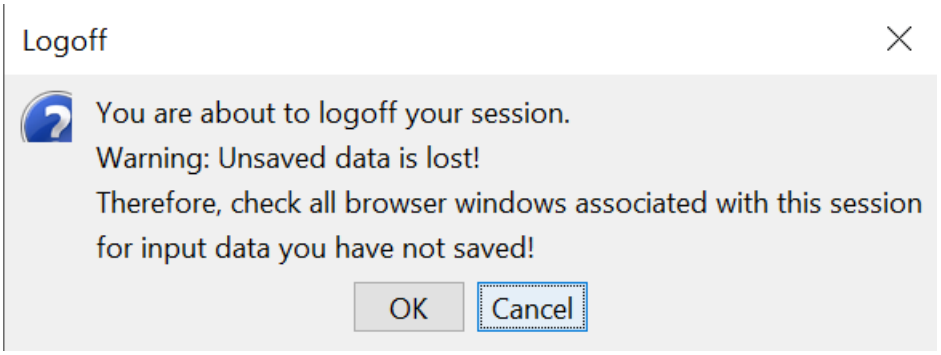


Action menu

The **Action** menu contains the **Logoff** menu option, which has the same function as the **Logoff** icon in the toolbar in the upper right corner of the screen. See also Toolbar Icons - User Account Administration dialog.



When you click the **Logoff** menu option or the icon in the toolbar, an error message dialog is displayed, warning you that all unsaved data will be lost, and prompting you to save all your data, close all browser windows belonging to the current session, and confirm that you want to log off.

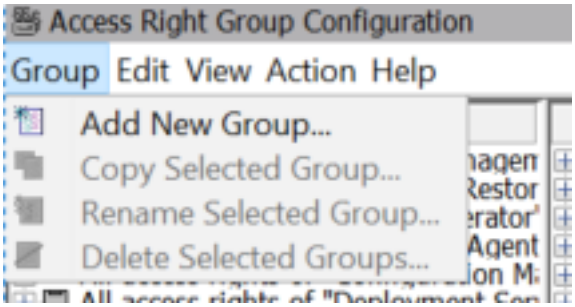


Help menu

The **Help** menu is displayed with all components of the **Account Management** area, except for **Export User Reports**. The **Help** menu options **Context Help**, **Help Topics**, **About** are the same for all components. For details, please refer to the corresponding component, e.g. Help menu - User Account Administration.

Group menu

The **Group** menu is only displayed in the Access Right Group Configuration dialog.



Icons and Controls

For a description of the icons, controls and columns of the Access Management user interface, please refer to the following sections:

User Account Administration dialog - User Interface Description

Toolbar Icons - User Account Administration dialog

System Account Administration dialog - User Interface Description

Toolbar Icons - System Account Administration dialog

Access Right Configuration dialog - User Interface Description

Toolbar Icons - Access Right Configuration dialog

Access Right Group Configuration dialog - User Interface Description

Toolbar Icons - Access Right Group Configuration dialog

Related Topics

Server and Application Access Control page 14

Access Management User Interface page 16

Introduction page 7

Access Management Security Levels and User Accounts page 9

2.2.4 Context Menu

To open the **Context Menu**, press the **right mouse key**. The commands displayed in the Context Menu are always related to the current working environment. The Context Menu always contains only commands relating to the current user interface area, used for editing the currently selected settings. Only relevant commands can be selected; commands which are not relevant are greyed out.

Selecting items

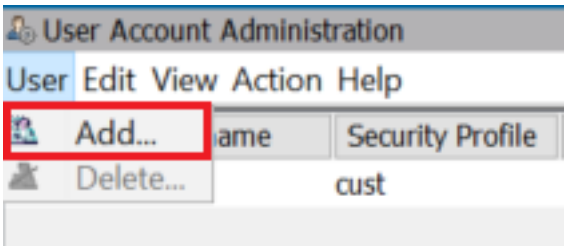
Before executing commands you need to select the required items or users, respectively.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

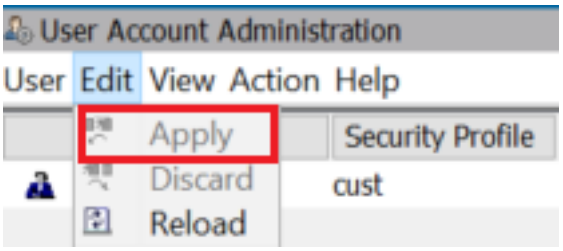
To select multiple **non-consecutive** items or to deselect individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Overview of Context Menu Commands (Examples):

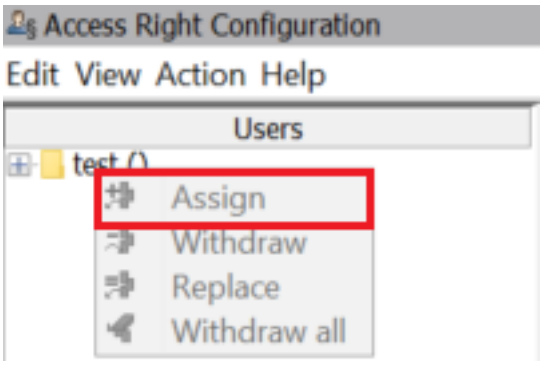
User Account Administration, User List (Left Hand Side Area)



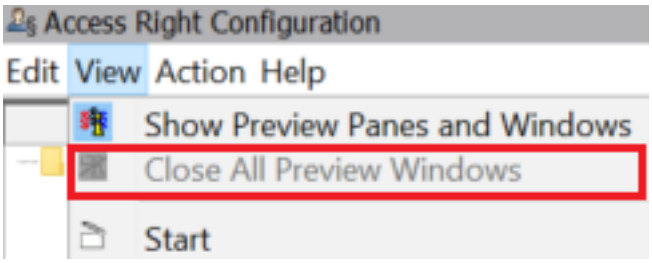
User Account Administration, Right Hand Side Area



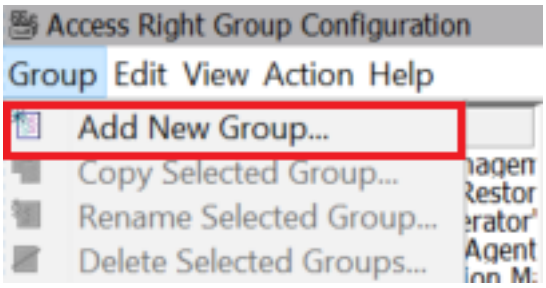
Access Right Configuration, Left and Right Hand Side Area



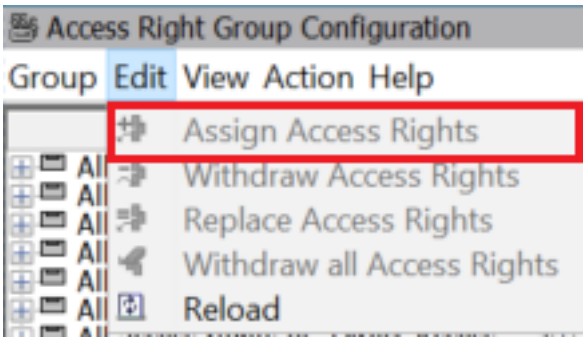
Access Right Configuration, Preview Pane



Access Right Group Configuration, Left Hand Side Area



Access Right Group Configuration, Left Hand Side Area



2.3 Web Session Manager

The **Session Manager** dialog displays the list of all running sessions that the current user is allowed to manage. This includes all sessions owned by the user and (in addition) all sessions owned by users with lower security levels - see Access Management Security Levels and User Accounts. The main purpose of the Web Session Manager is to kill orphaned sessions that have not yet timed out. A session is orphaned if for example a user closes all browser windows without logging off explicitly.

The Session Manager comprises of the following functional areas:

Session Settings

Existing Sessions

2.3.1 Session Settings

The following settings are displayed and can be entered under **Session Settings**:

- **The current value of the session inactivity timeout is xx minute(s)/ hour(s)/day(s)/week(s)/month(s).** This setting determines the currently set timeout value for inactive sessions. Inactive sessions will become invalid (and will automatically be deleted) when the timeout value is reached.

  Only administrators with appropriate access rights are allowed to change this value. When the value is changed, all running sessions or all users are deleted immediately; for all new sessions, the new value is valid.
- **The maximum count of concurrent sessions for one user is: xx**. This setting determines the current value set for the maximum number of concurrent sessions allowed for one user account.

  Only administrators with appropriate access rights are allowed to change this value.
- **The maximum count of concurrent sessions for your user account is: xxx** This setting determines the current value set for the maximum number of concurrent sessions.

  Only administrators with appropriate access rights are allowed to change this value.

Field Descriptions

See Session Settings

See Also

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.3.2 Existing Sessions

The **Existing Sessions** table displays the list of all running sessions that the current user is allowed to view and edit based on his/her privileges. Each table row corresponds to one session. Each session is described as a set of session properties, made up of **# (Sequential Number)**, **Kill**, **Mark**, **Account**, **Session**, **Client**, **Logon Time**, **Last Access**. The own session is marked by an asterisk (*); killing this session puts you back immediately to the logon screen without any warning.

Field Descriptions

(Sequential Number)

Kill

Mark

Account

Session

Client

Logon Time

Last Access

Sorting the Existing Sessions list

You can sort the entries in the **Existing Sessions** table (by **Account**, **Session**, **Client** (IP-Address**)**, **Login Time** and **Last Access**) by clicking on the column titles displayed as links (unterlined).

Clicking on a column title sorts the table by this column.

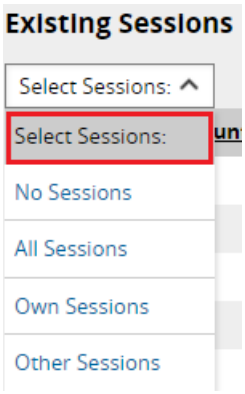
An arrow adjacent to the column title indicates the column by which the table is currently sorted, and it also shows the current sorting order (ascending or descending). Clicking on the column title again inverts the sorting order, e.g. from ascending to descending, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

These columns can be sorted but not edited.

Dropdown Menu "Select Sessions"

The **Select Sessions** dropdown box supports you in selecting and displaying specific sessions. Just click on one of the available options to display only sessions matching the selected option.



You can choose between the following selection criteria for displaying specific sessions:

No Sessions -> De-select all sessions

All Sessions -> Select all sessions

Own Sessions -> Select all sessions of which you are the owner

Other Sessions - Select all sessions with the exception of the sessions you own

Displaying NSL accounts during Network Single Logon using the NSL account

Using the **Network Single Logon** access method you have the possibility to log on without a password from a OpenScape Manager or RSP system. Sessions of this type are displayed as e.g. **htsadm@218.1.16.35** in the **Account** column. As you can see, not only the account name **htssvc0** or **htsadm** is displayed, but also the IP address **account@IP_address** of the server from which the access originated, i.e. of the server on which the user actually logged in. The solution provided up to now for NSL access performed a kind of "session re-

mapping" to an existing account. The new solution creates a dynamic account composed of **account@IP_address**. In the **Logging Management** application this account is displayed accordingly as **account@IP_address** in the **User** column. The **Details** column in Logging Management shows the complete path and the mapping of the Network Single Logon.

Check Boxes

mark	Marks a session for later deletion using the button **Kill all marked sessions**.

Buttons

Kill all marked sessions 	Clicking on **Kill all marked sessions** deletes the marked sessions and brings the associated users immediately back to the **Logon** screen.
kill 	Clicking on the icon  (Kill this session) in the **kill** column will delete a single session and bring the associated user back to the **Logon** screen.

Field Descriptions

(Sequential Number)

Kill

Mark

Account

Session

Client

Logon Time

Last Access

Related Topics

Change Password

Password Distribution (OpenScape 4000 Manager only)

Emergency Password Reset (EPR)

Account and Password Policy

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Server and Application Access Control

User Account Administration

System Account Administration

Access Right Configuration

Access Right Group Configuration

Export User Reports

Access Management tab sheet in System Management

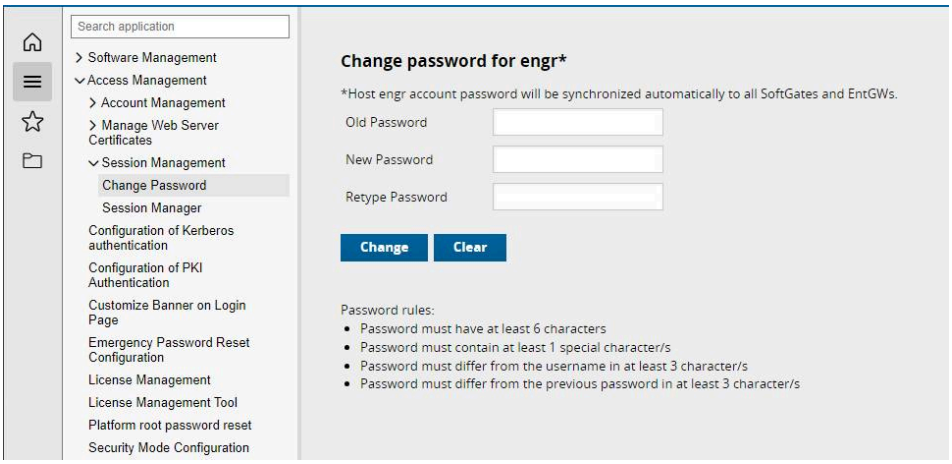
Introduction

Access Management Security Levels and User Accounts

2.4 Change Password

NOTICE: This section describes those parts of the **Change Password** feature that are identical for both the OpenScape 4000 Manager and Assistant. The feature **Password Distribution** is only available for the Manager and described in the Section Password Distribution (OpenScape 4000 Manager only).

The **Change Password** dialog is used to change the user's password. This dialog is only displayed if the current user has the necessary access rights to change the password.



Buttons

Change	Clicking on this button will apply the changes made, and the new password will become valid for future sessions.
Clear	Clicking on **Clear** deletes the contents of the entry fields, leaving them blank for new entries.

Password Rules

The rules for entering valid passwords are displayed in the **Change Password** dialog:

- Password must have at least 6 characters
- Password must not have more than 16 characters
- Password must contain at least one special character (neither digit nor letter)
- Password must differ from the username in at least three positions
- Password must differ from the old password in at least three positions

Additional Password Rules when Password History is enabled

In the Account and Password Policy dialog additional password and account rules as set in this dialog become can be enabled.

Note that administrators with superuser privileges are able to bypass these rules. Thus, it can happen that your old password is not conformant to these rules, while setting a new password forces you to obey the rules.

Field Descriptions

Old Password

New Password

Retype Password

Change

Clear

Related Topics

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Web Session Manager

Password Distribution (OpenScape 4000 Manager only)

Emergency Password Reset (EPR)

Account and Password Policy

Server and Application Access Control

User Account Administration

System Account Administration

Access Right Configuration

Access Right Group Configuration

Export User Reports

Access Management tab sheet in System Management

Introduction

Access Management Security Levels and User Accounts

2.5 Password Distribution (OpenScape 4000 Manager only)

This new Manager-only version of the **Change Password** dialog facilitates administration and distribution of passwords for individual users. Using this feature, you can not only change the password for the current user on the Manager application but also on all selected Assistants. (This feature is only available on the OpenScape 4000 Manager.)

2.5.1 Configuration

2.5.1.1 Assignment of Assistants

First, the Assistants have to be assigned to a user. This user has to be available on the assigned Assistants, i.e. there has to be an account for this user. The passwords of all these user accounts on the individual Assistants have to be identical, and changing of passwords needs to be allowed (i.e. the checkbox **Allowed to change password** in the User Account Administration dialog has to be checked (see User Account Administration)).

The user cannot adjust the assignment; this has to be done by the user called "**engr**" on the Manager.

Using a text processor, the user adds an IP address to the two files
`/var/secm/pwddist/<username>.cnf`
`/var/secm/pwddist/global.cnf`

Of course you can use the "vi" text processor for this task.

If you are not familiar with "vi", change to the folder "**/var/secm/pwddist**" and use the following command for each Assistant and each IP address:
`echo "192.023.045.056" >> global.cnf`

The file "**global.cnf**" is used for all users for which there is no user-specific file called **<username>.cnf**.

If the user's name is e.g. "Miller" and there is a file called "**Miller.cnf**", only the password of those Assistants listed in the file "Miller.cnf" is updated. If there are no Assistants listed in the file, the password is only changed locally on the Manager.

If the file "**Miller.cnf**" does not exist, the user accounts of the Assistants listed in the file "**global.cnf**" are updated.

NOTICE: It is not mandatory that the Assistants the IP addresses stand for are entered in System Management. In real life, however, this usually does not happen.

In addition, the log files are created in the folder
`/var/secm/pwddist/log`

2.5.1.2 Notes on Configuration

Please note:

1) The IP addresses of the Assistants assigned must exist. The Assistant have to be accessible via this IP address. Otherwise, the entry
   `"error while executing execurl: 10"`
   will be found in the log file.
2) The user accounts of the user whose password is to be changed have to have the same name on all Assistants assigned. Otherwise, nothing is

changed on the Assistants where the user account does not exist, and the entry
`"error while executing execurl: 11"`

will be found in the log file.

3) All user accounts of a user must have the same password on all Assistants assigned. Otherwise, nothing is changed on the Assistants where the password is different, and the entry
`"error while executing execurl: 11"`

will be found in the log file.

4) The user must have the right to change his password on all Assistants. Otherwise, nothing is changed on the Assistants where the user does not have the right to change his password. You would expect an error message; however, the log file contains the following success message:
`successfully reset password for user [User]`

5) The user must have the right to change his password on the Manager.

2.5.2 Procedure

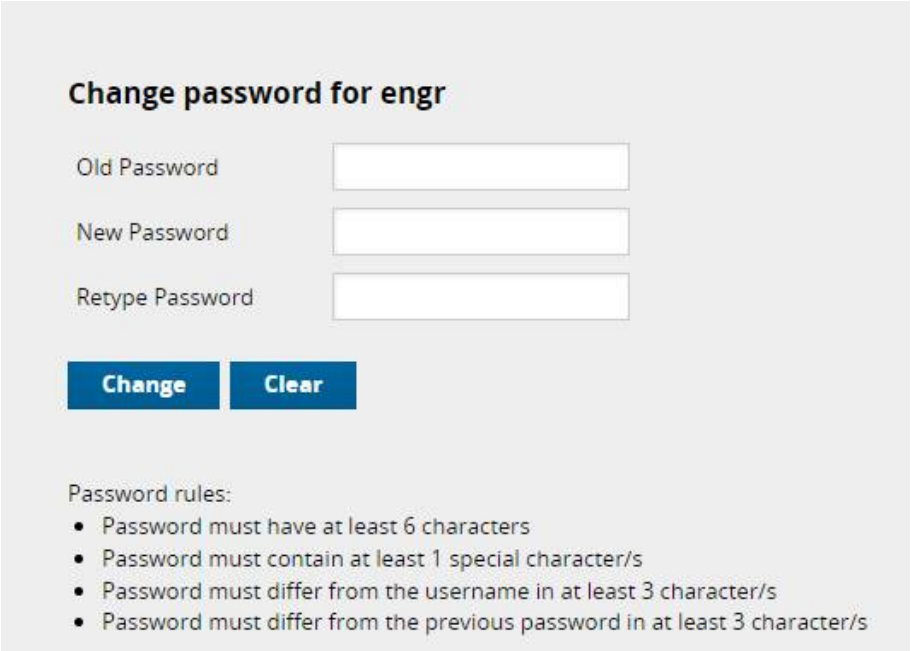
2.5.2.1 Notes

1) The changes are done by the user him-/herself, not by an administrator.
2) The user is responsible for changing the password at regular intervals.
3) New user accounts incl. passwords have to be set up manually by the administrator directly in the Assistant.
4) Any change on an assigned Assistant is individual and does not effect changes on the other Assistants, i.e. if some change fails on one Assistant, the process is not stopped but continues with the next Assistant. Therefore, it may happen that the passwords are changed on all but one Assistant. In order to obtain a consistent system again, the user has to manually make the changes directly on this Assistant in this case.
5) The passwords are changed one after another. Changing multiple passwords on different Assistants may take a while. Only after all passwords have been changed, the next changes can be started.

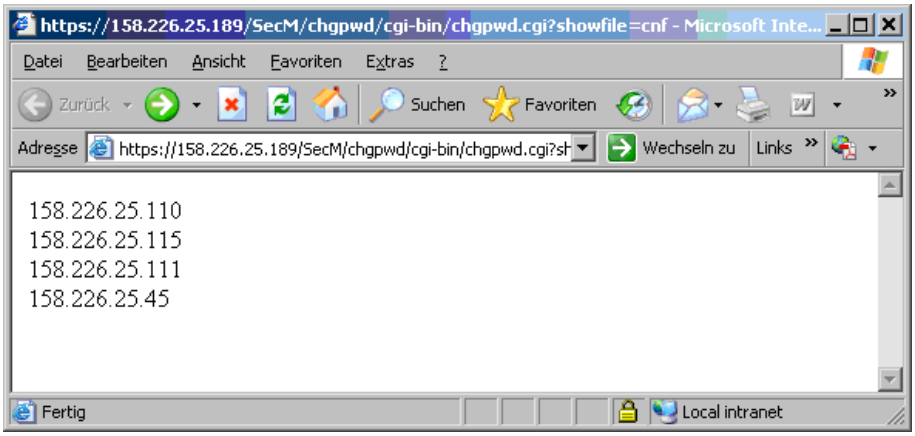
2.5.2.2 Step by Step

1) Log on to the Manager.

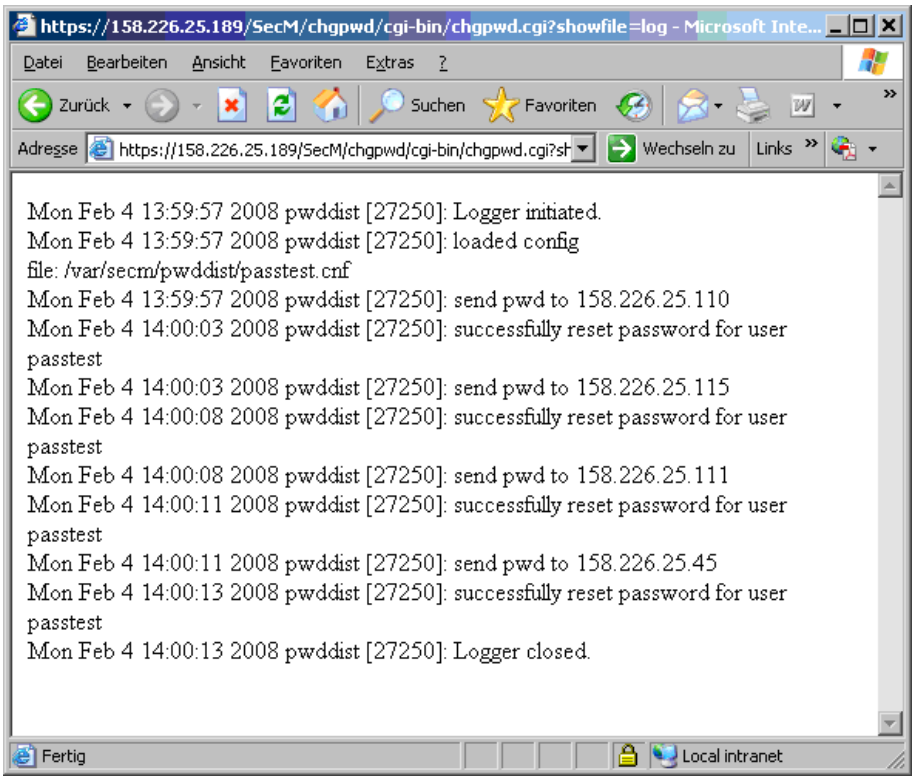
2) Navigate to **Change Password** via **Access Management** and **Session Management**. The Manager-only version of the **Change Password** dialog is displayed.



3) Enter the old password and the new password and confirm the new password in the respective entry fields (see Change Password).
4) If you do **not** check the checkbox **Change the password also on Assistants (Password Distribution)**, the password change only effects the local Manager.
5) If you check the checkbox **Change the password also on Assistants (Password Distribution)**, all passwords on the Assistants assigned are also changed.
6) If you click on the **Assistants** link, the Assistants assigned are displayed in a new window.



7) If you click on the **Log file** link, a log file with the results of the latest change procedure is displayed in a new window.



Field Descriptions

Old Password

New Password

Retype Password

Change the password also on Assistants (Password Distribution)

Change

Clear

Related Topics

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Web Session Manager

Change Password

Emergency Password Reset (EPR)

Account and Password Policy

Server and Application Access Control

User Account Administration

System Account Administration

Access Right Configuration

Access Right Group Configuration

Export User Reports

Access Management tab sheet in System Management

Introduction

Access Management Security Levels and User Accounts

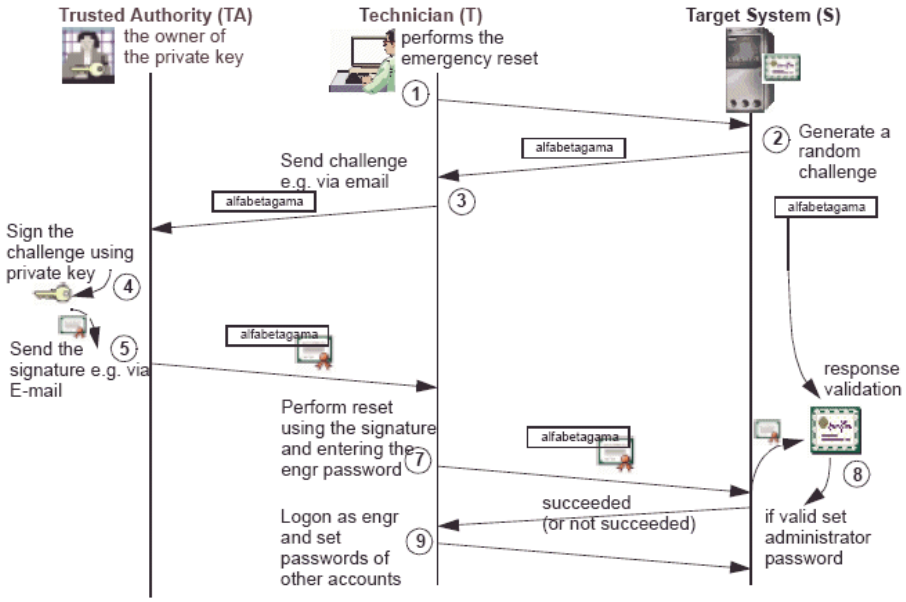
2.6 Emergency Password Reset (EPR)

Emergency Password Reset (EPR) provides a means to reset the administrator password of the Assistant, in case the password was lost or the system was corrupted.

Prior to using that feature, the system must be configured appropriately, and the feature must be enabled by the system administrator.

To allow the feature to be functional, the configuration must include an import of a certificate from a Trusted Authority of the system. The certificate is expected in X.509 PEM format. The user is authenticated and allowed to change password, judging his ability to sign a random message - issued by the system - with the private key of the certificate holder. The signature response must be a SHA512 message digest; no other algorithms are supported. The system is able to verify the submitted response using the installed certificate's public key. If verification succeeds, the emergency reset initiator is allowed to change the administrator password.

The work flow concept of the feature is as follows:



2.6.1 EPR - Configuration

Preparing the system for emergency reset:

- The administrator enables the feature, configures the general settings (see EPR-General configuration),

  and

- Imports a certificate - public key (see Installing a certificate)

The certificate's private key must be stored securely by a Trusted Authority. It is not relevant, if the certificate is issued by a 3rd party Certification Authority (CA) or it is a customer self-signed certificate. Both are accepted and neither the authenticity of the certificate, nor its revocation is checked during import.

Example of generating a self-signed certificate:

```
openssl req -x509 -newkey rsa:2048 -keyout epr-self.key -
out epr-self.crt -days 3650
```

This command involves a dialog to create the self-signed RSA 2048-bit certificate. The passphrase for the private key (epr-self.key) and the certificate properties must be entered. The passphrase and the private key must be stored securely on distinct locations by the Trusted Authority.

Variant for ECDSA certificate:

```
openssl req -x509 -newkey ec -pkeyopt
 ec_paramgen_curve:secp384r1 -keyout epr-self.key -out epr-
self.crt -days 3650
```

During emergency password reset

- **Step 1:** The user initiates the password reset via a public page or a terminal login.
- **Step 2:** The user requests a random challenge (random 32-byte long string) from the system (see Requesting a new challenge).
- **Step 3:** The user requests the Trusted Authority to sign the random challenge with the certificate's private key.
- **Step 4-5:** The Trusted Authority signs the random challenge and sends it back to the administrator. The signature must be a SHA512 digest. No other digest algorithms are accepted.

  The challenge can be signed by the Trusted Authority with the following command:

  ```
  openssl dgst -sha512 -sign private.key -out response.sha
   challenge
  ```

  where

  – `private.key` is the private key of the imported certificate.
  – `challenge` is the file with the challenge.

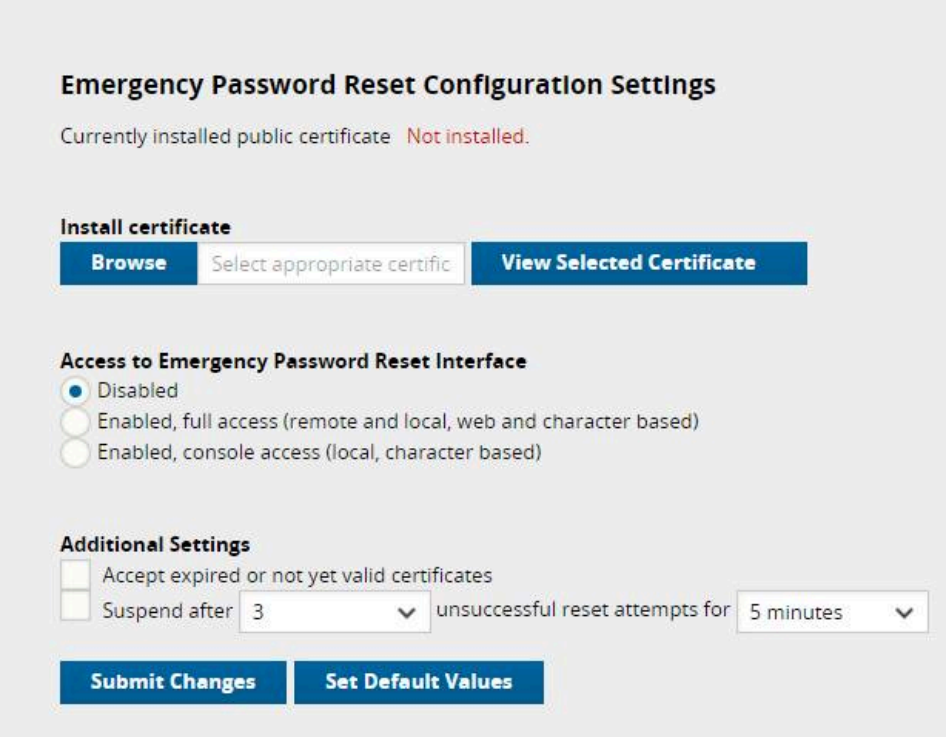
    Please note, that the file with challenge must **NOT** contain the end-of-line character.
  – `response.sha` is the file with the signed challenge.

  The transformation of the signed challenge to BASE64 format (PEM) can be done with the following command:

  ```
  openssl enc -base64 -in response.sha > response.sha.b64
  ```

- **Step 6:** The user submits a signed challenge to the system (see Challenge).
- **Step 7:** The system verifies the challenge against the installed certificate's public key.
- **Step 8:** If the verification succeeds, the user is allowed to change the Assistant's, administration password (see Execute password reset).

2.6.1.1 EPR-General configuration



How to Access the General EPR Configuration Window

- This window is only available to the system administrator, e.g. to the user account "engr".
- The window is invoked from the **Start Page** using the menu **Access Management** > **Emergency Password Reset Configuration Settings**

EPR Configuration Window - Toolbar Items

The Toolbar contains the following buttons:

Help => Opens the online help and displays the help index

Home => Links to the Launchpad

Start => Opens a new browser window which displays the homepage of the OpenScape 4000 Manager.

Logoff=> Logs off the current user, closes the running session for all associated browser windows and returns to the login screen..

Installing a certificate

- Click **Browse** to select a file which contains the certificate managed by Trusted Authority.

  NOTICE: Only X.509 PEM formatted certificates are accepted.

- Click **View Selected Certificate** to show details of selected certificate.

  See Certificate Details, page 44.

- Click **Submit Changes** to save the current settings.

  Or

- Click **Set Default Values** to discard the changes and reset to the default values. The certificate is left unchanged.

Options for Accessing the Emergency Password Reset Interface

The access to the Emergency Password Reset con be configured using the following options:

- **Disabled:** Feature Disabled (no EPR possible)
- **Enabled, full access:** EPR possible via browser and terminal login
- **Enabled, console access:** EPR possible via terminal login

Additional Settings

- **Accept expired or not yet valid certificates:** do not check certificate validity during install
- **Suspend:** suspend feature after specified invalid attempts for a specified time.

2.6.1.2 Certificate Details

Purpose of this window

The **Certificate Details** page shows the details of the selected certificates.

- Click **Back to Configuration Settings** to close the window and return to the configuration page.
- See EPR-General configuration, page 42.

2.6.2 EPR - Reset

2.6.2.1 Requesting a new challenge

NOTICE: A challenge is a 32 byte long random alphanumeric string. When saved to file it must be treated 'as-is': no character encoding, no terminating newline, etc.

In order to request a new challenge:

- Open the "Emergency Password Reset" window by clicking on the **Emergency Password Reset** link in the Login Page.
- Then, click on the **New Challenge** button to generate new random challenge. As a result, the **Reset** page is displayed (see Resetting the password).

2.6.2.2 Resetting the password

Challenge

The generated challenge is displayed in the **Challenge** text field.

- Click **New Challenge** to discard the current challenge and request a new one
- Click **Cancel Challenge** to discard the current challenge

---

NOTICE: A valid response is a SHA512 message digest generated by the Trusted Authority ofinstalled certificate. This is a 256 byte long binary file. No other message digest method is supported.

Response

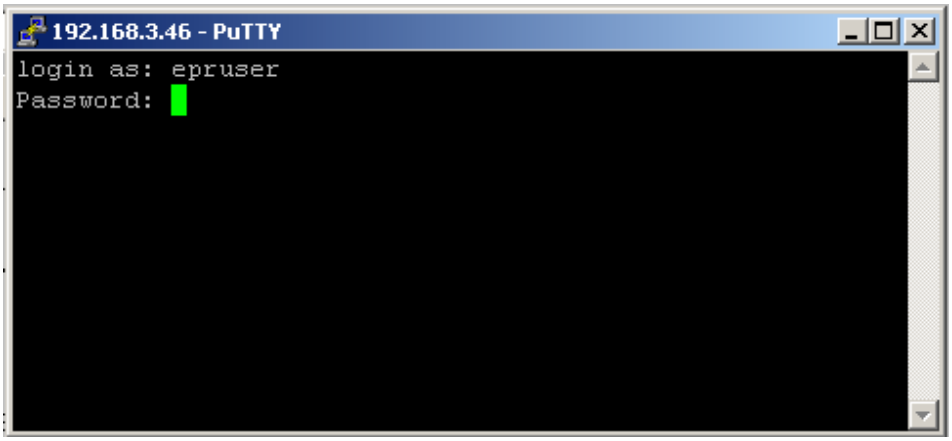
- In the **Response** text field, enter a BASE64 encoded response,

  or
- Click **Browse** to select binary or BASE64 encoded response file.
- Click **Set Password** to reset the administrator password.

Setting a new administrator password

- In **New Password**, type the new administrator password
- In **Retype password**, approve the new password by retyping.
- Click **Set password** to send the request to the server.

2.6.3 EPR - Resetting via the console



- Login as: "epruser" (without quotation marks) and public password: "epr2000$" (without quotation marks).

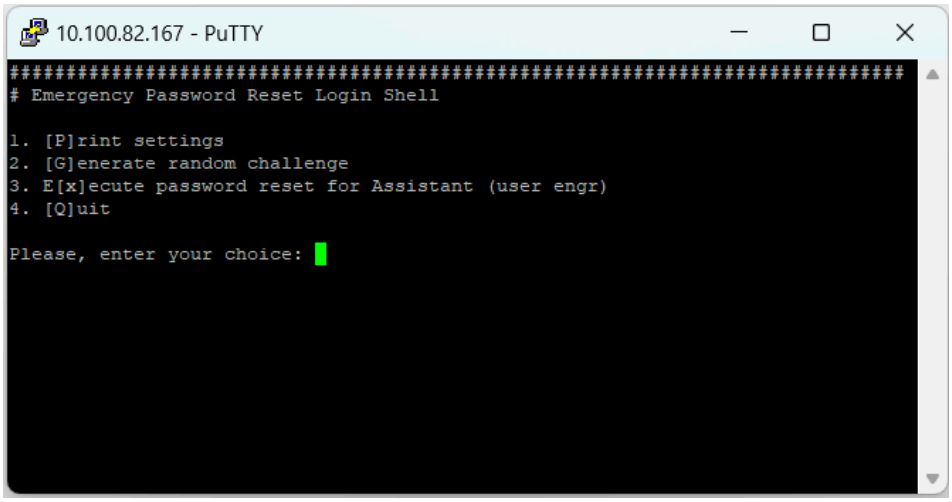


Figure 1: EPR login shell, initial menu

The **Emergency Password Login Shell** displays the following options.

1) Print current settings [P]
2) Generate new random challenge [G]
3) Execute password reset for Assistant (user engr) [x]
4) Quit [Q]

- Type the letter shown in brackets for the required option and press [ENTER].

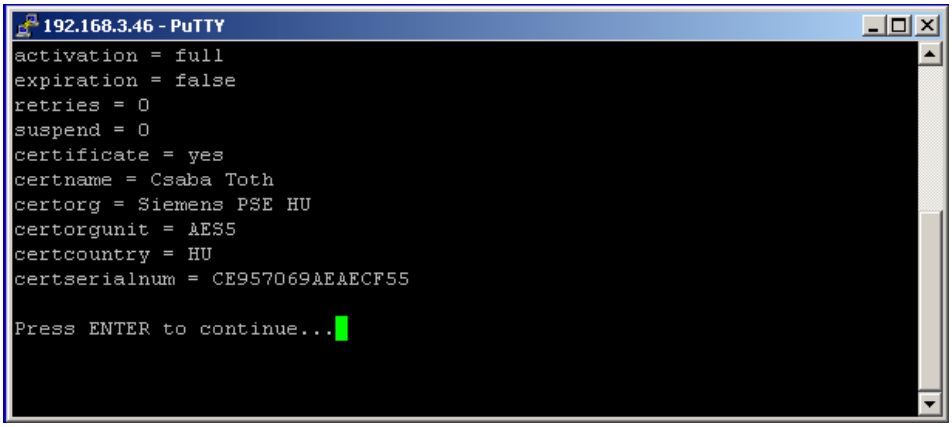
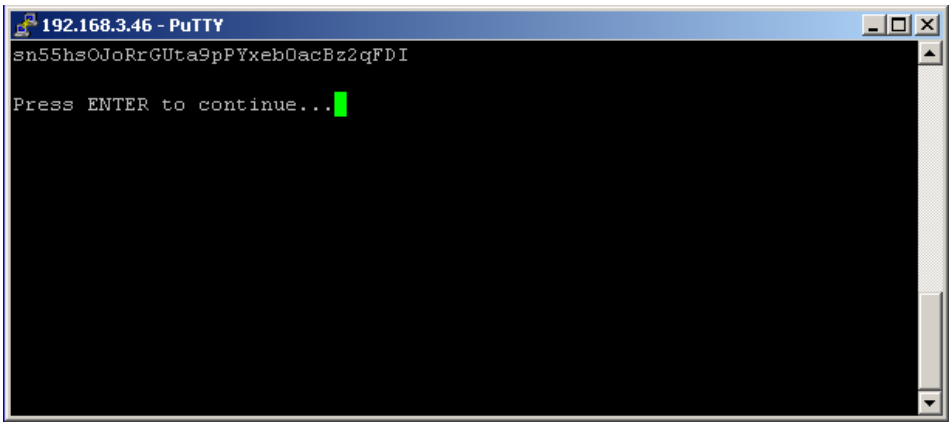


Figure 2: Print current settings

- Press [ENTER] to show more of the current settings.
- At hte end of the list, press [ENTER] to return to the initial menu.

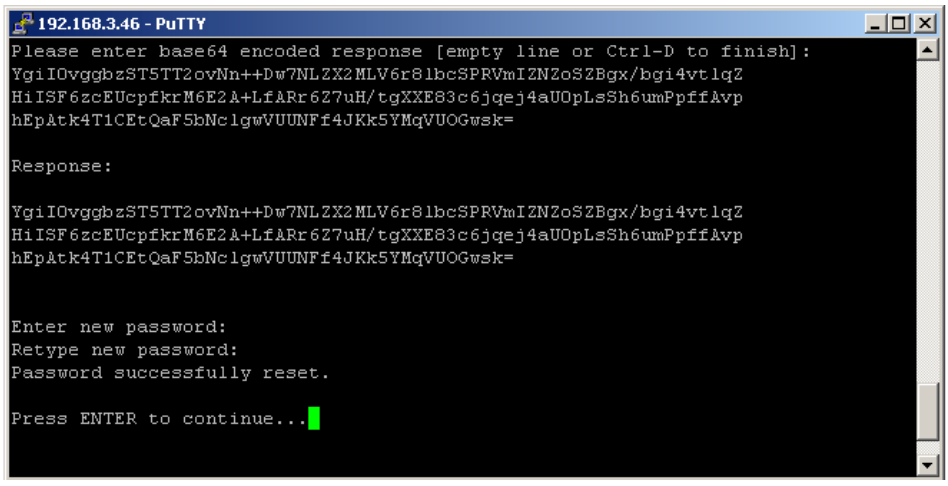
Generate new random challenge



A new random challenge is generated and displayed.

- Press [ENTER] to return to the initial menu.

Execute password reset



- After Response, enter a response by pasting a BASE64 encoded response.
- Enter a new line or press [Ctrl]-[D] to complete the input.
- In Enter new password, type the new password.
- In Retype new password, repeat the new password.
- Press [ENTER] to return to the initial menu.

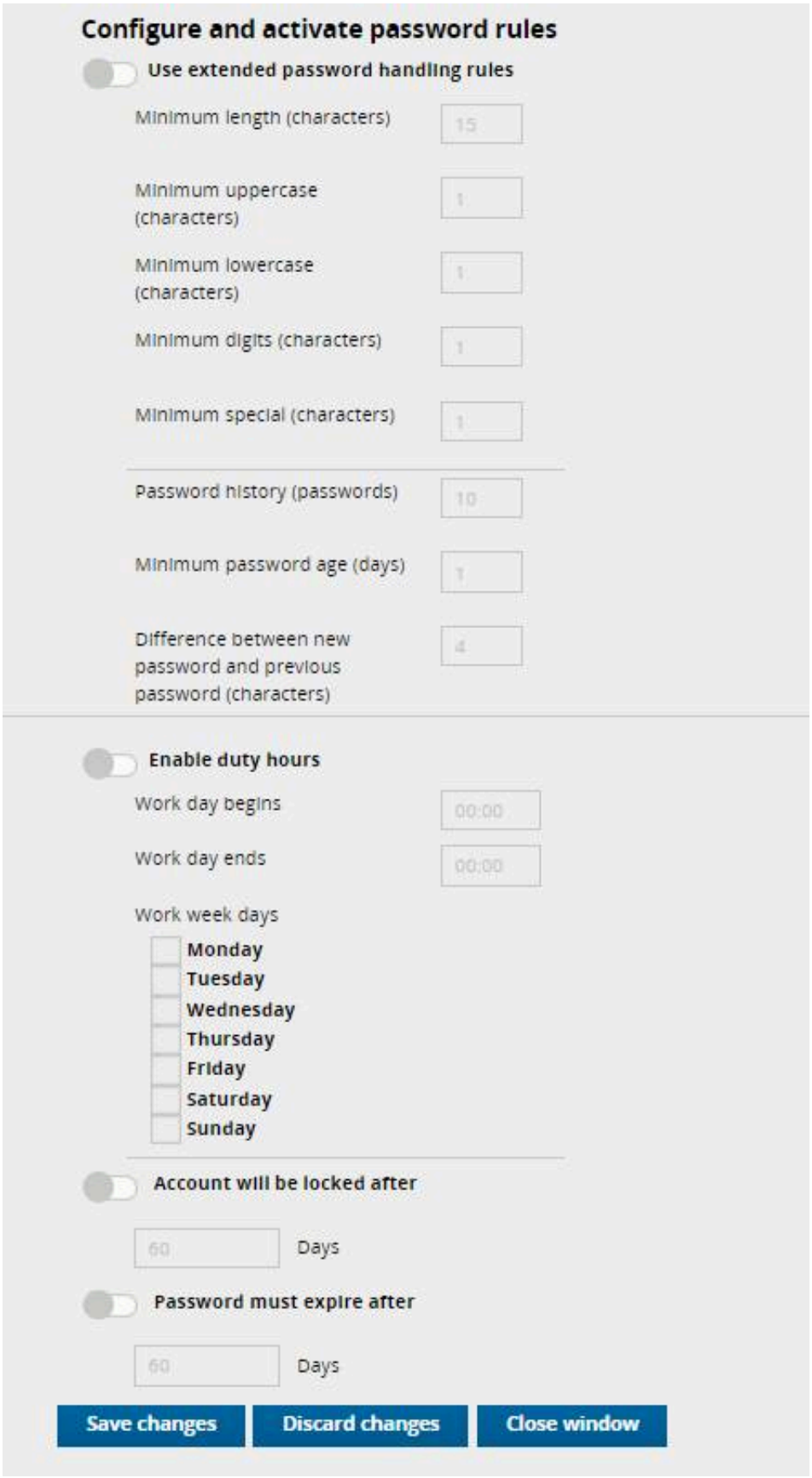
2.7 Account and Password Policy

The **Account and Password Policy** dialog is used to activate and configure advanced rules for password policies and rules for time-controlled account use.

Start the application

The **Configuration** page for configuring account and password policy is accessible from the start page:

Account Management -> Account and Password Policy


Configure and activate password rules
Use extended password handling rules
Minimum length (characters)
15
Minimum uppercase (characters)
1
Minimum lowercase (characters)
1
Minimum digits (characters)
1
Minimum special (characters)
1
Password history (passwords)
10
Minimum password age (days)
1
Difference between new password and previous password (characters)
4
Enable duty hours
Work day begins
00:00
Work day ends
00:00
Work week days
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Account will be locked after
60
Days
Password must expire after
60
Days
Save changes
Discard changes
Close window

Guidelines for Password Policies

All account passwords, both administrative and non-administrative, must comply with the following rules (for possible **xx** values and more information, please refer to **Field Descriptions)**:

- Passwords must be at least **xx** characters long.
- Passwords must contain a specified mix of upper case letters, lower case letters, numbers, and special characters.
- Re-use any of the previous **xx** passwords must not be possible.
- Change of passwords must not be allowed more than once in **xx** days, except in the case of an administrator or a privileged user. Privileged users may be required to reset a user's forgotten passwords and the ability to change passwords more than once per day.
- When a password is changed, the new password must differ from the previous password by at least **xx** characters.
- When a password is changed, users must not be able to use dictionary words.

  For the dictionary check the cracklib is used with the default database `/usr/share/cracklib/pw_dict.pwd`, which is installed by OS (currently SLES10 SP3).

NOTICE:

The password and account rules are only enabled if the corresponding checkboxes are checked. The '`passwd`' command line tool is disabled!

At least one login is necessary after creating an account or after an account is unlocked. Otherwise, the account will be blocked after the number of days set in the **Configure and Activate Password Rules** section.

Field Descriptions

Use extended password handling rules

Enable duty hours

Account is locked after: xx days of inactivity

Password must expire after: xx days

Related Topics

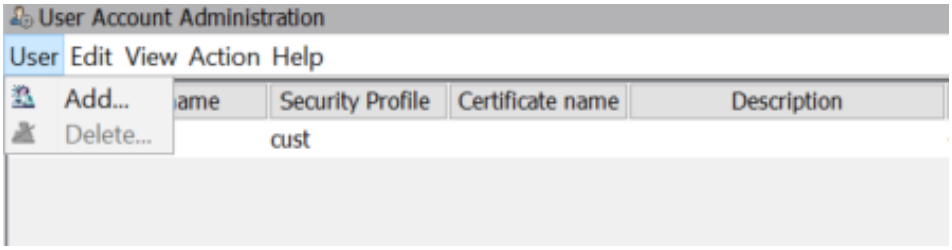
Change Password

Emergency Password Reset (EPR)

2.8 User Account Administration

The **User Account Administration** dialog is used to add users to or delete users from the system, or to modify the password properties of a selected user or group of users.

To modify the access rights of these users, use the **Access Right Configuration** dialog.



Left Hand Side Area (User List)

The columns in the left hand part of the dialog show the User Accounts List, User Account Administration dialog list of currently registered users and their account settings.

Selecting Multiple Users

This dialog offers the possibility to select multiple users and to set or change properties to the same value for multiple users with a single click. When you click on **Apply** a dialog prompt will notify you that the password properties of multiple users are being changed.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non**-consecutive items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Right Hand Side Area

The right hand side of the **User Account Administration** dialog contains the following areas:

- **Identification area**,
- Actions area,
- Properties area,
- Autolock area.

These areas are used to define or edit the properties of existing and new user accounts. For a detailed description of this area, please refer to Areas in the User Account Administration dialog on page 259, and Controls and Buttons in the User Account Administration dialog on page 260.

The **User Account Administration** dialog contains the following UI components:

- User Accounts List, User Account Administration dialog
- Toolbar Icons - User Account Administration dialog
- Menu Bar
- Toolbar

  The **Toolbar Icons** have the same functionality as the entries in the main menus. For a detailed description of the icons in the toolbar, see Toolbar Icons - User Account Administration dialog.
- Context Menu
- User menu
- Edit menu - User Account Administration
- View menu, User Account Administration
- Action menu, User Account Administration

- Help menu - User Account Administration
- User Account Administration dialog - User Interface Description
- Columns in the User Account Administration dialog
- Areas in the User Account Administration dialog
  - **Identification area**,
  - Actions area,
  - Properties area,
  - Autolock area.
- Controls and Buttons in the User Account Administration dialog

Field Descriptions

User Name

Security Profile

Description

New Password

Retype Password

Delete Password

Force password change

Max. password validity

Password never expires

Lock user account

Allowed to change password

Access through Network Single Logon only

Lock account automatically

occurring during

Unlock it automatically

Apply (Button)

Discard (Button)

Reload

Related Topics

Columns in the System Account Administration dialog

Areas in the System Account Administration dialog

Controls and Buttons in the System Account Administration dialog

Export User Reports

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.8.1 User Accounts List, User Account Administration dialog

User Accounts List - Displaying the Configured User Data, Access Rights and Properties

The **User Accounts List** on the **left hand side** of the **User Account Administration** dialog displays the list of all user accounts registered in the **Access Management** application. The user account data and properties are described in: Columns in the User Account Administration dialog

User Accounts List - Changing User Data and Password Settings

The **right hand side** pane of the **User Account Administration** dialog displays the Areas in the User Account Administration dialog containing the fields and controls used to change the user data and password settings of one or more users.

- **Identification area**,
- Actions area,
- Properties area,
- Autolock area.

NOTICE: Only users with appropriate administrator privileges are permitted to change password settings.

Related Topics

User Account Administration

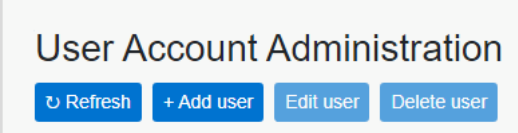
Change Password

User menu

Edit menu - User Account Administration

2.8.2 User menu

The **User** menu is only displayed in the User Account Administration dialog. It is used to add users to or delete users from the system. It contains the following entries:



- **Add**

  Click on **Add** in the **User** menu to open the Add New User dialog. You can also use the Context Menu or the icons in the Toolbar to execute this command.
- **Delete**

  Click on **Delete** in the **User** menu to open the Delete User Accounts dialog. You can also use the Context Menu or the icons in the Toolbar to execute this command.

Related Topics

Toolbar

Menu Bar

Context Menu

Add New User

Delete User Accounts

Edit menu - User Account Administration

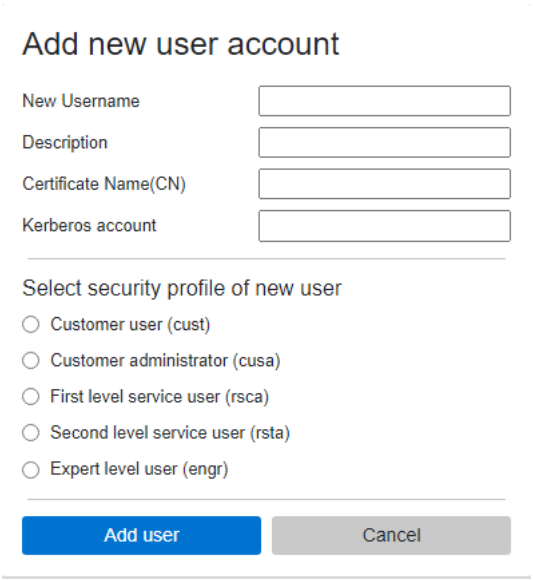
Group menu - Access Right Group Configuration

Help menu - User Account Administration

Export User Reports

2.8.3 Add New User

The **Add new user account** dialog is displayed when you click on **Add** in the User menu or in the Context Menu, or by choosing the corresponding icon in the Toolbar.



To add a new user, you have to

- enter the name of the new user in the New username field,

  NOTICE: IMPORTANT for V8R0: The name of an account must have at least three characters, must not exceed 32 characters, must start with a lowercase letter ('a'..'z'), and must consist of 'a'..'z', '0'..'9', '-', and '_' only.

- enter a description for the new user (account) name into the Description field,
- assign certificate (Common Name property) to this user in the **Certificate Name (CN)** field; this field can be empty when PKI authentication is not used on system.

- select one of the radio buttons for the **Security profile** of the new user:
  - Customer user (cust),
  - Customer administrator (cusa),
  - First level service user (rsca),
  - Second level service user (rsta), or
  - Expert user (engr).

  Access rights of the new account will be inherited from security profile and will provide same functionality as predefined accounts have. For details about user accounts please refer to Security Levels and Predefined User Accounts on page 9.
- Confirm the new account by clicking on the **OK** button, or
- cancel the entries you made by clicking on **Cancel.**

Alternative Ways to Execute the Command(s)

Using the User menu

or

Using the Context Menu

or

Using the Toolbar

Related Topics

Toolbar

Menu Bar

Context Menu

User menu

Delete User Accounts

Group menu - Access Right Group Configuration

Edit menu - User Account Administration

Help menu - User Account Administration

Export User Reports

See also

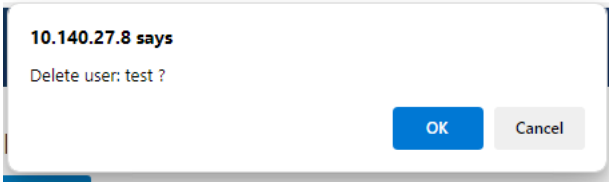
Toolbar Icons - User Account Administration dialog

User Account Administration and System Account Administration - Field Descriptions

Add new user - Field Descriptions.

2.8.4 Delete User Accounts

Clicking on **Delete** in the **User** menu or on the corresponding **toolbar button** opens the **Delete User Accounts**confirmation dialog.



- Click on **OK** to confirm and execute the deletion of the selected user or users.
- Click on **Cancel** to abort the deletion.

Alternative Ways to Execute the Command(s)

Using the User menu

or

Using the Context Menu

or

Using the Toolbar

See also

Toolbar Icons - User Account Administration dialog

User Account Administration and System Account Administration - Field Descriptions

Related Topics

Toolbar

Menu Bar

Context Menu

User menu

Add New User

Group menu - Access Right Group Configuration

Edit menu - User Account Administration

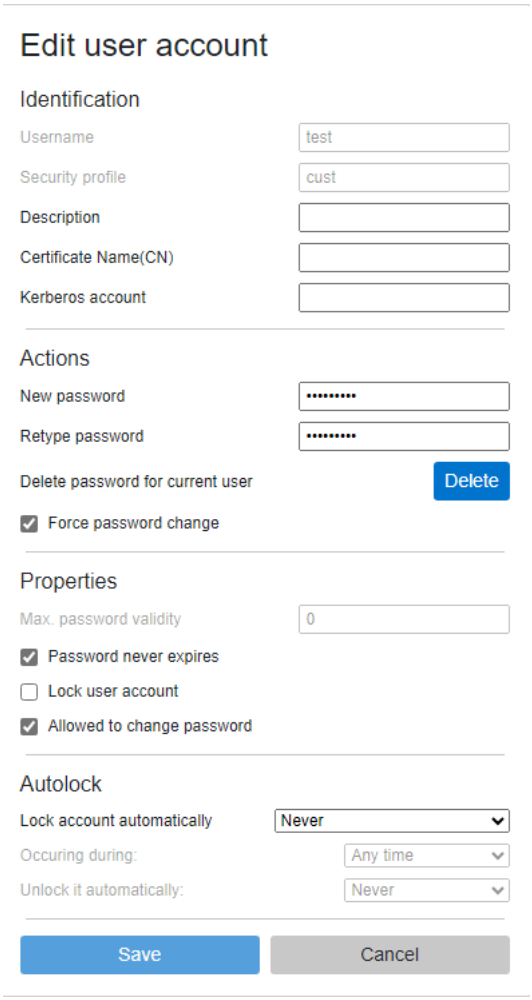
Help menu - User Account Administration

Export User Reports

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.8.5 Edit menu - User Account Administration

The **Edit** menu is displayed in all dialogs of the **Account Management** component. It contains the following entries:



Menu Options

Apply	Clicking on **Apply** in the **Edit** menu applies the selected properties to the selected user(s). This command has the same function as the **Apply** button in the lower right part of the screen and the **Apply modifications** icon in the toolbar. You can also use the Context Menu or the Toolbar to execute this command.
Discard	Clicking on **Discard** in the **Edit** menu discards the applied changes made to the selected user(s). This command has the same function as the **Discard** button in the lower right part of the screen and the **Discard modifications** icon in the toolbar. You can also use the Context Menu or the Toolbar to execute this command.
Reload	Clicking on **Reload** in the **Edit** menu updates the contents of the **User Account Administration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. This command has the same function as the **Reload data from server** icon in the Toolbar.

Alternative Ways to Execute the Command(s)

Using the Edit menu - User Account Administration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

Before executing commands you need to select the required items or users, respectively.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Toolbar

Menu Bar

Context Menu

User menu

Group menu - Access Right Group Configuration

View menu, User Account Administration

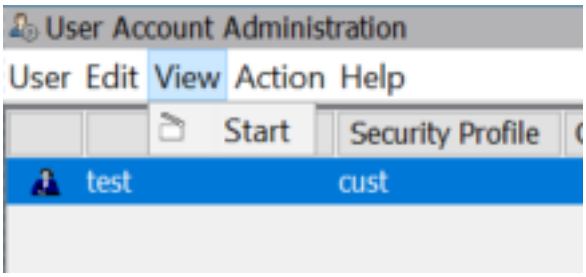
Action menu, User Account Administration

Help menu - User Account Administration

Export User Reports

2.8.6 View menu, User Account Administration

The options displayed in the **View** menu may vary, depending on the software component selected. In the User Account Administration and System Account Administration components, the **View** menu contains the **Start** option.



The **Start** option in the **View** menu has the same function as the **View Start Page** icon in the toolbar in the upper right corner of the screen.

When you click the **Start** menu option or the icon in the toolbar, a new browser window opens, displaying the OpenScape 4000 Assistant/Manager **Start Page**. The OpenScape 4000 Assistant/Manager **Start Page** displays the list of all applications which the currently logged-on user is allowed to access and to use.

See also Toolbar Icons - User Account Administration dialog.

Related Topics

Toolbar

Menu Bar

User menu

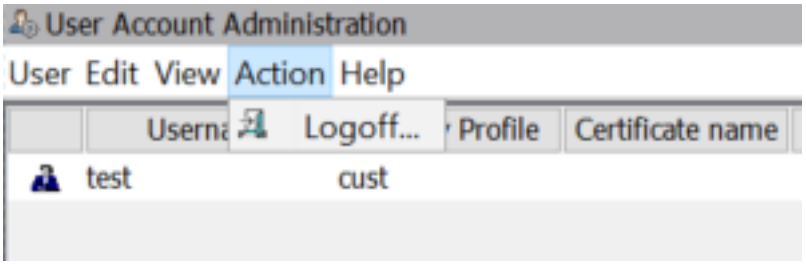
Edit menu - User Account Administration

Action menu, User Account Administration

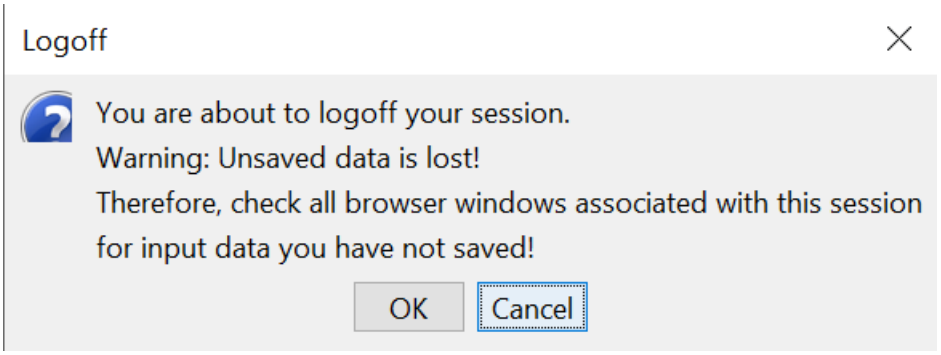
Help menu - User Account Administration

2.8.7 Action menu, User Account Administration

The **Action** menu contains the **Logoff** menu option, which has the same function as the **Logoff** icon in the toolbar in the upper right corner of the screen. See also Toolbar Icons - User Account Administration dialog.



When you click the **Logoff** menu option or the icon in the toolbar, an error message dialog is displayed, warning you that all unsaved data will be lost, and prompting you to save all your data, close all browser windows belonging to the current session, and confirm that you want to log off.



Related Topics

Toolbar

Menu Bar

User menu

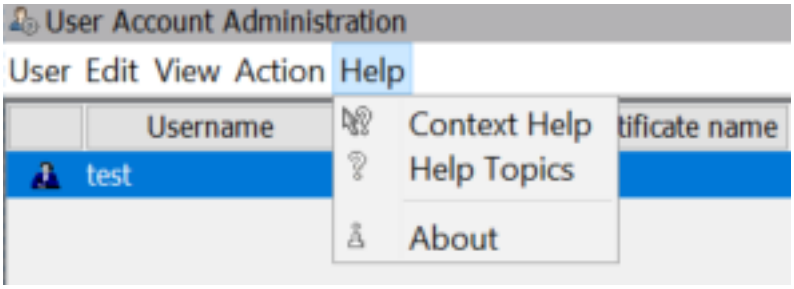
Edit menu - User Account Administration

View menu, User Account Administration

Help menu - User Account Administration

2.8.8 Help menu - User Account Administration

The **Help** menu is displayed with all components of the **Account Management** area, except for **Export User Reports**. The **Help** menu options are the same with all components, as follows:



Context Help	Clicking on **Context Help** opens the context-sensitive Online Help related to a specific item that you select with the mouse. The Context Help can alternatively be started by selecting a specific item in the UI with the mouse and then pressing **CTRL+F1**.
Help Topics	Clicking on the **Help Topics** opens the Online Help Topics. The Online Help can also be started by pressing the **F1** key.
About	The **About** dialog contains the information about the software version of the program, the release date, and the copyright provisions.

Related Topics

Toolbar

Menu Bar

User menu

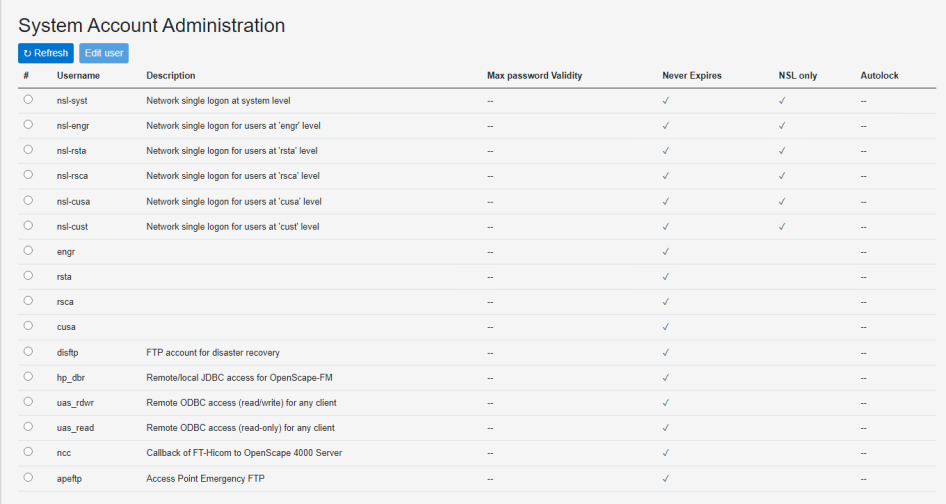
Edit menu - User Account Administration

View menu, User Account Administration

Action menu, User Account Administration

2.9 System Account Administration

The **System Account Administration** dialog is used to administer a specific user group (NSL and system accounts), i.e. by adding, changing or deleting system accounts or by changing the password properties of a specific account or group of accounts. Modifications of access rights for specific user accounts or groups of accounts should be performed using the **Access Right Configuration** feature.



Left Hand Side Area

The columns on the **left hand side** of the dialog show the list of accounts the current user is allowed to manage. This dialog offers the possibility to select multiple accounts and to set or change properties to the same value for multiple users with a single click. The user interface is similar to the **User Account Administration** dialog.

When you click on **Apply** a dialog prompt will notify you that the password properties of multiple user accounts are being changed.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Right Hand Side Area

The **right hand side** of the **System Account Administration** dialog contains the following areas:

- Identification area,
- Actions area,
- Properties area,
- Autolock area.

These areas are used to define or edit the properties of existing and new system accounts. For a description of these areas, please refer to Areas in the System Account Administration dialog on page 263, and Controls and Buttons in the System Account Administration dialog on page 264.

The list of displayed accounts is determined by the accounts that have been created on the server, and by the current user's access rights, i.e.: which user is the "caretaker" or owner of which accounts.

There are three different types of accounts, indicated by different icons:

- **System accounts**: Linux accounts created for different purposes to assure proper operation of OpenScape 4000 features and communication to their partner systems. These accounts are not used for interactive logon.
- **Predefined administrator accounts**: Accounts created for logon of other ("lower-leveled") administrators.

- **Network Single Logon (NSL) accounts** Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from. Note that all NSL accounts are open by default! This means that full access to the server via Network Single Logon is allowed without any password protection, as long as passwords are not set in the **System Account Administration** dialog!

For a detailed list of all account categories and accounts, please refer to Access Management Security Levels and User Accounts.

UI components

The **System Account Administration** dialog contains the following UI components:

- System Accounts List, System Account Administration dialog
- Toolbar
- The **Toolbar Icons** have the same functionality as the entries in the main menus. For a detailed description of the icons in the toolbar, please refer to Toolbar Icons - System Account Administration dialog.
- Menu Bar
- Context Menu
- Edit menu - System Account Administration
- View menu, System Account Administration
- Action menu, System Account Administration
- Help menu - System Account Administration
- System Account Administration dialog - User Interface Description
- Columns in the System Account Administration dialog
- Areas in the System Account Administration dialog
  - Identification area
  - Actions area
  - Properties area
  - Autolock area
- Controls and Buttons in the System Account Administration dialog
- Access Management Security Levels and User Accounts

Field Descriptions

User Name

Description

New Password

Retype Password

Delete Password

Force password change

Max. password validity

Password never expires

Lock user account

Lock account automatically

occurring during

Unlock it automatically

Apply (Button)

Discard (Button)

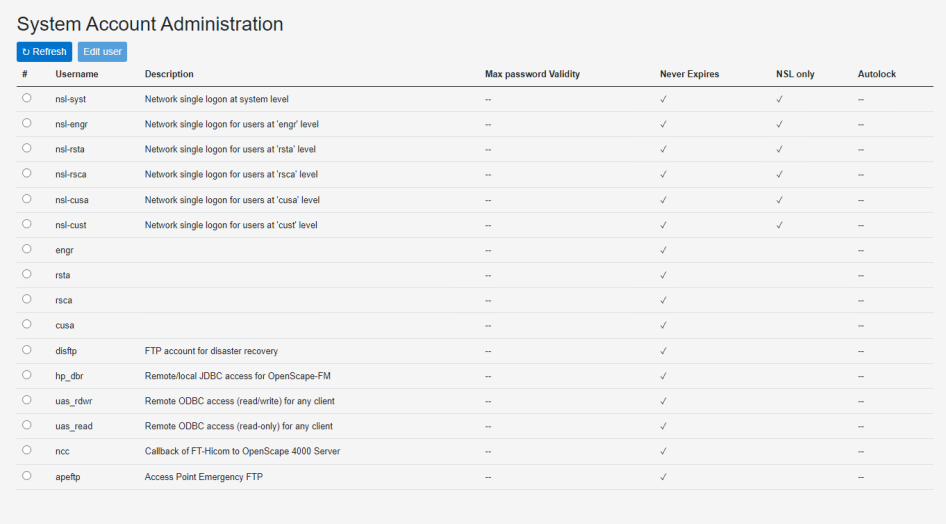
Reload

Related Topics

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.9.1 System Accounts List, System Account Administration dialog



Left Hand Side Area

The columns in the **left hand** pane of the dialog show the list of all system accounts the current user is allowed to manage. This dialog offers the possibility to select multiple system accounts and to set or change properties to the same value for multiple users with a single click. The user interface is similar to the **User Account Administration** dialog.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non consecutive** items or to deselect individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Right Hand Side Area

The **right hand side** of the **System Account Administration** dialog contains the following areas:

- Identification area
- Actions area
- Properties area
- Autolock area

These areas are used to define or edit the properties of existing and new system accounts. For a detailed description of this area, please refer to Areas in the System Account Administration dialog on page 263, and Controls and Buttons in the System Account Administration dialog on page 264.

The list of displayed accounts is determined by the accounts that have been created on the server, and by the current user's access rights, i.e.: which user is the "caretaker" or owner of which accounts.

There are three different types of accounts, indicated by different icons:

- **System accounts**: Linux accounts created for different purposes to assure proper operation of OpenScape 4000 features and communication to their partner systems. These accounts are not used for interactive logon.
- **Predefined administrator accounts**: Accounts created for logon of other ("lower-leveled") administrators.
- **Network Single Logon (NSL) accounts** Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from. Note that all NSL accounts are open by default! This means that full access to the server via Network Single Logon is allowed without any password protection, as long as passwords are not set in the **System Account Administration** dialog!

For a detailed list of all account categories and accounts, please refer to Access Management Security Levels and User Accounts.

Related Topics

User Account Administration

Edit menu - System Account Administration

View menu, System Account Administration

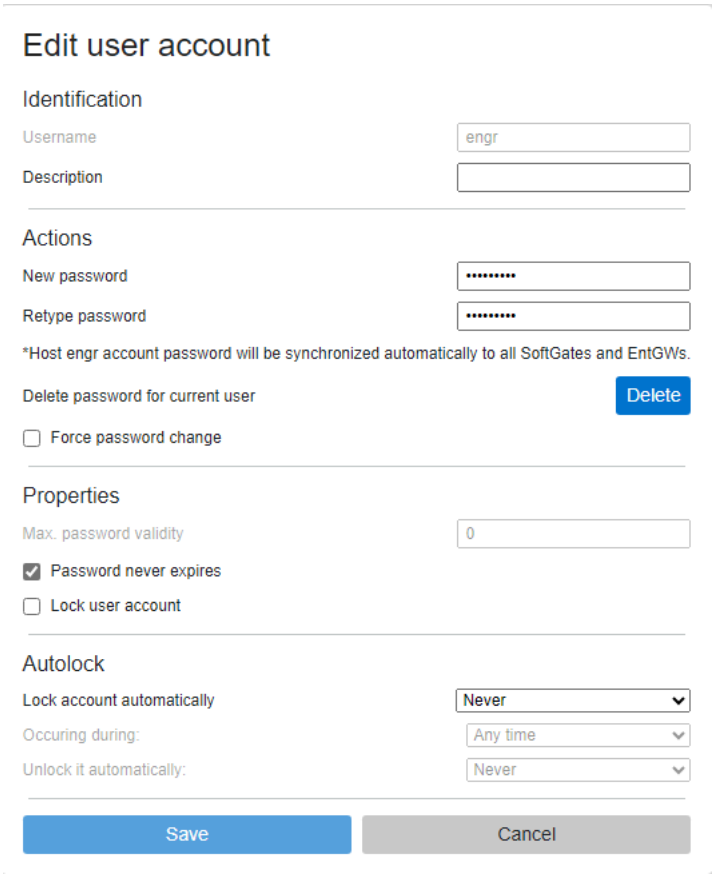
Toolbar

Context Menu

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.9.2 Edit menu - System Account Administration

The **Edit** menu is displayed in all dialogs of the **Account Management** component. In the **System Account Configuration** dialog it contains the following entries:



Menu Options

Apply	Clicking on **Apply** in the **Edit** menu applies the selected properties to the selected user(s). This command has the same function as the **Apply** button in the lower right part of the screen and the **Apply modifications** icon in the toolbar. You can also use the Context Menu or the Toolbar to execute this command.
Discard	Clicking on **Discard** in the **Edit** menu discards the applied changes made to the selected user(s). This command has the same function as the **Discard** button in the lower right part of the screen and the **Discard modifications** icon in the toolbar. You can also use the Context Menu or the Toolbar to execute this command.
Reload	Clicking on **Reload** in the **Edit** menu updates the contents of the **System Account Administration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. This command has the same function as the **Reload items from Server** icon in the Toolbar.

Alternative Ways to Execute the Command(s)

Using the Edit menu - System Account Administration or Using the Context Menu or Using the Toolbar

Selecting items

Before executing commands you need to select the required items or users, respectively.

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Toolbar

Menu Bar

Context Menu

View menu, System Account Administration

Action menu, System Account Administration

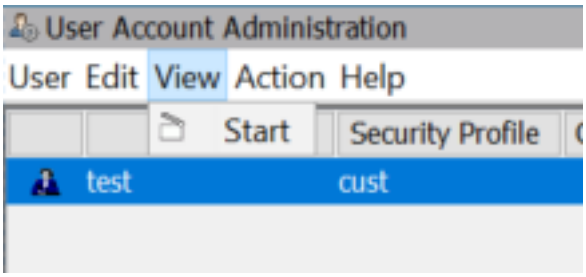
Help menu - System Account Administration

System Account Administration dialog - User Interface Description

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.9.3 View menu, System Account Administration

The options displayed in the **View** menu may vary, depending on the software component selected. In the User Account Administration and System Account Administration components, the **View** menu contains the **Start** option.



The **Start** option in the **View** menu has the same function as the **View Start Page** icon in the tool bar in the upper right corner of the screen.

Whe you click the **Start** menu option or the icon in the toolbar, a new browser window opens, displaying the OpenScape 4000 Assistant/Manager **Start Page**. The OpenScape 4000 Assistant/Manager **Start Page** displays the list of all applications which the currently logged-on user is allowed to access and to use.

See also Toolbar Icons - System Account Administration dialog.

Related Topics

Toolbar

Menu Bar

Edit menu - System Account Administration

Action menu, System Account Administration

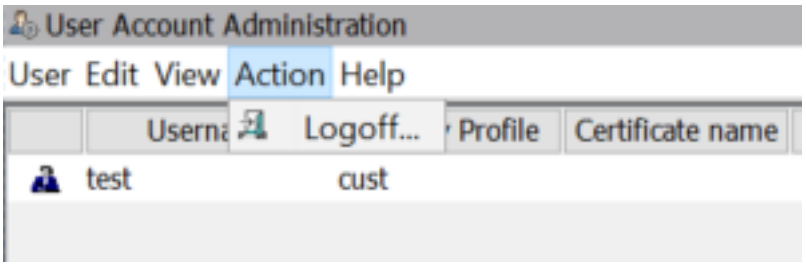
Help menu - System Account Administration

System Account Administration dialog - User Interface Description

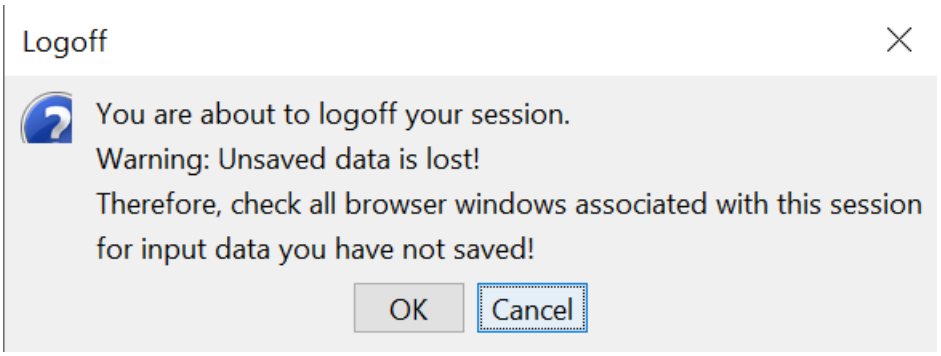
Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.9.4 Action menu, System Account Administration

The **Action** menu contains the **Logoff** menu option, which has the same function as the **Logoff** icon in the toolbar in the upper right corner of the screen. See also Toolbar Icons - System Account Administration dialog.



When you click the **Logoff** menu option or the icon in the toolbar, an error message dialog is displayed, warning you that all unsaved data will be lost, and prompting you to save all your data, close all browser windows belonging to the current session, and confirm that you want to log off.



Related Topics

Toolbar

Menu Bar

Edit menu - System Account Administration

View menu, System Account Administration

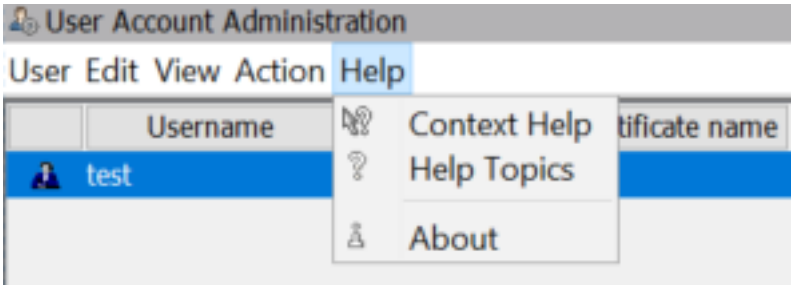
Help menu - System Account Administration

System Account Administration dialog - User Interface Description

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.9.5 Help menu - System Account Administration

The **Help** menu is displayed with all components of the **Account Management** component, except for **Export User Reports**. The **Help** menu options are the same with all components, as follows:



Context Help	Clicking on **Context Help** opens the context-sensitive Online Help related to a specific item that you select with the mouse. The Context Help can alternatively be started by selecting a specific item in the UI with the mouse and then pressing **CTRL+F1**.
Help Topics	Clicking on the **Help Topics** opens the Online Help Topics. The Online Help can also be started by pressing the **F1** key.
About	The **About** dialog contains the information about the software version of the program, the release date, and the copyright provisions.

Related Topics

Toolbar

Menu Bar

Edit menu - System Account Administration

View menu, System Account Administration

Action menu, System Account Administration

System Account Administration dialog - User Interface Description

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.10 Access Right Configuration

The **Access Right Configuration** dialog is used to assign available access right groups (for execution of applications) to users.

The process of assigning only some out of a large amount of access rights is simplified by assigning "access right groups".

A set of predefined access right groups is available after installation. It may be expanded by new access right groups in the **Access Right Group Configuration** dialog. Changes in one of these access right groups will affect all users with that group assigned.

The **Access Right Configuration** dialog is vertically divided into two panes, or areas:

Users (Left Hand Side Area)

The left hand side area, labeled **Users**, displays a two-level tree containing all available users (top level) and their assigned access right groups (lower level).

Access Right Groups (Right Hand Side Area)

The right hand side area, labeled **Access Right Groups**, contains all assignable access right groups.

Preview Panes

Each window area has a **Preview Pane** (at the bottom of the window) that can be turned on and off. The Preview Panes - Access Right Configuration show the properties of the selected user or access right group. The height of the preview panes can be changed.

Both the user tree and the group list have extended selection style, and menu functions are enabled depending on the selections made in these lists, both in the standard menus and in the Context menu.

Selecting items

To select multiple consecutive items (user accounts or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

UI components in the Access Right Configuration dialog

The **Access Right Configuration** dialog contains the following UI components:

- Access Right Configuration dialog - User Interface Description

  The **Toolbar Icons** have the same functionality as the entries in the main menus. For a detailed description of the icons in the toolbar, see Toolbar Icons - Access Right Configuration dialog.
- Menu Bar
- Toolbar

  For a detailed description of the icons in the toolbar, see Toolbar Icons - Access Right Configuration dialog.
- Context Menu
- Edit menu - Access Right Configuration
- View Menu - Access Right Configuration

  The **Show Preview Panes and Windows** menu option in the **View** menu is used to show/hide the **Preview Panes**.

  For more information about the Preview Panes please refer to Preview Panes - Access Right Configuration.
- Action menu, Access Right Configuration
- Help menu - Access Right Configuration
- Areas in the Access Right Configuration dialog
- Preview Panes - Access Right Configuration

Related Topics

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

User Account Administration dialog - User Interface Description

Access Right Configuration dialog - User Interface Description

Access Right Group Configuration dialog - User Interface Description

Areas in the Access Right Configuration dialog

2.10.1 Areas in the Access Right Configuration dialog

The **Access Right Configuration** dialog is vertically divided into two panes, or areas:

- Users (Left Hand Side Area), Access Right Configuration dialog

  The left hand side area, labeled **Users**, displays a two-level tree containing all available users (first level) and their assigned access right groups (second level).
- Access Right Groups (Right Hand Side Area), Access Right Configuration dialog

  The right hand side area, labeled **Access Right Groups**, contains all assignable access right groups.

Selecting items

To select multiple consecutive items (user accounts or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

- Preview Panes - Access Right Configuration

  Each window area has a **Preview Pane** (at the bottom of the window) that can be turned on and off. The Preview Pane shows the properties of the selected user or access right group, respectively. The height of the preview panes can be changed.

  Both the user tree and the group list have extended selection style, and menu functions are enabled depending on the selections made in these lists.
- Toolbar

  The **Toolbar Icons** have the same functionality as the entries in the main menus. For a description of the icons in the toolbar, please refer to Toolbar Icons - Access Right Configuration dialog.
- Menu Bar

For more details about each of the areas, please refer to:

Users (Left Hand Side Area), Access Right Configuration dialog

Access Right Groups (Right Hand Side Area), Access Right Configuration dialog

Assigning/Withdrawing Access Right Groups To/From Users

Edit menu - Access Right Configuration

Preview Panes - Access Right Configuration

Preview Pane, Left Hand Side Area, Access Right Configuration dialog

Preview Pane, Right Hand Side Area, Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Related Topics

Context Menu

Show/Hide Preview Panes

Displaying Multiple Preview Panes Simultaneously

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

2.10.1.1 Users (Left Hand Side Area), Access Right Configuration dialog

Displays a two-level tree structure containing all avaliable **users** (top level) and their assigned **access right groups** (secondary level). Each user is represented by a folder in the tree structure. Each folder contains the access right groups assigned to this user. You can open each folder to display and view the access right groups assigned to a specific user.

Selecting items

To select multiple consecutive items (user accounts or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

For more information about assigning and withdrawing access right groups for specific users, please refer to the Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog section.

See also Access Right Configuration, Areas in the Access Right Configuration dialog, and Preview Panes - Access Right Configuration.

Related Topics

Context Menu

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Assigning/Withdrawing Access Right Groups To/From Users

Edit menu - Access Right Configuration

Preview Panes - Access Right Configuration

Access Management tab sheet in System Management, User Interface

2.10.1.2 Access Right Groups (Right Hand Side Area), Access Right Configuration dialog

Displays all access right groups that can be assigned to users.

For more information about assigning and withdrawing access right groups for specific users, please refer to the Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog section.

Selecting items

To select multiple consecutive items (user accounts or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

See also Access Right Configuration, Areas in the Access Right Configuration dialog, and Preview Panes - Access Right Configuration.

Related Topics

Context Menu

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Assigning/Withdrawing Access Right Groups To/From Users

Edit menu - Access Right Configuration

Preview Panes - Access Right Configuration

Access Management tab sheet in System Management, User Interface

2.10.2 Assigning/Withdrawing Access Right Groups To/From Users

Assigning Access Right Groups To Users

There will be different ways to assign access right groups to users:

- Select one or more groups in the right hand side window. Drag the selected group(s) with the mouse over that user or users on the left hand side to whom those groups should be assigned.

  or

- Select one or more groups in the right hand side window. In the left hand side window, select the user(s) which should get these groups. Be sure to select only users from this list. Choose **Edit** - **Assign** from the menu bar or press the appropriate button in the Toolbar or in the Context Menu. With that function, groups can be assigned to more than one user in one step.

Withdrawing Access Right Groups From Users

To withdraw assigned groups you have to:

- Select the groups to withdraw from a user in the left hand side window. Be sure to select only groups from this list. Choose **Edit** - **Withdraw** from the menu bar or press the appropriate button in the Toolbar or in the Context Menu.

  or

- In the left hand side area, select one or more users from whom you want to withdraw access right groups. The right hand side area displays the access right groups that can be withdrawn from the selected users. In the right hand side area, select the access right groups you want to withdraw. Choose **Edit** - **Withdraw** from the menu bar or press the appropriate button in the Toolbar or in the Context Menu. A security prompt is then displayed and

the selected access rights are being withdrawn, provided that you have previously marked one or more user accounts in the left hand side area.

All changes are sent immediately to the server and therefore apply to all new logons of affected users. The changes may also affect already running sessions, since Access Management notifies other applications in regular time intervals about those changes.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

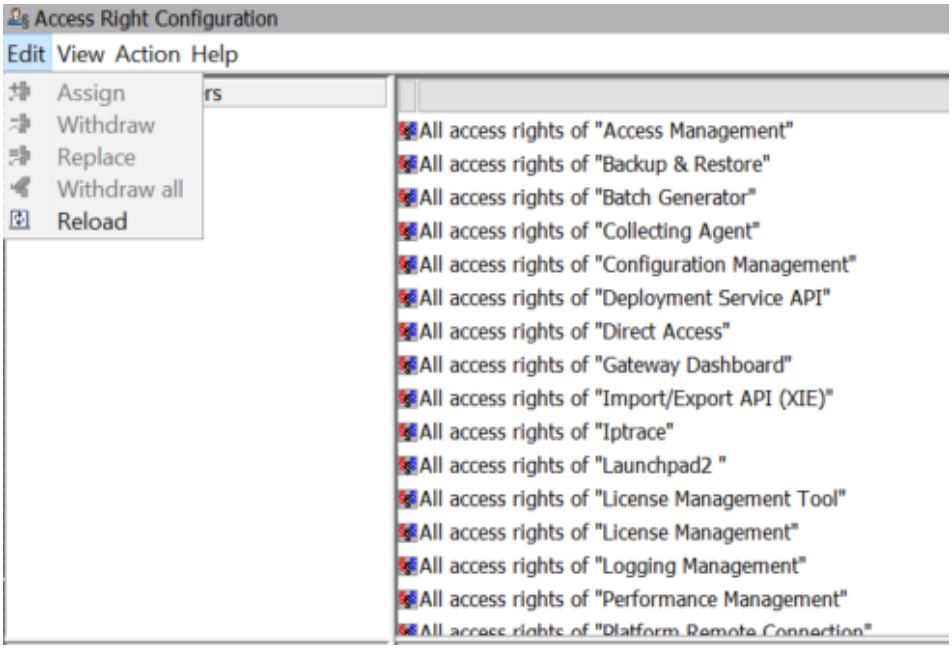
Areas in the Access Right Configuration dialog

Edit menu - Access Right Configuration

Toolbar Icons - Access Right Configuration dialog

2.10.3 Edit menu - Access Right Configuration

The **Edit** menu is displayed in all dialogs of the **Account Management** component. In the **Access Right Configuration** dialog it contains the following entries:



Menu Options

Assign	Clicking on **Assign** in the **Edit** menu assigns the access right group(s) selected in the right area to the user(s) selected in the left area. You can also use the Context Menu or the Toolbar to execute this command.
Withdraw	Clicking on **Withdraw** in the **Edit** menu removes access right group(s) selected in the left area from the associated user(s). You can also use the Context Menu or the Toolbar to execute this command. **Note:** The **Withdraw** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.
Replace	Select the required user(s) in the left hand side area, and the access right groups that should replace the existing access right groups in the right hand side area. Click on **Replace** in the **Edit** menu to replace the previously assigned access right groups with the currently selected access right groups. The previously assigned access right groups will be overwritten during this process. Difference to **Assign**: In the case of **Assign** the newly selected access right groups are appended (added) to the already existing assigned access right groups, which are not overwritten. Alternative ways to execute this command: Via the Context Menu or via the Toolbar. **Note:** The **Replace** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.
Withdraw All	In the left hand side area, select the user(s) to which you want to apply this command. Click on **Withdraw All** in the **Edit** menu to withdraw all assigned access rights from the selected user(s). Alternative ways to execute this command: Via the Context Menu or via the Toolbar. **Note:** The **Withdraw All** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Reload	Clicking on **Reload** in the **Edit** menu updates the contents of the **Access Right Configuration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. This command has the same function as the **Reload items from Server** icon in the Toolbar.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items or users, press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

Assigning/Withdrawing Access Right Groups To/From Users

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Preview Panes - Access Right Configuration

Access Management tab sheet in System Management, User Interface

2.10.4 View Menu - Access Right Configuration

The **View** menu in the **Access Right Configuration** dialog contains the following options:

- **Show Preview Panes and Windows**

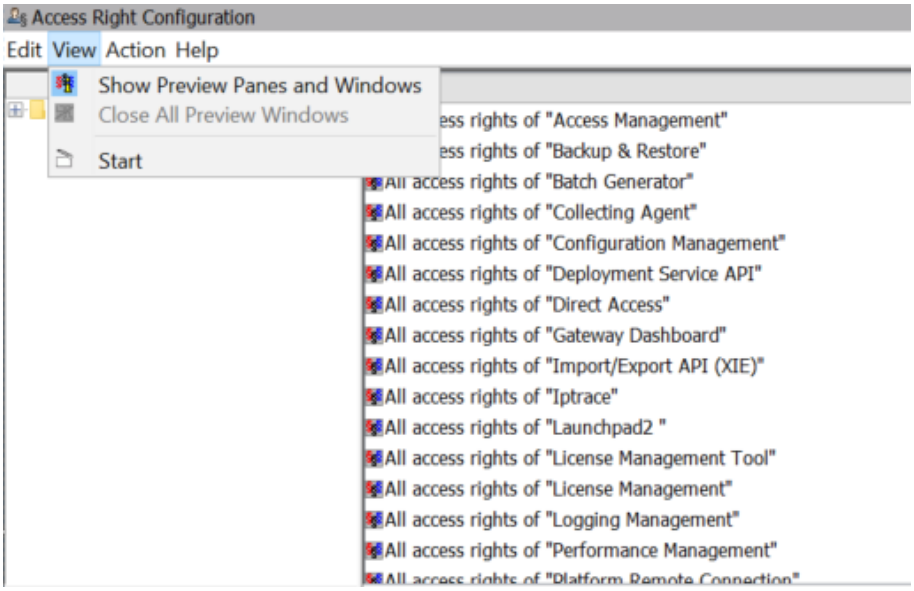
  The **Show Preview Panes and Windows** menu option in the **View** menu of the **Access Right Configuration** dialog is used to show/hide the **Preview Panes** at the bottom of the **Access Right Configuration** dialog. The Preview Panes display short descriptions of the selected access right(s).

  For more information please refer to Preview Panes - Access Right Configuration.
- **Close All Preview Windows**

  This option closes all open text dialogs containing preview text. To open/display the closed preview windows again, use the **Show Preview Panes and Windows** option in the **View** menu.

- **Start**

  Clicking the **Start** option in the **View** menu (or the **View Start Page** icon in the toolbar) opens a new browser window and displays the **OpenScape 4000 Assistant/Manager Start Page**.



Related Topics

Context Menu

Preview Panes - Access Right Configuration

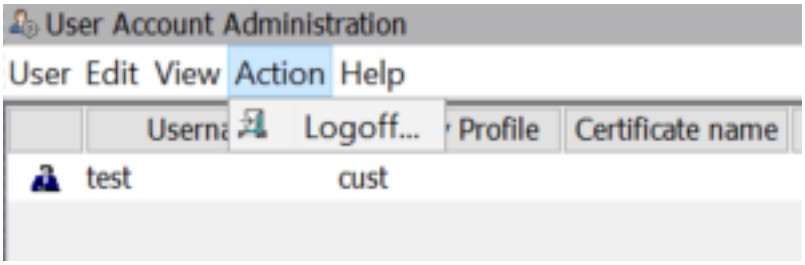
Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

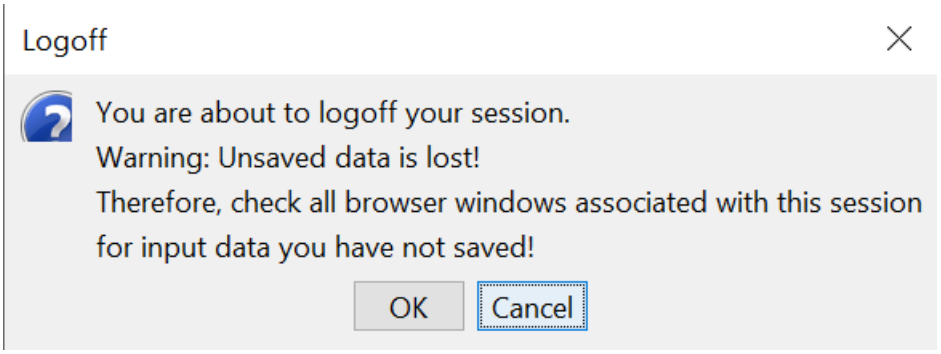
Assigning/Withdrawing Access Right Groups To/From Users

2.10.5 Action menu, Access Right Configuration

The **Action** menu contains the **Logoff** menu option, which has the same function as the **Logoff** icon in the toolbar in the upper right corner of the screen. See also Toolbar Icons - Access Right Configuration dialog.



When you click the **Logoff** menu option or the icon in the toolbar, an error message dialog is displayed, warning you that all unsaved data will be lost, and prompting you to save all your data, close all browser windows belonging to the current session, and confirm that you want to log off.



Related Topics

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Assigning/Withdrawing Access Right Groups To/From Users

2.10.6 Preview Panes - Access Right Configuration

The **Show Preview Panes and Windows** menu option in the **View** menu and in the **Context** menu of the **Access Right Configuration** dialog is used to show/hide the **Preview Panes** at the bottom of the **Access Right Configuration** dialog. The Preview Panes display short descriptions of the selected access right(s) or of all access rights assigned to the selected user, respectively. The height of the preview panes can be changed.

Topics Covered

Show/Hide Preview Panes,

Displaying Multiple Preview Panes Simultaneously,

Preview Pane, Left Hand Side Area, Access Right Configuration dialog,

Preview Pane, Right Hand Side Area, Access Right Configuration dialog,

Context Menu

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

Assigning/Withdrawing Access Right Groups To/From Users

2.10.6.1 Show/Hide Preview Panes

The **Preview Panes** at the bottom of the two areas of the **Access Right Configuration** dialog can be shown or hidden by activating/deactivating the **Show Preview Panes and Windows** option in the View Menu - Access Right Configuration or in the Context Menu. The height of the preview panes can be changed.

The preview panes list all access rights that are currently part of the selected access right group. If - in the left hand side area - you selected a user instead of an access right group, the preview pane on the left hand side displays a list of

all access rights currently assigned to this user, and the title of the preview pane changes to **Access Rights of the Selected User**.

If, on the other hand, you selected a specific access right in the left hand side area, the title of the preview pane will change to **Access Rights of the Selected Access Right Group**.

Related Topics

Context Menu

Displaying Multiple Preview Panes Simultaneously,

Preview Pane, Left Hand Side Area, Access Right Configuration dialog,

Preview Pane, Right Hand Side Area, Access Right Configuration dialog,

Areas in the Access Right Configuration dialog

2.10.6.2 Displaying Multiple Preview Panes Simultaneously

The icon in the preview pane title bar changes to a magnifying glass when you move the mouse pointer over it. The height of the preview panes can be changed.

How to open an additional Preview Pane text dialog

- Move the mouse over the icon displayed in the header of a preview pane. The icon changes to a magnifying glass.
- Click on the magnifying glass. An additional preview text dialog is opened. It contains the same text that is displayed in the corresponding original preview pane, i.e. a short description of the selected access right or of all access rights of the selected user (left hand side window) or of the selected access right group (right hand side window), respectively.
- Alternative method: You can also open the text dialog by double-clicking the selected object (user account, access right or access right group).
- You can open several preview text dialogs successively and leave them open on the screen.
- To close one or more text dialogs you can either click the **Close** button in each of the text dialogs, or select **Close All Preview Windows** in the **View** menu or in the **Context** menu to close all preview windows at once.

It is possible to display several text windows simultaneously.

Use the View Menu - Access Right Configuration to

- show/hide the preview panes,
- close all additional preview windows containing preview text,
- return to the **OpenScape 4000 Assistant/Manager Start Page**.

For additional details please refer to Areas and Preview Panes in the Access Right Configuration dialog.

Related Topics

Context Menu

Show/Hide Preview Panes

Preview Pane, Left Hand Side Area, Access Right Configuration dialog,

Preview Pane, Right Hand Side Area, Access Right Configuration dialog,

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

2.10.6.3 Preview Pane, Left Hand Side Area, Access Right Configuration dialog

The Preview Pane at the bottom of the left hand side area of the **Access Right Configuration** dialog may display two different titles, as follows:

Access Rights of the Selected User

This title is displayed in the left hand side preview pane if you selected a **user** in the left hand side area.

Access Rights of the Selected Access Right Group

This title is displayed in the left hand side preview pane if you selected an **access right group** in the left hand side area.

Show/Hide Preview Panes

You can show or hide the **Preview Panes** as required. The height of the preview panes can be changed.

For more information, please refer to Show/Hide Preview Panes.

Displaying Several Preview Panes Simultaneously

You can open several preview text dialogs and have them all displayed on the screen simultaneously.

For more information, please refer to Displaying Multiple Preview Panes Simultaneously.

Related Topics

Context Menu

Show/Hide Preview Panes

Preview Pane, Right Hand Side Area, Access Right Configuration dialog,

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

2.10.6.4 Preview Pane, Right Hand Side Area, Access Right Configuration dialog

The preview pane labeled **Access Rights of the Selected Access Right Group** at the bottom of the right hand side area of the **Access Right Configuration** dialog displays the list of all access rights belonging to an access right group.

Show/Hide Preview Panes

You can show or hide the **Preview Panes** as required, as described in the Show/Hide Preview Panes section. The height of the preview panes can be changed.

Displaying Several Preview Panes Simultaneously

You can open several preview text dialogs and have them all displayed on the screen simultaneously.

For more information, please refer to Displaying Multiple Preview Panes Simultaneously.

Related Topics

Context Menu

Show/Hide Preview Panes

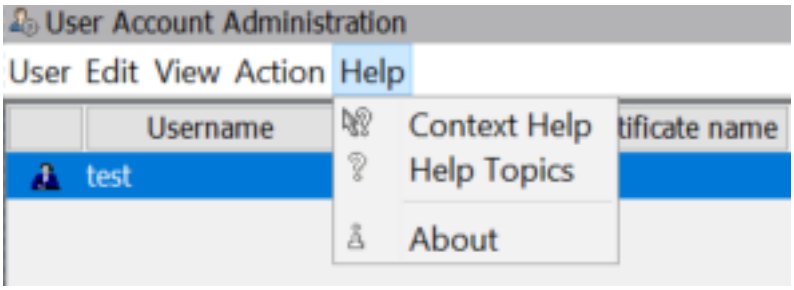
Preview Pane, Left Hand Side Area, Access Right Configuration dialog,

Areas in the Access Right Configuration dialog

Toolbar Icons - Access Right Configuration dialog

2.10.7 Help menu - Access Right Configuration

The **Help** menu is displayed with all components of the **Account Management** component, except for **Export User Reports**. The **Help** menu options are the same with all components, as follows:



Context Help	Clicking on **Context Help** opens the context-sensitive Online Help related to a specific item that you select with the mouse. The Context Help can alternatively be started by selecting a specific item in the UI with the mouse and then pressing **CTRL+F1**.
Help Topics	Clicking on the **Help Topics** opens the Online Help Topics. The Online Help can also be started by pressing the **F1** key.
About	The **About** dialog contains the information about the software version of the program, the release date, and the copyright provisions.

Related Topics

Menu Bar

Toolbar

Access Management User Interface

2.11 Access Right Group Configuration

The **Access Right Group Configuration** dialog is used to create and modify access right groups.

Access right groups are used to administer the rights of users to execute and use applications.

The process of assigning only some out of a large amount of access rights is simplified by assigning pre-defined "access right groups", as described in Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.

A set of predefined access right groups is available after installation. Additional access right groups can be created and modified in the **Access Right Group Configuration** dialog. Changes in one of these access right groups will affect all users with that group assigned.

Use the Access Right Configuration dialog to assign access right groups to specific users.

User Interface Components

The **Access Right Group Configuration** dialog consists of a vertically divided window with two panes, each displaying access rights and access right groups in a multi-level tree structure. The user interface is made up of the following components:

- Areas in the Access Right Group Configuration dialog
  - Access Right Groups (Left Hand Side Pane), Access Right Group Configuration dialog

    Three types of access right groups can be displayed: **Predefined ARGs**, **Manually created ARGs**, and **ARGs for Dynamic Applications**. You can use the View menu - Access Right Group Configuration or the Context Menu to show or hide each of these groups, as required.
  - Access Rights - Component/Application Tree (Right Hand Side Pane), Access Right Group Configuration dialog
- Preview Panes, Access Right Group Configuration dialog

  The Preview Panes, Access Right Group Configuration dialog at the bottom of the two dialog areas show short descriptions of the currently selected access rights. The **Preview Panes** can be displayed and hidden, respectively, using the **Display Info on Access Right** option in the View menu - Access Right Group Configuration or in the Context Menu. The height of the preview panes can be changed.
- Toolbar

  The **Toolbar Icons** have the same functionality as the entries in the main menus. For a description of the icons in the toolbar, please refer to Toolbar Icons - Access Right Group Configuration dialog.
- Menu Bar
- Context Menu
- Group menu - Access Right Group Configuration
- Edit menu - Access Right Group Configuration
- View menu - Access Right Group Configuration
- Action menu, Access Right Group Configuration
- Help menu - Access Right Group Configuration

Related Topics

Access Right Configuration dialog - User Interface Description

System Account Administration dialog - User Interface Description

User Account Administration dialog - User Interface Description

Areas and Preview Panes in the Access Right Group Configuration dialog

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

2.11.1 Areas in the Access Right Group Configuration dialog

The **Access Right Group Configuration** dialog consists of a vertically divided window with two panes, structured as follows:

- Access Right Groups (Left Hand Side Pane), Access Right Group Configuration dialog

  Three types of access right groups can be displayed: **Predefined ARGs**, **Manually created ARGs**, and **ARGs for Dynamic Applications**. You can use the View menu - Access Right Group Configuration or the Context Menu to show or hide each of these groups, as required.
- Access Rights - Component/Application Tree (Right Hand Side Pane), Access Right Group Configuration dialog
- Preview Panes, Access Right Group Configuration dialog

  The Preview Panes, Access Right Group Configuration dialog at the bottom of the two dialog areas show short descriptions of the currently selected access rights. The **Preview Panes** can be displayed and hidden, respectively, using the **Display Info on Access Right** option in the View menu - Access Right Group Configuration or the corresponding icons in the Toolbar. The height of the preview panes can be changed.

  – Preview Pane, Left Hand Side Area, Access Right Group Configuration dialog
  – Preview Pane, Right Hand Side Area, Access Right Group Configuration dialog

  For more information please refer to Areas and Preview Panes in the Access Right Group Configuration dialog.
- Toolbar

  The **Toolbar Icons** have the same functionality as the entries in the main menus. For a description of the icons in the toolbar, please refer to Toolbar Icons - Access Right Group Configuration dialog.
- Menu Bar

Related Topics

Context Menu

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

2.11.1.1 Access Right Groups (Left Hand Side Pane), Access Right Group Configuration dialog

The **Access Right Group Configuration** dialog consists of a vertically divided window with two panes, each displaying access rights and access right groups in a multi-level tree, structured as follows:

Left Hand Side Pane: Access Right Groups

- Top Level: All available access right groups (ARGs).

  Contains the folders of all available access right groups, grouped by registration units.

  One access right group may contain several components.

  Three categories of access right groups can be displayed: **Predefined ARGs**, **Manually created ARGs**, and **ARGs for Dynamic Applications**. You can use the View menu - Access Right Group Configuration or the Context Menu to show or hide each of these group categories, as required. See also Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.
- Second Level: Subfolders; Each subfolder usually represents one component containing all access rights assigned to the user within this component.
- Third Level: All access rights assigned to the user within an access right group.

See also Areas in the Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

Toolbar Icons - Access Right Group Configuration dialog

Edit menu - Access Right Group Configuration

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

Access Management tab sheet in System Management, User Interface

2.11.1.2 Access Rights - Component/Application Tree (Right Hand Side Pane), Access Right Group Configuration dialog

The **Access Right Group Configuration** dialog consists of a vertically divided window with two panes, each displaying access rights and access right groups in a multi-level tree, structured as shown below.

Right Hand Side Pane: Access Rights - Component/Application Tree

In this area you can choose between the **Component Tree** view and the **Application Tree** view. To switch to the alternate view, select **Access Rights - Show Component Tree** or **Access Rights - Show Application Tree**, respectively, in the View menu - Access Right Group Configuration, in the Context Menu or in the Toolbar. In the **Context Menu** these view options are only displayed if the mouse pointer is located in the right hand side dialog area.

- **Component Tree view**
  - Top Level: Each folder represents a component. The applications within components are hidden in this view. Within each component, the assignable access rights are directly displayed as selectable items.
  - Second Level: The assignable access rights are directly displayed as selectable items within each component.

    You can use Drag&Drop to assign access rights (from the right hand side pane) to certain access right groups (in the left hand side pane) - see description in Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.
- **Application Tree view**
  - Top Level: Each top level folder represents a component. Applications are displayed as subfolders within the components. Each component may contain one or more applications.
  - Second Level: This level is only visible in the **Application Tree** view. Applications are displayed as subfolders within components in this view. Each component may contain one or more applications. Within each application, the assignable access rights are displayed as selectable items.
  - Third Level: The assignable access rights are displayed as selectable items within the application folders in this view. (Available components may consist of more than one application offered on the user's start page.)

  You can use Drag&Drop to assign access rights individually (from the right hand side pane) to certain access right groups (in the left hand side pane)-

see description in Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.

NOTICE: Assigning at least one access right from an application to an access right group has the effect that the respective application will be displayed on the Start Page for all users having the required access rights for this application.

See also Areas in the Access Right Group Configuration dialog and Areas and Preview Panes in the Access Right Group Configuration dialog, and Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

Toolbar Icons - Access Right Group Configuration dialog

Edit menu - Access Right Group Configuration

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

Access Management tab sheet in System Management, User Interface

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

2.11.2 Preview Panes, Access Right Group Configuration dialog

The **Preview Panes** at the bottom of the two dialog areas, labeled **Information on Access Right**, show short descriptions of the currently selected access right(s).

You can show or hide the **Preview Panes** by activating or deactivating the **Display Info on Access Right** option in the View menu - Access Right Group Configuration, respectively. The height of the preview panes can be changed.

For additional information, please refer to

Access Right Groups (Left Hand Side Pane), Access Right Group Configuration dialog, and

Access Rights - Component/Application Tree (Right Hand Side Pane), Access Right Group Configuration dialog.

Related Topics

Areas in the Access Right Group Configuration dialog

View menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

2.11.2.1 Preview Pane, Left Hand Side Area, Access Right Group Configuration dialog

The **Preview Panes** at the bottom of the two areas of the **Access Right Group Configuration** dialog, both labeled **Information on Access Right**, can be shown or hidden, respectively, by activating or deactivating the **Display Info on Access Right** option in the View menu - Access Right Group Configuration. The height of the preview panes can be changed.

The **Preview Panes** show short descriptions of the currently selected access right(s).

Related Topics

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

Access Management tab sheet in System Management, User Interface

View menu - Access Right Group Configuration

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

2.11.2.2 Preview Pane, Right Hand Side Area, Access Right Group Configuration dialog

The **Preview Panes** at the bottom of the two areas of the **Access Right Group Configuration** dialog, both labeled **Information on Access Right**, can be shown or hidden, respectively, by activating or deactivating the **Display Info on Access Right** option in the View menu - Access Right Group Configuration. The height of the preview panes can be changed.

The **Preview Panes** show short descriptions of the currently selected access right(s).

Related Topics

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

Access Management tab sheet in System Management, User Interface

View menu - Access Right Group Configuration

Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

2.11.3 Assigning/Withdrawing Access Rights, Access Right Group Configuration dialog

Note that the following operations are **not valid** for **predefined** access right groups.

Assigning Access Rights to Access Right Groups

1) Select an access right in the right hand side window area.

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

2) Drag the selected access right with the mouse into the left hand area, and drop the access right on that access right group to which the access right should be assigned.

If you selected multiple **non-consecutive** items you need to press and hold down the **Ctrl** key while performing the Drag&Drop action in order to avoid de-selecting the selected items.

or

1) Select one or more access rights in the right hand side area.

2) In the left hand side area, select the access right group(s) which should get these groups. Be sure to select only access right groups from this list.

3) Choose **Edit** - **Assign** from the menu bar

or

Click the appropriate button in the Toolbar

or

Choose the appropriate command from the Context Menu

Using this feature, access rights can be assigned to more than one access right group in one step.

Withdrawing Access Rights from Access Right Groups

1) Select the access rights to be withdrawn from an access right group in the left hand side area.

2) Choose **Edit - Withdraw** from the menu bar

or

Click the appropriate button in the Toolbar.

or

Choose the appropriate command from the Context Menu.

All changes are sent immediately to the server and therefore apply to all new logons of affected users. The changes may also affect already running sessions, since Access Management notifies other applications in regular time intervals about those changes.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

View menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

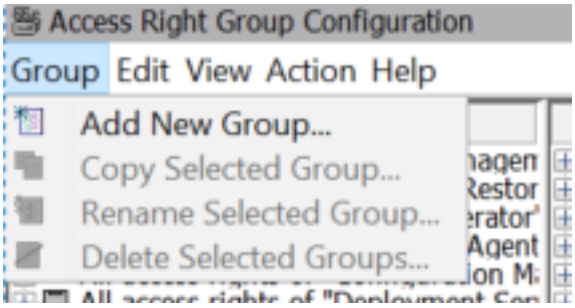
Areas in the Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

Access Management tab sheet in System Management, User Interface

2.11.4 Group menu - Access Right Group Configuration

The **Group** menu is only displayed in the Access Right Group Configuration dialog. It is used to add, copy, rename and delete access right groups from the system. It contains the following entries:



Menu Options

Add New Group	Opens the **Add new Access Right Group** dialog.
Copy Selected Group	Opens the **Copy selected Access Right Group** dialog.
Rename Selected Group	Opens the **Rename selected Access Right Group** dialog.
Delete Selected Groups	Deletes the selected access right group(s) after confirmation with **OK**.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

Edit menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

View menu - Access Right Group Configuration

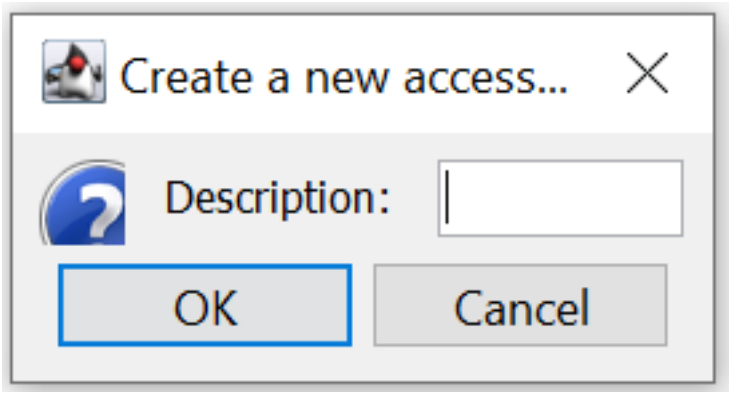
Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

2.11.5 Add New Access Right Group

The **Add new Access Right Group** dialog is displayed when you click on **Add new group** in the **Group**menu or on the icon in the toolbar.



User Interface

Description	Entry field for account name of access right group. The functionality of the **Description** field is the same for all of the following actions started from the **Group** menu: **Add new group**, **Copy selected group**, **Rename selected group.**
OK	Confirm and execute action.
Cancel	Abort action.

Related Topics

Toolbar

Context Menu

Menu Bar

User menu

Delete User Accounts

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

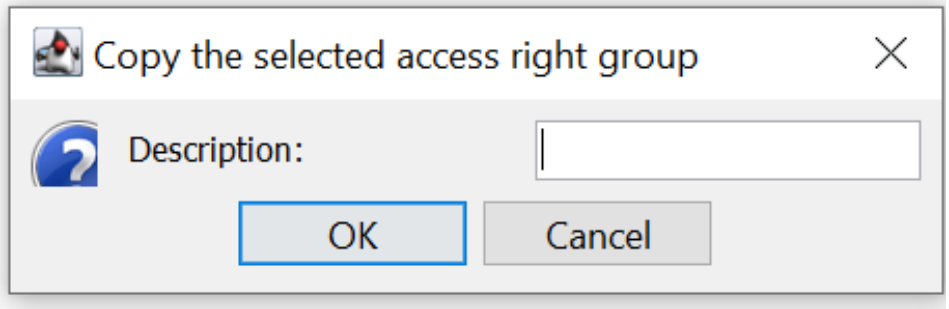
Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

2.11.6 Copy selected Access Right Group

The **Copy the selected Access Right Group** dialog is displayed when you click on **Copy selected group** in the **Group** menu or alternatively on the icon in the Toolbar or the Context Menu.



User Interface

Description	Entry field for account name of access right group. The functionality of the **Description** field is the same for all of the following actions started from the **Group** menu: **Add new group**, **Copy selected group**, **Rename selected group.**
OK	Confirm and execute action.
Cancel	Abort action.

Related Topics

Toolbar

Context Menu

Menu Bar

User menu

Delete User Accounts

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

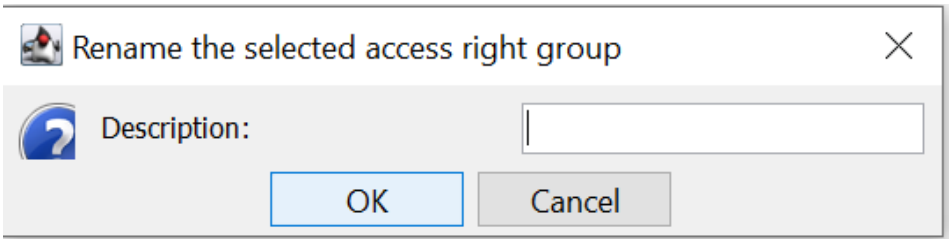
Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

2.11.7 Rename selected Access Right Group

The **Rename selected Access Right Group** dialog is displayed when you click on **Rename selected group** in the **Group**menu or on the icon in the toolbar.



User Interface

Description	Entry field for account name of access right group. The functionality of the **Description** field is the same for all of the following actions started from the **Group** menu: **Add new group**, **Copy selected group**, **Rename selected group.**
OK	Confirm and execute action.
Cancel	Abort action.

Related Topics

Toolbar

Context Menu

Menu Bar

User menu

Delete User Accounts

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

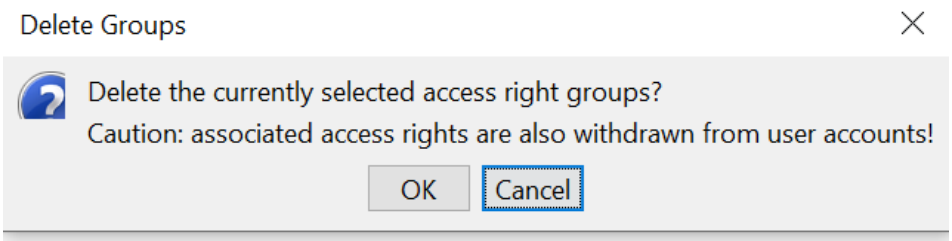
Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

2.11.8 Delete Groups

The **Delete Groups** dialog is displayed when you click on **Delete Selected Groups** in the **Group**menu or on the corresponding icon in the toolbar.

To delete an access right group or several groups, you need to select the group(s), then click on **Delete Selected Groups** in the **Group** menu or on the corresponding icon in the toolbar, and finally confirm the deletion with **OK**.



NOTICE: Assigning at least one access right from an application to an access right group has the effect that the respective application will be displayed on the Start Page for all users having the required access rights for this application.

User Interface

OK	Confirm and execute action.

Cancel	Abort action.

Related Topics

Toolbar

Context Menu

Menu Bar

User menu

Delete User Accounts

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

2.11.9 Edit menu - Access Right Group Configuration

The **Edit** menu is displayed in all dialogs of the **Account Management** component. In the **Access Right Group Configuration** dialog it contains the following entries:

Menu Options

Assign Access Rights	Clicking on **Assign Access Rights** in the **Edit** menu assigns the selected access right(s) selected in the right area to the group(s) selected in the left area. You can also use the Context Menu or the Toolbar to execute this command.
Withdraw Access Rights	• Clicking on **Withdraw Access Rights** in the **Edit** menu removes access right(s) selected in the left area from the associated access right group(s). • You can also use the Context Menu or the Toolbar to execute this command. • **Note:** The **Withdraw Access Rights** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.
Replace Access Rights	• Select the batch of manually created access right groups (this feature only works with MANUALLY CREATED access right groups) in the left hand side area, and the batch of individual access rights or higher-ranking folders in the right hand side area. Click on **Replace Access Rights** in the **Edit** menu to replace the previously assigned access rights with the currently selected access rights. The previously assigned access rights will be overwritten during this process. Difference to **Assign**: In the case of **Assign** the newly selected access rights are appended (added) to the already existing assigned access rights, which are not overwritten. Alternative ways to execute this command: Via the Context Menu or via the Toolbar. • **Note:** The **Replace Access Rights** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Withdraw All Access Rights	• Select the batch of manually created access right groups (this feature only works with MANUALLY CREATED access right groups) in the left hand side area. You can hide the other categories of access right groups, thus only displaying the manually created access right groups. Click on **Withdraw All Access Rights** in the **Edit** menu to withdraw all assigned access rights from the selected access right group(s). Alternative ways to execute this command: Via the Context Menu or via the Toolbar. **Note:** The **Withdraw All Access Rights** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.
Reload	Clicking on **Reload** in the **Edit** menu updates the contents of the **Access Right Group Configuration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. This command has the same function as the **Reload items from Server** icon in the Toolbar.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Toolbar

Context Menu

Group menu - Access Right Group Configuration

View menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

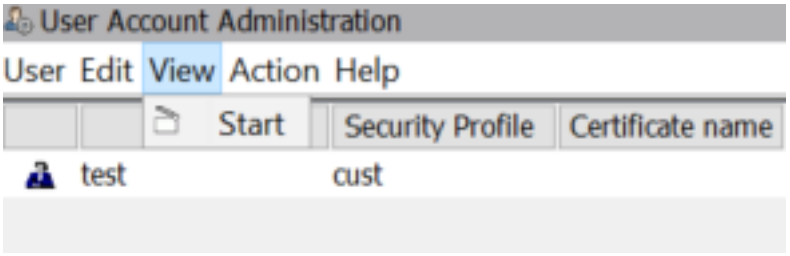
Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

Access Right Configuration dialog - User Interface Description

2.11.10 View menu - Access Right Group Configuration

The **View** menu contains the following entries:



Menu Options

Start	Same function as **View Start Page** icon in toolbar. Opens new browser window displaying **OpenScape 4000 Assistant/Manager Start Page**.

Alternative Ways to Execute the Command(s)

Using the Edit menu - Access Right Group Configuration

or

Using the Context Menu

or

Using the Toolbar

Selecting items

To select multiple consecutive items (access rights or access right groups, respectively), press and hold down the **Shift** key while selecting items/users with the left mouse key.

To select multiple **non-consecutive** items or to de-select individual items, press and hold down the **Ctrl** key while selecting items/users with the left mouse key.

Related Topics

Context Menu

Group menu - Access Right Group Configuration

View menu - Access Right Group Configuration

Help menu - Access Right Group Configuration

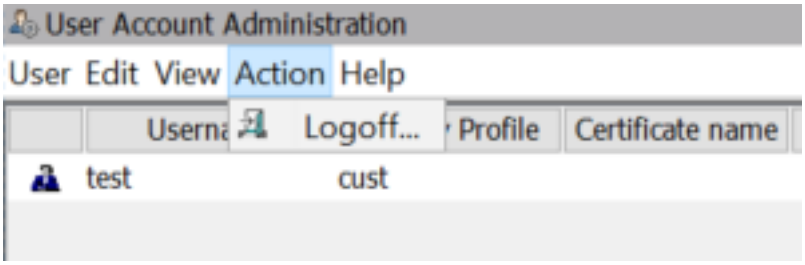
Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog.

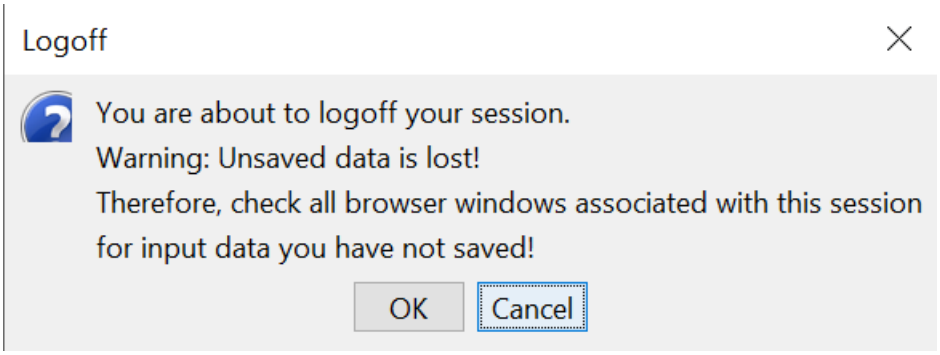
Access Right Configuration dialog - User Interface Description

2.11.11 Action menu, Access Right Group Configuration

The **Action** menu contains the **Logoff** menu option, which has the same function as the **Logoff** icon in the toolbar in the upper right corner of the screen. See also Toolbar Icons - Access Right Group Configuration dialog.



When you click the **Logoff** menu option or the icon in the toolbar, an error message dialog is displayed, warning you that all unsaved data will be lost, and prompting you to save all session data, close all browser windows belonging to the current session, and confirm your intention to log off.



Related Topics

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

View menu - Access Right Group Configuration

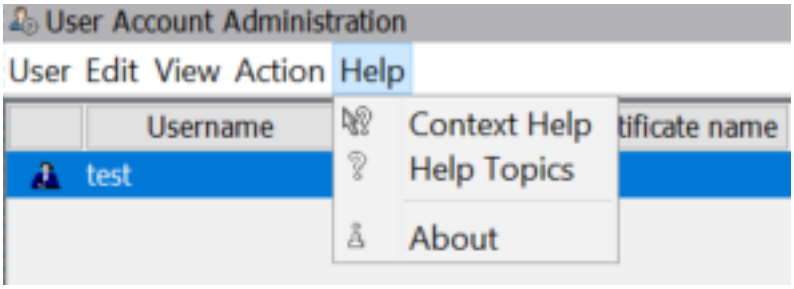
Help menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

2.11.12 Help menu - Access Right Group Configuration

The **Help** menu is displayed with all components of the **Account Management** component, except for **Export User Reports**. The **Help** menu options are the same with all components, as follows:



Context Help	Clicking on **Context Help** opens the context sensitive Online Help related to a specific item that you select with the mouse. The Context Help can alternatively be started by selecting a specific item in the UI with the mouse and then pressing **CTRL**+**F1**.
Help Topics	Clicking on the **Help Topics** opens the Online Help Topics. The Online Help can also be started by pressing the **F1** key.
About	The **About** dialog contains the information about the software version of the program, the release date, and the copyright provisions.

Related Topics

Menu Bar

User menu

Group menu - Access Right Group Configuration

Edit menu - Access Right Group Configuration

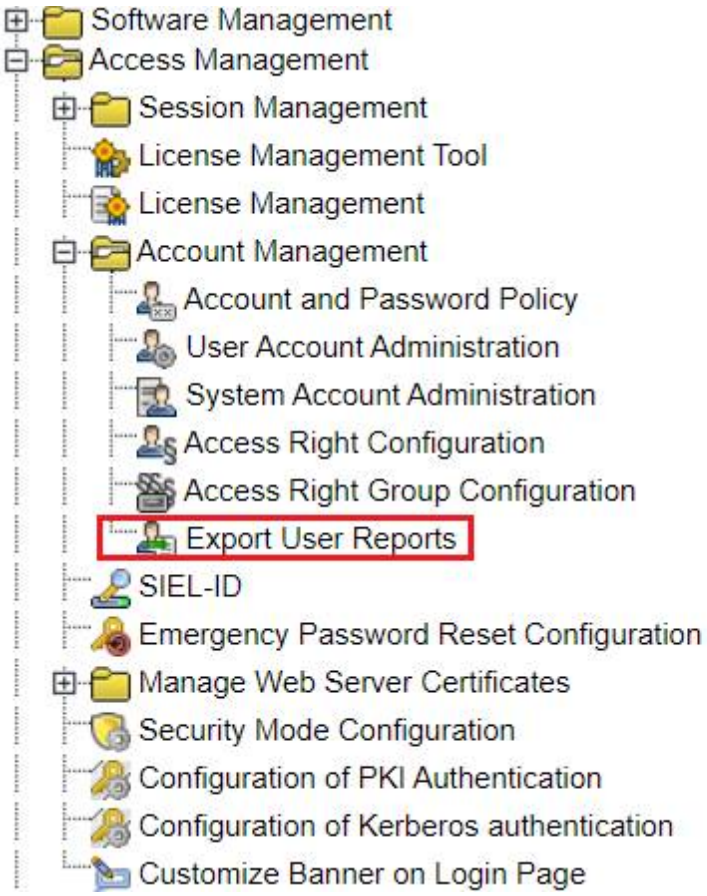
View menu - Access Right Group Configuration

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

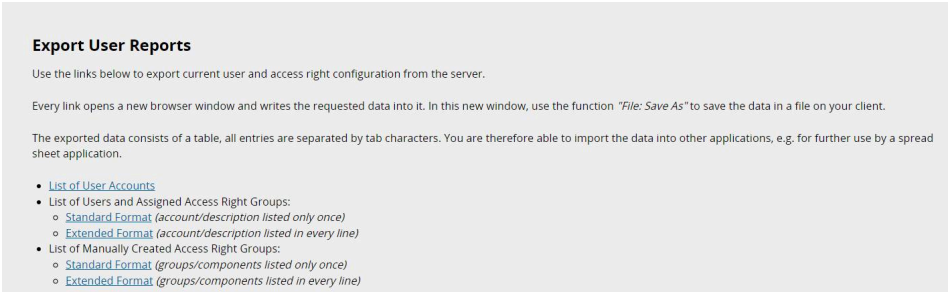
2.12 Export User Reports

The **Export User Reports** link on the **Start Page** of **Access Management**, **Account Management** folder opens the **Export User Reports** window.



Use the links in the **Export User Reports** window to export user and access right configuration data from a system's server.

The **Export User Reports** feature is used to display and export the following user data:



List of User Accounts, Export User Reports window

List of Users and Assigned Access Right Groups, Export User Reports window

List of Manually Created Access Right Groups, Export User Reports window

2.12.1 List of User Accounts, Export User Reports window

Click on the **List of User Accounts** link to display the list of all installed user IDs and their corresponding password attributes for a system. Clicking on this link opens a new browser window in which the requested data will be displayed.

To save the data to a file on your system, select **File** -> **Save As** in the newly opened browser window, and save the contents as a **text file** (***.txt**).

If you want to directly save the data to a file without previous display, click on the **List of User Accounts** link with the right mouse key and select **Save Target As** from the context menu, then save the data to a **text file** (***.txt**).

To import the text file into a spread sheet program for further editing or evaluation, e.g. into MS Excel, select **Data** -> **External Data** -> **Import Text File**.

	A	B	C	D	E
1	# eur.cgi v1.0				
2	**Export User Reports: List of User Accounts**	**6/24/2010 12:17**	**Manager**	**0.52**	
3	**Username**	**Description**	**Locked**	**Max. Password Validity**	**Change Password Allowed**
4	stevie	stevieb@mycomp.com, x12345	No	40	No
5	gert	gertf@mycomp.com, x98765	No	80	Yes
6	peter	peters@mycomp.com, x24680	No	40	Yes
7	mark	markw@mycomp.com, x86420	No	40	Yes
8	chris	chriss@mycomp.com, x13579	No	-1	No
9	# 0				
10					

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: List of User Accounts

User Name

Description

Locked

Max. Password Validity

Change Password Allowed

2.12.2 List of Users and Assigned Access Right Groups, Export User Reports window

Click on the **List of Users and Assigned Access Right Groups** link to display the list of all installed user IDs and all access right groups assigned to these user accounts. Clicking on this link opens a new browser window in which the requested data will be displayed.

To save the data to a file on your system, select **File** -> **Save As** in the newly opened browser window, and save the contents as a **text file** (***.txt**).

If you want to directly save the data to a file without previous display, click on the **List of User Accounts** link with the right mouse key and select **Save Target As** from the context menu, then save the data to a **text file** (***.txt**).

To import the text file into a spread sheet program for further editing or evaluation, e.g. into MS Excel, select **Data** -> **External Data** -> **Import Text File**. User name and corresponding description are displayed in each row.

	A	B	C	D	E	F
1	**# eur.cgi v1.0**					
2	**Export User Reports: List of Users and Assigned Access Right Groups**	**6/24/2010 12:17**	**Manager**	**0.52**		
3	**Username**	**Description**	**ID of Access Right Group**	**Description of Access Right Group**		
4	stevie	stevieb@mycomp.com, x12345	arg3	Local Administrator		
5	gert	gertf@mycomp.com, x98765	arg2	Config. Management read-only		
6			all-PM	All access rights of "Performance Management"		
7	peter	peters@mycomp.com, x24680	arg3	Local Administrator		
8			all-RepGen	All access rights of "Report Generator"		
9	mark	markw@mycomp.com, x86420	all-SysM	All access rights of "System Management"		
10			arg2	Config. Management read-only		
11	chris	chriss@mycomp.com, x13579	all-cm_subadr	All access rights of "Configuration Management"		
12			all-SysM	All access rights of "System Management"		
13			all-FaultM	All access rights of "Fault Management"		
14	# 0					

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: Liste of Users and Assigned Access Right Groups

User Name

Description

ID of Access Right Group

Description of Access Right Group

2.12.3 List of Manually Created Access Right Groups, Export User Reports window

Click on the **List of Manually Created Access Right Groups** link to display the list of all installed user IDs and their assigned access rights. Clicking on this link opens a new browser window in which the requested data will be displayed.

To save the data to a file on your system, select **File** -> **Save As** in the newly opened browser window, and save the contents as a **text file** (***.txt**).

If you want to directly save the data to a file without previous display, click on the **List of User Accounts** link with the right mouse key and select **Save Target As** from the context menu, then save the data to a **text file** (***.txt**). To import the text file into a spread sheet program for further editing or evaluation, e.g. into MS Excel, select **Data** -> **External Data** -> **Import Text File**. User name and corresponding description are displayed in each row.

	A	B	C	D	E	F
1	**# eur.cgi v1.0**					
2	**Export User Reports: List of Manually Created Access Right**	**6/24/2010 12:18**	**Manager**	**0.52**		
3	**ID of Access Right Group**	**Description of Access Right Group**	**ID of Component**	**Description of Component**	**ID of Access Right**	**Description of Access Right**
4	**arg1**	Expert Switch Administration	**SecM**	**Access Management**	H300_ACF1_feature	ComWin AMO Access Right Group 01
5					nsl_own	Network Single Logon
6			**cm_subadm**	**Configuration Management**	HZ0	6.5 / 6.6 PIN (read access)
7			**LicM**	**License Management**	retrieveLicData	View License Data
8					storeLicData	Install License Data
9			**HBR**	**HBR**	HBR_Admin	Administration Backup Device
10					HBR_Backup	Backup
11	**arg2**	**Config. Management read-only**			HBR_Schedule	Backup Schedule Configuration
120	**arg3**	**Local Administrator**			HBR_Common	Read Access
121			**LogM**	**Logging Management**	logm_all	LogM Feature
122			**SecM**	**Access Management**	wsm_own	Manage own sessions
123			**Lap**	**Lap**	dynamicAdaptions	Dynamic Adaptations
124					sendBroadcast	Broadcast

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: Liste of Manually Created Access Right Groups

ID of Access Right Group

Description of Access Right Group

ID of Component

Description of Component

ID of Access Right

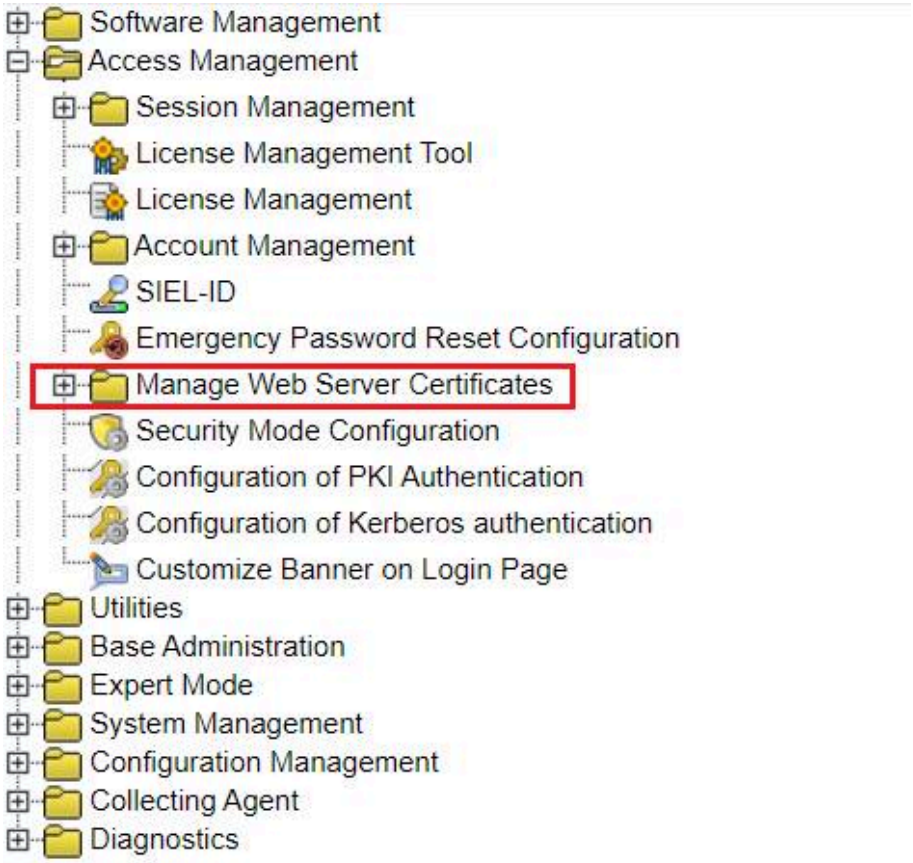
Description of Access Right

2.13 Manage Web Server Certificates

The **Manage Web Server Certificates** area comprises the following features:

- Certificates for this Web Server
  - Activate - HG35xx Board NOT Installed
  - Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only
  - Generate
  - Import
  - Generate via CSR

- Certificate Network Management
  - Root Certificate
  - Sign CSR
  - Import of Certificate Authority (CA) for distribution to clients



2.13.1 Certificates for this Web Server

Two public key asymmetric algorithms are supported for web server certificates:

- RSA

  RSA was standardized in 1994 and it is the most used algorithm which has stood the test of time. The key has a length of 2048 bits and it is considered to be a security standard.
- ECDSA

  ECDSA was standardized in 2005 and, compared to RSA, offers the same level of security but with smaller key sizes. Smaller keys result in faster computations and less storage space required.

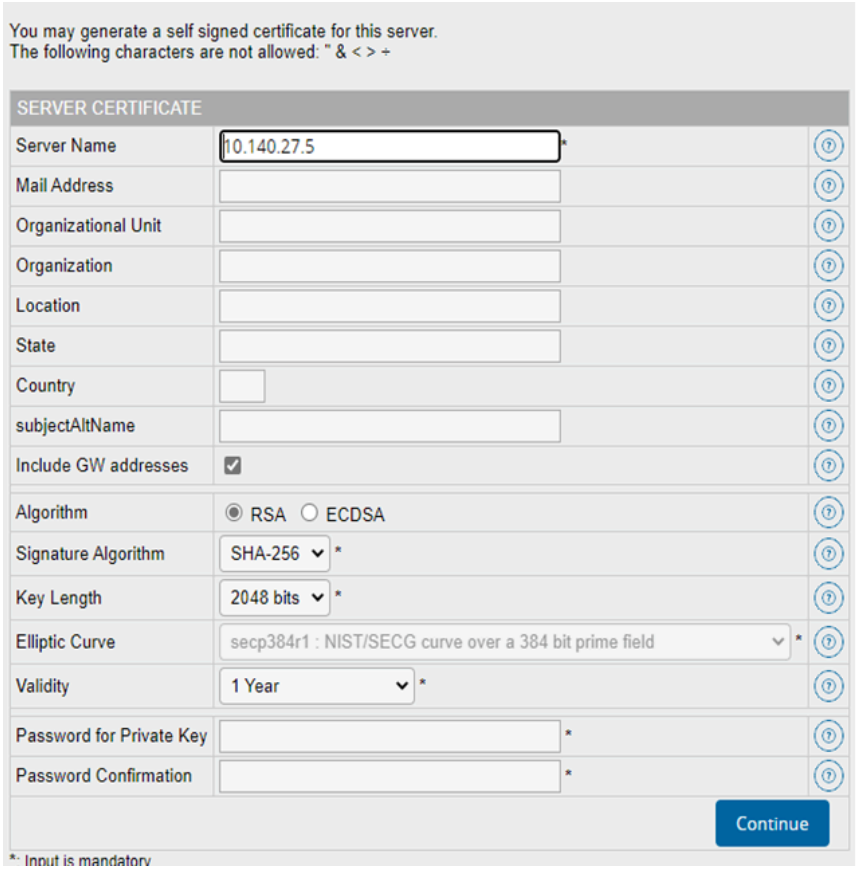
SHA-2 support for Digital Signatures

OpenScape 4000 supports the SHA-2 set of cryptographic hash functions to digitally sign certificates generated on the system. SHA-2 provides a stronger security of the generated certificates. The SHA-2 family implemented in OpenScape 4000 consists of several hash functions: SHA256, SHA384 and SHA512 (SHA224 is not supported by Internet Explorer and therefore not provided as an option). The number in the name of the function represents the

length of the hash values in bits. OpenScape 4000 uses the OpenSSL tool to generate and sign certificates.

You can choose the below parameters during the generation of a certificate. The SPE SSL Root Certificate and SPE SSL Certificate dialogs offer:

- Algorithm type radio button where the selection affects the following parameters
- A Signature Algorithm drop-down box where you can select the cryptographic function: SHA-256, SHA-384, or SHA-512.
- For RSA, the key length must be specified. The minimum length of 2048 bits is considered a security standard.
- For ECDSA the elliptic curve must be specified. All openssl supported elliptic curves for ECDSA algorithm are listed here. The most popular curves are: NIST-approved Suite B, e.g. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1).



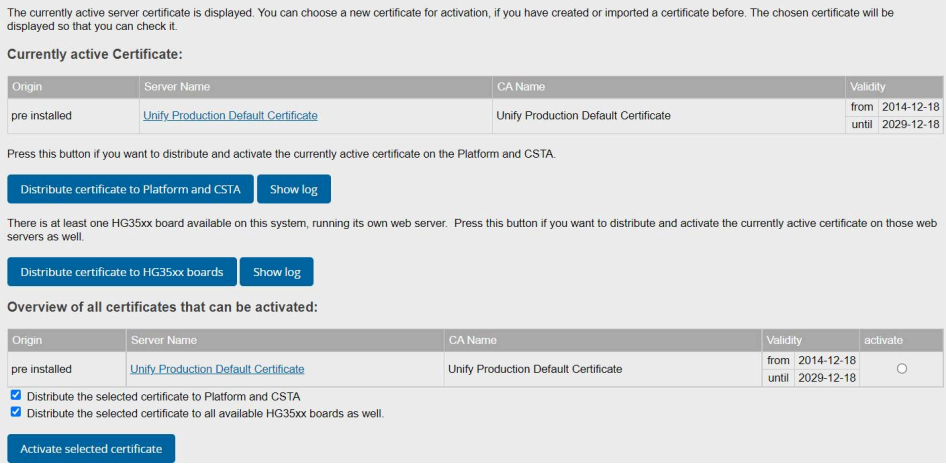
- Activate - HG35xx Board NOT Installed
- Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only
- Generate
- Import
- Generate via CSR

2.13.1.1 Activate - HG35xx Board NOT Installed

On the **Start Page** of **Access Management** navigate to **Manage Web Server Certificates -> Certificates for this Web Server**.

Click or double-click **Activate** to open the **Activate Server Certificate** dialog. The following certificates are displayed:

- Currently Active Certificate (Table in Activate Server Certificate dialog)
- Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)



User Interface

The following certificates are displayed in the **Activate Server Certificate** dialog:

- Currently Active Certificate (Table in Activate Server Certificate dialog)

  The active security certificate currently used by the SSL HTTP Server, and
- Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

  The list of all certificates that can be activated. You can select a new certificate to be activated from this list if you previously generated or imported such a certificate. The selected certificate will then be displayed for verification purposes.

  Only signed certificates can be activated.

> **NOTICE:** The software is shipped with a pre-installed security certificate by default. A password is not required with pre-installed certificates. The Password entry field is not displayed with pre-installed certificates.

Distributing the CURRENTLY ACTIVE Certificate To Platform - Assistant only

1) Click on the **Distribute Certificate to Platform** button beneath the **Currently Active Certificate** table.

   The subsequent **Activate Server Certificate** dialog is displayed and you are prompted to enter the password for the private key of the certificate.

2) Enter the password and click on **Distribute Certificate**.
3) The **Status** dialog will then display the progress of distribution and activation.
4) Distribution finishes with one of the following messages:
   - a confirmation message regarding the successful distribution of the certificate, or
   - an error message informing you that an error occurred during the distribution of the active server certificate to the Platform.

   The error message is displayed on the screen and you are prompted to repeat the process.
5) If the error still persists, you should send the displayed error message to your system administrator or to the service department.

NOTICE:

For Standalone and Survivable SoftGates and Standalone and Survivable EntGW, when the SoftGate SW receives the web certificate from Assistant it is forwarding it to the Platform Portal before the Apache web server is restarted to activate the certificate.

Activating a Certificate

If you want to activate another certificate instead of the currently active one, please proceed as follows:

1) In the **Activate Server Certificate** dialog, **Overview of all certificates that can be activated** table, **Activate** column, select the radio button of the certificate you want to activate. If you want the selected certificate to be activated and distributed to the Platform at the same time, check the **Distribute the selected certificate to Platform** checkbox located beneath the **Overview of all certificates that can be activated** table.(The distribution of ertificates to Platform is only available for the Assistant.)

   Only signed certificates can be activated.
2) Click **Continue**.

   The certificate details are then displayed in the **Activate Server Certificate** dialog, and the program prompts you to enter the password for the private key.

   Entering a password is not required with pre-installed certificates. Therefore, the password prompt and the password entry field are not displayed with pre-installed certificates.
3) Enter the **Password** for the private key, if required, and click on **Activate certificate**.

NOTICE: The Web Server and OpenScape 4000 processes always need to be restarted after activating a new certificate. All currently running sessions, including your own session, will be terminated upon restart.

A warning message is displayed, alerting you that the Web Server and OpenScape 4000 processes need to be restarted after activating a new

certificate, and that all currently running sessions, including your own session, will be terminated on the server.

The selected certificate is activated and displayed as new **Currently active Certificate** in the **Activate Server Certificate** dialog.

or

4) Click on **Back** in the **Activate Server Certificate** dialog if you do not want to activate the new certificate.

Field Descriptions

Activate (Link on Start Page of Access Management)

Currently Active Certificate (Table in Activate Server Certificate dialog)

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

Delete Certificate (Button in Certificate Information view, Display Certificate dialog)

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Distribute active certificate (Button beneath Currently Active Certificate table, Activate Server Certificate dialog**)**

Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

Activate (Radio Button in Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog**)**

Distribute the selected certificate to all available HG35xx boards as well (Checkbox beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Activate selected certificate (Button beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Activate certificate (Button, Activate Server Certificate dialog)

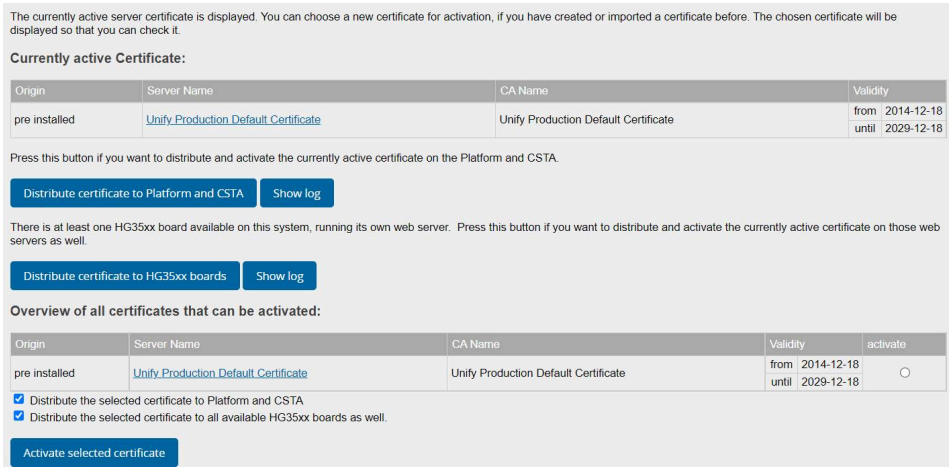
Back (Button, Activate Server Certificate dialog)

2.13.1.2 Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only

Provided that on this system there is at least one HG35xx board with an independently running Web Server installed, the following additional controls will be displayed in the **Activate Server Certificate** dialog:

- Distribute active certificate (Button beneath Currently Active Certificate table, Activate Server Certificate dialog)

- Distribute the selected certificate to all available HG35xx boards as well (Checkbox beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)



NOTICE: The HG35xx boards that are not based on Linux (STMI and NCUI) support only RSA certificates for web based administration. If the selected certificate type is ECDSA, it will not be distributed to these types of boards. All SoftGate based boards support ECDSA.

User Interface

The following certificates are displayed in the **Activate Server Certificate** dialog:

- Currently Active Certificate (Table in Activate Server Certificate dialog)

  The active security certificate currently used by the SSL HTTP Server, and
- Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

  The list of all certificates that can be activated. You can select a new certificate to be activated from this list if you previously generated or imported such a certificate. The selected certificate will then be displayed for verification purposes.

  Only signed certificates can be activated.

NOTICE: The software is shipped with a pre-installed security certificate by default. A password is not required with pre-installed certificates. The Password entry field is not displayed with pre-installed certificates.

Distributing the CURRENTLY ACTIVE Certificate To Platform - Assistant only

1) Click on the **Distribute Certificate to Platform** button beneath the **Currently Active Certificate** table.

   The subsequent **Activate Server Certificate** dialog is displayed and you are prompted to enter the password for the private key of the certificate.
2) Enter the password and click on **Distribute Certificate**.

3) The **Status** dialog will then display the progress of distribution and activation.
4) Distribution finishes with one of the following messages:
   - a confirmation message regarding the successful distribution of the certificate, or
   - an error message informing you that an error occurred during the distribution of the active server certificate to the Platform.

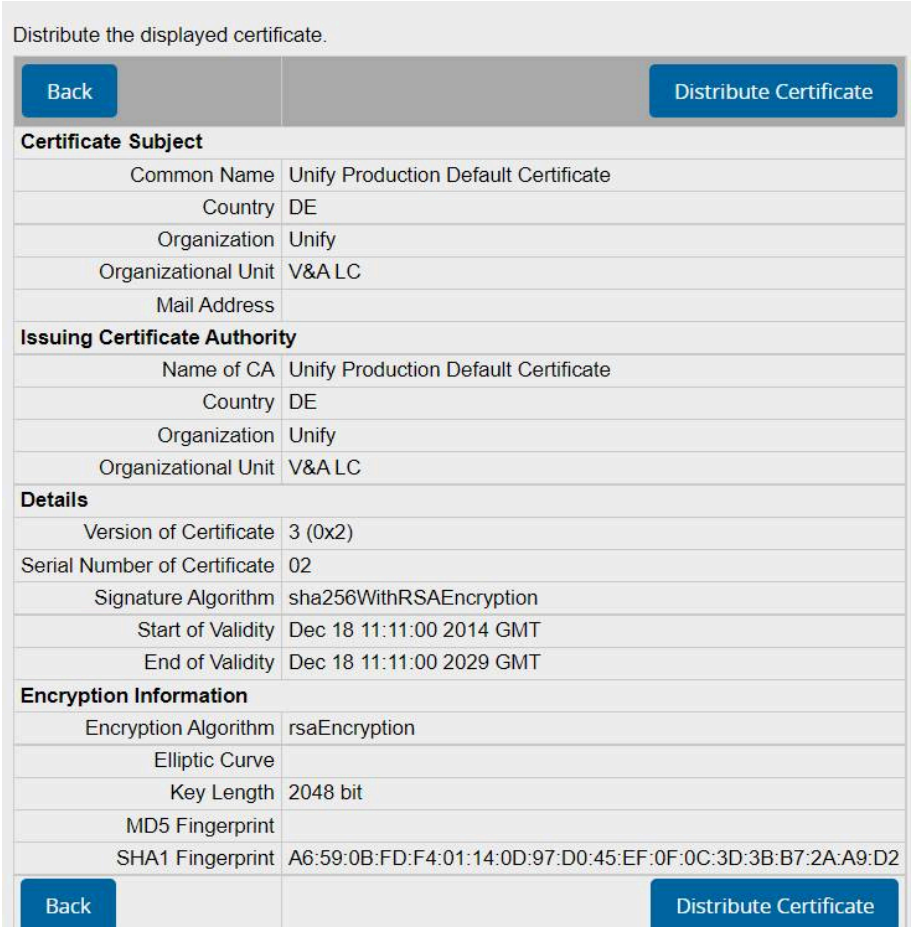
   The error message is displayed on the screen and you are prompted to repeat the process.
5) If the error still persists, you should send the displayed error message to your system administrator or to the service department.

NOTICE: HG35xx boards that are not based on Linux (STMI and NCUI) support only RSA certificates for web based administration. If the selected certificate type is ECDSA, it will not be distributed to these types of boards. All SoftGate based boards support ECDSA.

Distributing the CURRENTLY ACTIVE Certificate To All Available HG35xx Boards

1) Click on the **Distribute Certificate to HG35xx boards** button beneath the **Currently Active Certificate** table.

   The subsequent **Activate Server Certificate** dialog is displayed and you are prompted to enter the password for the private key of the certificate.



2) Enter the password and click on **Distribute Certificate**.
3) The **Status** dialog will then display the progress of distribution and activation.
4) Distribution finishes with one of the following messages:

   - a confirmation message regarding the successful distribution of the certificate, or
   - an error message informing you that an error occurred during the distribution of the active server certificate to the HG35xx boards.

   The error message is displayed on the screen and you are prompted to repeat the process, and -- if the error should occur again -- you should verify the configuration using the Gateway Dashboard, update the board list, and establish a connection to all boards listed.
5) If the error still persists, you should send the displayed error message to your system administrator or to the service department.

Activating and Distributing a SELECTED Certificate to All Available HG35xx boards and/or to Platform - Assistant only

If you want to activate another certificate instead of the currently active one, please follow the steps described in the **Activating a Certificate** section.

If you want the selected certificate to be activated and distributed to all available HG35xx boards and/or Platform at the same time, please proceed as follows:

1) Check the **Distribute the selected certificate to Platform** checkbox located beneath the **Overview of all Certificates That Can Be Activated** table.
2) Check the **Distribute the selected certificate to all available HG35xx boards** checkbox located beneath the **Overview of all Certificates That Can Be Activated** table.
3) Click on the **Activate selected certificate** button located beneath the **Overview of all Certificates That Can Be Activated** table.

   The selected certificate is activated on the server as usual an distributed to all available HG35xx boards at the same time.

Field Descriptions

Activate (Link on Start Page of Access Management)

Currently Active Certificate (Table in Activate Server Certificate dialog)

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

Delete Certificate (Button in Certificate Information view, Display Certificate dialog)

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Distribute active certificate (Button beneath Currently Active Certificate table, Activate Server Certificate dialog**)**

Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

Activate (Radio Button in Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog**)**

Distribute the selected certificate to all available HG35xx boards as well (Checkbox beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Activate selected certificate (Button beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

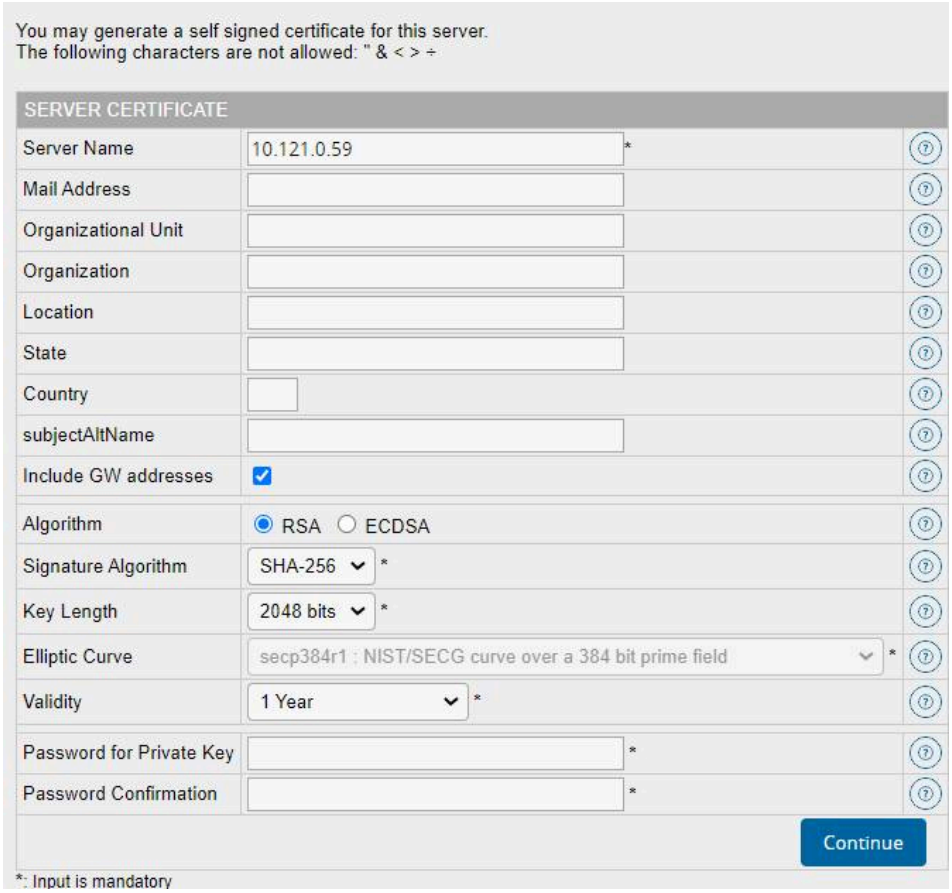
Activate certificate (Button, Activate Server Certificate dialog)

Back (Button, Activate Server Certificate dialog)

2.13.1.3 Generate

The **Generate** feature provides the simplest method of creating a new SSL certificate and having it self signed by the server.

For this purpose the server creates an internal own Certificate Authority (CA) that automatically self-signs the newly created certificate. The name of this Certificate Authority is always identical with the server name. The certificate created and self signed by this method can then be activated. A root certificate is not necessary for creating a new certificate.



If a self signed certificate already exists for the server, the data of the existing certificate and a corresponding note are displayed in the browser in the **Display Certificate** dialog.

NOTICE: Warning! If you create a new certificate although a self signed certificate already exists for this server, the existing certificate will be overwritten.

Creating a New Certificate

1) On the **Start Page** of **Access Management**, navigate to **Manage Web Server Certificates -> Certificates for this Web Server** and click or double-click on **Generate**.

   A self signed certificate has already been created for this server

   If a self signed certificate already exists for this server, the data of the existing certificate will be displayed in the browser in the **Display Certificate**

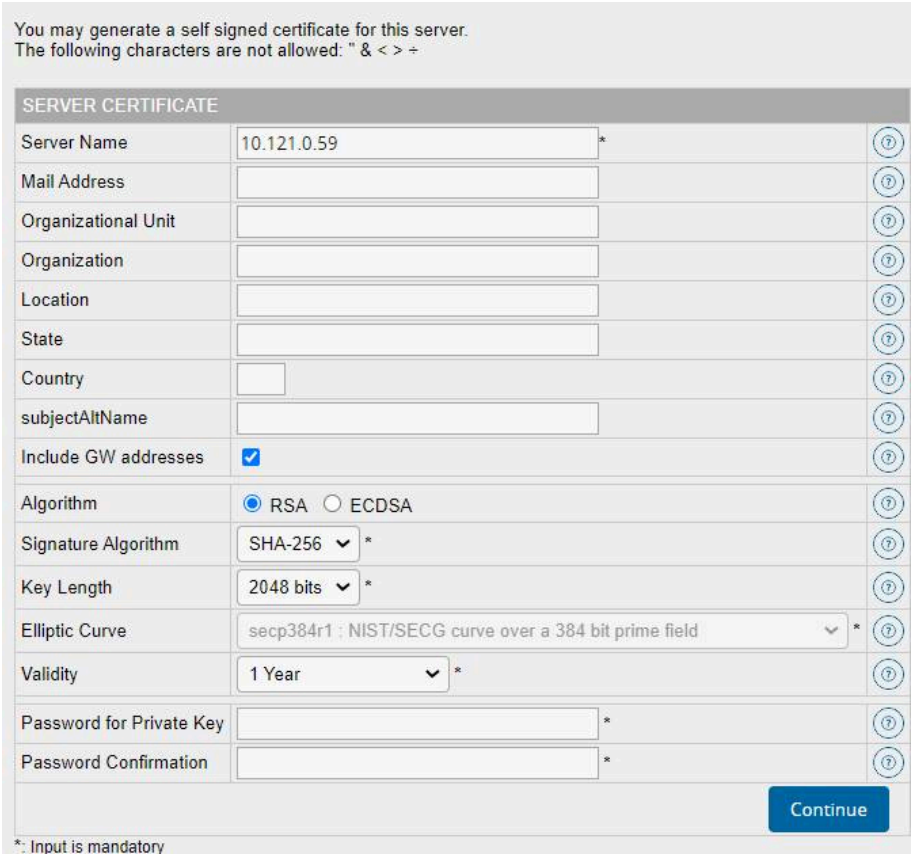
dialog. A notification in the dialog informs you that a self signed certificate has already been created and exists for this server.

If no self signed certificate exists for this server, the program goes directly to the **Generate Server Certificate (self signed)** dialog. Some fields contain pre-defined default values which you can accept.

NOTICE: Warning! If you create a new certificate although a self signed certificate already exists for this server, the existing certificate will be overwritten.

Click on **New Certificate** in the **Display Certificate** dialog.

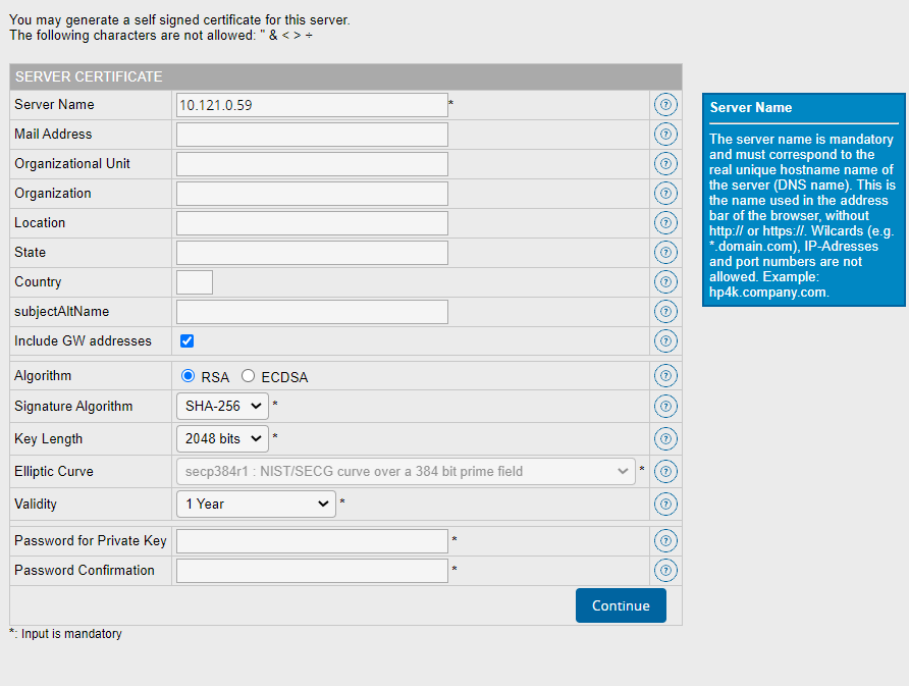
The **Generate Server Certificate (self signed)** dialog opens. Besides the entry fields it contains important additional notes regarding data entry. The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.



Mandatory fields are flagged with a red asterisk (*).

2) To get additional context information related to the individual entry fields, click on the "**?**" to the right of each entry field. The context-specific

information related to the respective field is displayed as a tooltip in the browser.



3) Enter all required data, and click on **Continue**.

   By entering a **Password** you are securing the private key of the certificate against fraudulent use.

   NOTICE: This password is not saved anywhere! Therefore, it has to be entered again when activating this certificate, even if this is done days or months later. Losing the password causes the private key and the certificate to be unusable.

   After creating a new certificate the program goes back to the **Activate Server Certificate** dialog. The newly created certificate is displayed and is already preselected (highlighted) as a rule. In the **Origin** column the entry **Generated** is displayed in this case.

4) To activate the newly generated certificate, select the radio button in the **Activate** colum - if the radio button is not selected already - and click on **Continue**.

   The detail data of the selected certificate are displayed in the **Activate Server Certificate** dialog, and you are prompted to enter the password for the private key of this certificate.

   Only signed certificates can be activated.

5) Enter the **password** and click on **Activate certificate**.

The certificate is activated and displayed as new **Currently active Certificate** in the **Activate Server Certificate** dialog.

The **Status** of certificates that can be activated is additionally indicated by a **color**. The colors have the following meaning:

red = signed certificate, active on server

green = signed certificate available, ready for activation.

NOTICE: The Web Server and OpenScape 4000 processes always need to be restarted after activating a new certificate. All currently running sessions, including your own session, will be terminated upon restart.

A warning message is displayed, alerting you that the Web Server needs to be restarted after activating a new certificate, and that all currently running sessions, including your own session, will be terminated on the server.

If you click on **OK** the selected certificate is activated and displayed as new **Currently active Certificate** in the browser.

Distributing a Certificate to All Available HG35xx Boards of a System

Provided that on this system there is at least one HG35xx board with an independently running Web Server installed, you have the option to distribute either the currently active certificate or a selected certificate to all available HG35xx boards. For more information please refer to the following links:

- Distributing the CURRENTLY ACTIVE Certificate To All Available HG35xx Boards

  and
- Activating and Distributing a SELECTED Certificate to All Available HG35xx boards and/or to Platform - Assistant only

Generate Server Certificate (self-signed) dialog, Field Descriptions

Server Name

Mail Address

Organizational Unit

Organization

Location

State

Country

Subject Alternative Name (subjectAltName)

Signature Algorithm

Key Length - for RSA only

Validity

Password for Private Key

Password Confirmation

Continue (Button)

Activate Server Certificate dialog, Field Descriptions

Activate (Link on Start Page of Access Management)

Currently Active Certificate (Table in Activate Server Certificate dialog)

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

Delete Certificate (Button in Certificate Information view, Display Certificate dialog)

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Distribute active certificate (Button beneath Currently Active Certificate table, Activate Server Certificate dialog**)**

Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

Activate (Radio Button in Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog**)**

Distribute the selected certificate to all available HG35xx boards as well (Checkbox beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Activate selected certificate (Button beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Activate certificate (Button, Activate Server Certificate dialog)

Back (Button, Activate Server Certificate dialog)

2.13.1.4 Import

This feature enables you to import a certificate and private key created on a different host. The supported file format is X.509 PEM and PKCS #12. After the import the Web Server needs to be configured for usage of this certificate and its associated private key. In order to decode the encoded private key you need to enter the password.

Importing a New Certificate

1) On the **Start Page** of **Access Management**, navigate to the **Manage Web Server Certificates -> Certificates for this Web Server** area.

2) Click or double-click on **Import**.

   The **Import Server Certificate and Key** is displayed. Importing a certificate and private key created on a different host is possible under the following conditions:

   - Supported file format: X. 509 PEM and PKCS #12. If the file extension is *.p12, it is treated as a PKCS #12 file. Otherwise, X.509 PEM format is used.
   - Private key and password for decoding are required and exist.

3) Click on **Browse** and select the appropriate file.

   Supported file format: X. 509 PEM and PKCS #12. If the file extension is *.p12, it is treated as a PKCS #12 file. Otherwise, X.509 PEM format is used.

4) Enter the **Password** for the private key.

5) Click on **Import**.

   The program goes back to the **Activate Server Certificate** dialog. The imported certificate is displayed and is already preselected (highlighted) as a rule. In the **Origin** column the entry **Imported** is displayed in this case. The imported certificate can now be activated.

   The **Status** of the selected certificate is additionally indicated by a **color**. The colors have the following meaning:

   red = signed certificate, active on server

   green = signed certificate available, ready for activation.

Field Descriptions

File with Key and Certificate (Entry Field)

Password for Private Key (Entry Field)

Import Certificate (Button)

2.13.1.5 Generate via CSR

The **Generate via CSR** feature is used to generate a Certificate Sign Request (CSR) for a new certificate. For testing purposes, the CSR is automatically transformed into a self signed certificate which you can test. After having tested the self signed certificate you can export the CSR and send it to a Certificate Authority (CA) for signing. As soon as you receive the signed certificate back from the CA, you can import and activate it.

Generating a New Certificate Sign Request (CSR)

1) On the **Start Page** of **Access Management**, navigate to the **Manage Web Server Certificates -> Certificates for this Web Server** area.
2) Click on **Generate via CSR** to generate a new certificate sign request (CSR).
3) Click on **Generate New Certificate Request**.

   a) If no CSR exists on the server, the **Generate Server Certificate (self signed)** dialog is displayed.
   b) If a CSR or a self signed certificate, respectively, already exists on this server, the **Generate Certificate via CSR** dialog is displayed. The data of the existing, currently active certificate are displayed in the entry fields and can be taken over for the new CSR.

   Mandatory fields are flagged with a red asterisk (*).

   The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.
4) To get additional context information related to the individual entry fields, click on the **"?"** icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.
5) Enter all required data, and click on **Continue**.

   By entering a **Password** you are securing the private key of the certificate against fraudulent use.

   NOTICE: This password is not saved anywhere! Therefore, it has to be entered again when activating this certificate, even if this is done days or months later. Losing the password causes the private key and the certificate to be unusable.

   When you click on "**?**", additional context information is displayed as a tooltip with each entry field.

   For testing purposes the CSR is automatically turned into a self signed certificate upon creation, so that you can test it afterwards.

Displaying the Newly Generated Certificate Sign Request (CSR)

1) The **Display Certificate** dialog opens. The data of the new CSR and the confirmation "Your certificate request has been generated and automatically self signed for testing." is displayed.
2) Click on **Continue**.

   The **Generate Certificate via CSR** dialog opens again. The generated certificate is displayed in the list and marked with BLUE color. The BLUE color indicates the status "CSR generated, not exported yet".

Testing the New Self Signed Certificate

1) To test the new, self signed certificate, click the **Test** icon in the **Action** column of the table displayed in the **Generate Certificate via CSR** dialog.

   After successful testing the **Activate Server Certificate** dialog is opened again. In the **Origin** column the text will read **Generated via CSR** in this case. The generated test certificate is displayed in the list and is already

selected and marked with GREEN color. This means the certificate is now self signed and can be activated.

The **Status** of the selected certificate is additionally indicated by a specific color. The **colors** have the following meaning:

red = signed certificate, active on server

green = signed certificate available, active, ready for activation

yellow = CSR exported, certificate not signed yet blue = CSR generated, not exported yet.

Depending on the curren status of a certificate the **Test**, **Export**, **Import**, **Activate** actions can be executed or not executed, respectively.

Exporting a New Certificate Request (CSR)

1) Once you have successfully tested the CSR, **export** it by clicking on the **Export** icon in the **Action** column.

The **Export Certificate Request (CSR)** dialog is opened. The content of the certificate (encrypted code) is displayed in the **EXPORT CSR** area.

Depending on the current status of a certificate can the action be executed or not executed, respectively (greyed out).

Copying the CSR with Copy&Paste or Exporting CSR To File

1) Copy the content of the CSR with Copy&Paste to a text file and save this file, or export the content of the CSR to a file by clicking on **Export CSR to File**.

NOTICE: If you use Copy&Paste please make sure to include the complete header (---BEGIN CERTIFICATE REQUEST ---) and footer (---END CERTIFICATE REQUEST ---) lines with the code that you are saving to a file. The server type used is "Apache + mod_ssl + OpenSSL".

Exporting the CSR To a File

1) If you click on the **Export CSR to File** button, the **File Download** dialog opens. Click on **Save** and **not** on **Open** in this dialog.
2) The file name **server.csr** is automatically entered as default value in the **File Name** field. You can accept this file name or change it to a name of your choice. Save the file to a folder of your choice.
3) Once the **Download finished** dialog is displayed, click on **Close** to terminate the process.
4) You can then send the exported CSR to your Certificate Authority for signing purposes.

The Export process can be repeated for each CSR for an unlimited number of times.

After successfully exporting a CSR, its Status is set to YELLOW in the **Generate Certificate via CSR** dialog. This means that the certificate has already been exported once. The **Status** of the displayed CSRs and/or

certificates is indicated by specific colors. The **colors** have the following meaning:

red = signed certificate, active on server

green = signed certificate available, active, ready for activation

yellow = CSR exported, certificate not signed yet

blue = CSR generated, not exported yet.

Importing a Signed Certificate

A certificate that belongs to a previously generated CSR with a corresponding private key, and that has been signed by an external Certificate Authority (CA), may be imported and displayed by entering the password for the private key.

1) **Import** the signed certificate once you have received it from the CA by clicking on the **Import** icon of the signed CSR in the **Action** column, **Generate Certificate via CSR** dialog.

   To import a certificate, you must previously have exported it.

   Similarly to Exporting a CSR, when **importing** a certificate you can either use Copy&Paste to copy the content of the signed certificate from a text file to the displayed area beneath **IMPORT SIGNED CERTIFICATE**, or import the certificate as a file by clicking on **Browse** and selecting the desired file name.

Entering the Password for the Private Key

1) Enter the **Password for private key** and click on **Continue**. After successful import the imported, signed certificate is displayed as certificate that can be activated in the **Generate Certificate via CSR** dialog.

   Depending on the curren status of a certificate the **Test**, **Export**, **Import**, **Activate** actions can be executed or not executed, respectively.

Displaying the Imported, Signed Certificate

1) After successful import the **Status** of the imported certificate is set to GREEN. GREEN means that the certificate has been imported and signed, and can be activated.

   The **Status** of the displayed CSRs and/or certificates is indicated by specific colors. The **colors** have the following meaning:

   red = signed certificate, active on server green = signed certificate available, active, ready for activation yellow = CSR exported, certificate not signed yet blue = CSR generated, not exported yet.

   To activate an imported certificate, please follow the steps described in the Activate - HG35xx Board NOT Installed section. Only signed certificates can be activated.

Field Descriptions

Server Name (Table Column)

CA Name (Table Column**)**

Validity (from / until) (Table Column**)**

Generated (Table Column)

Exported (Table Column)

Imported (Table Column)

Action (Table Column)

Test (Button)

Export (Button)

Import (Button)

Activate (Button)

Certificate Information

Delete Certificate (Button)

Server Name (Entry Field)

Mail Address

Organizational Unit

Organization

Location

State

Country

Signature Algorithm

Key Length - for RSA only

Validity

Password for Private Key

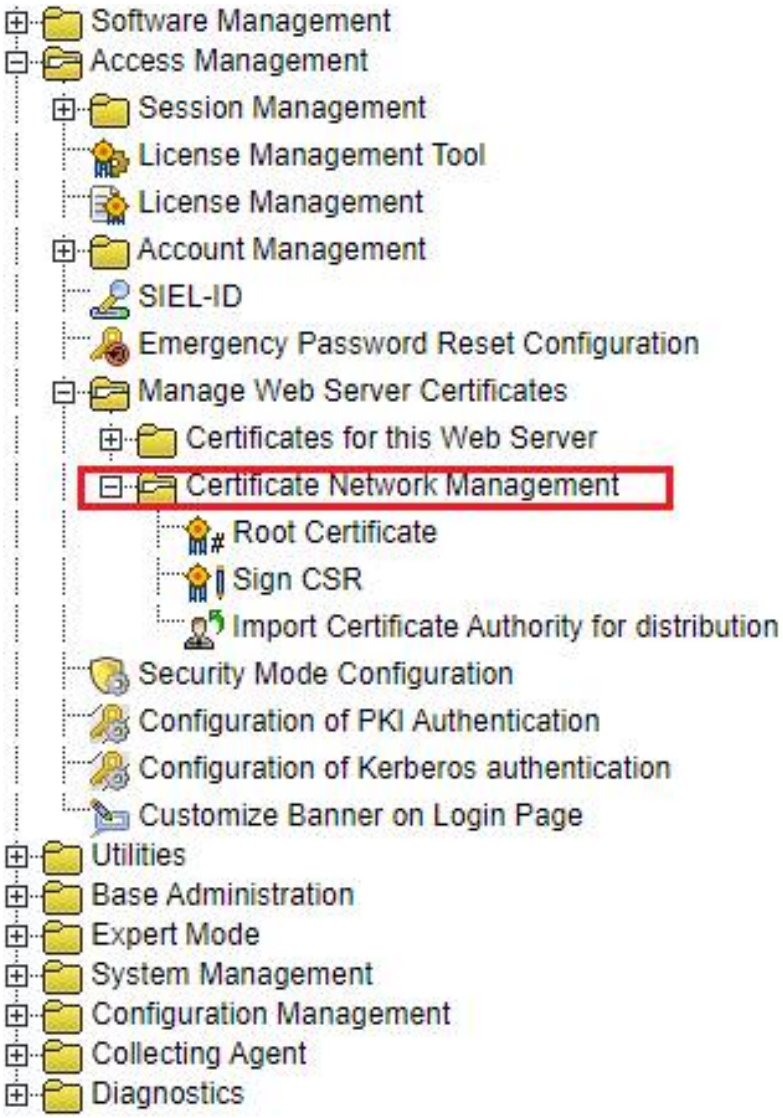
Password Confirmation

Continue (Button)

Back (Button)

2.13.2 Certificate Network Management

The **Certificate Network Management** area comprises the features for administering SSL security certificates within an OpenScape/HiPath 4000 network. These features are required for users having an OpenScape/HiPath 4000 network with a OpenScape 4000 Manager server administering one or more OpenScape/HiPath 4000 Assistant systems.



The following features are available:

Root Certificate

Sign CSR

Import of Certificate Authority (CA) for distribution to clients

2.13.2.1 Root Certificate

This feature allows you to create your own Root Certificate which you can then use to sign all external Certificate Signing Requests (CSRs) for all systems within an OpenScape/HiPath 4000 network.

The aim of this feature is to have all SSL security certificates for all systems within an OpenScape/HiPath 4000 network signed and certified by just one Certificate Authority (CA).

Only the Root CA needs to be imported into the individual browsers, not the certificate itself.

A Root Certificate is a special type of self signed certificate. The difference between self signed certificate and root certificate is that with self signed certificates you need to specify the server name, whereas in the case of the root certificate you need to specify a name for the Certificate Authority (CA). The name of the root certificate does not refer to a specific server.

Open the Root Certificate dialog

- Navigate to **Start Page -> Access Management -> Certificate Network Management**.

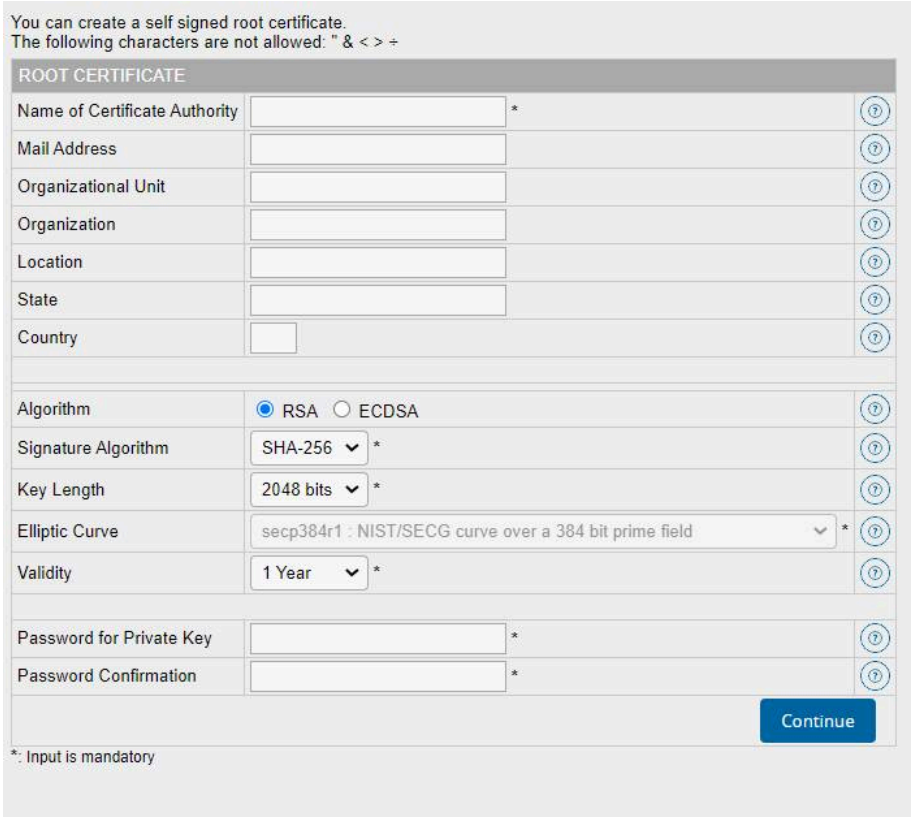
  The **Root Certificate** dialog opens.

  – **Root Certificate Does Not Exist Yet**

  If no Root Certificate has been created for this server yet, the empty **Root Certificate** dialog will open.

  – **Root Certificate Already Exists**

  If a self signed Root Certificate has already been created for this server, the data of the existing certificate will be displayed together with a corresponding note in the **Root Certificate** dialog in the browser.



Signing, Downloading, Creating Root Certificates

WARNING: If you create a new root certificate although a self signed root certificate already exists for this server, the existing root certificate will be overwritten.

1) If you want to use the existing root certificate for signing CSRs, click the Sign CSR. link.

   You can use this root certificate to sign external CSRs.
2) You may download the root certificate and import it to the Trusted Root CA store of the client browser and to the Java Runtime Environment by clicking **Root Certificate (link)** in this dialog.
3) If you want to create a new root certificate and overwrite the existing root certificate, click on New Root Certificate (Button).

Creating a New Root Certificate

After clicking the **New Root Certificate** button in the **Root Certificate** dialog the **Generate Root Certificate** dialog opens.

The data of the existing root certificate - if one exists - are displayed in the entry fields and can be taken over for the new root certificate.

1) Enter all required data.

   Mandatory fields are flagged with a red asterisk (*).

   The following characters are not allowed in the entry fields: **" & < > ÷** as well as accented and special characters.
2) To get additional context information related to the individual entry fields, click on the "**?**" icon to the right of each entry field. The context-specific information related to the respective field is displayed as a tooltip in the browser.
3) Click on **Continue**.

Displaying the Newly Created Root Certificate

The data of the newly created root certificate are displayed together with the following message:

"The certificate has been created as displayed below. With this Root Certificate you can now sign externally generated certificate requests."
Click on Sign CSR in order to sign external CSRs with the newly created root certificate.

Field Descriptions

Root Certificate (link)

New Root Certificate (Button)

Name of Certificate Authority (entry field)

Mail Address

Organizational Unit

Organization

Location

State

Country

Signature Algorithm

Key Length - for RSA only

Validity

Password for Private Key

Password Confirmation

Continue (Button)

2.13.2.2 Sign CSR

This feature allows you to sign all external Certificate Signing Requests (CSRs) for all systems within an OpenScape/HiPath 4000 network.

The prerequisite is that you have previously created a self signed Root Certificate of your own.

The aim of this feature is to have all Certificate Signing Requests (CSRs) for all systems within an OpenScape/HiPath 4000 network signed and certified by just one local Certificate Authority (CA) using a self signed root certificate of your own.

1) Navigate to **Start Page -> Access Management -> Sign CSR**.

   The **Sign Certificate Request (CSR)** dialog opens.
   Root Certificate Does Not Exist Yet

   If no Root Certificate has been created for this server yet, the following error message will be displayed on the empty screen:

   Error : No Root Certificate has been created, so that the Certificate Requests can be signed. Please create a Root Certificate first.

   Create a new Root Certificate as described in the Signing, Downloading, Creating Root Certificates section, and continue with Step 2 or 3 on page 152.

Importing CSR with Copy&Paste

1) **Open** the Certificate Signing Request (CSR).

   You can either use Copy&Paste to copy the content of the signed certificate from a text file to the **Paste Certificate Request** dialog area, or import the certificate from a file by clicking on **Browse** and selecting the <filename.csr> file name.

   NOTICE: Important: Only BASE64 encoded PKCS#10 requests are accepted. Please make sure to also copy the delimiter lines (BEGIN and END)!

Importing CSR From File

1) Click on **Browse** to open the **File Download** dialog. Select the desired path and file name (e.g. server.csr), and click on **Save**, **not** on **Open**.

Entering Password for Private Key of Root Certificate

1) In the **Sign Certificate Request (CSR)** dialog, enter the **Password for the Private Key** of the root certificate, and click on **Sign Certificate Request**.
2) The program goes back to the **Display Certificate** dialog, and displays the **Certificate Information** data. Click on **Continue**.
3) **Sign Certificate Request (CSR)** dialog opens. The content of the signed certificate (encrypted code) is displayed in the **Export Signed Certificate**

dialog area. The following message is displayed: "The signed certificate is displayed. You may now import this certificate into your external web server."

4) Click on **Export signed certificate into file** or copy the content of the certificate with Copy&Paste into a text file, and save this file.

NOTICE: If you use Copy&Paste please make sure to include the complete header (---BEGIN CERTIFICATE REQUEST ---) and footer (---END CERTIFICATE REQUEST ---) lines with the code that you are saving to a file. The server type used is "Apache + mod_ssl + OpenSSL".

---

5) If you click on **Export signed certificate into file**, the **File Download** dialog opens. Click on **Save**, and **not** on **Open**.
6) The file name **server.crt** is automatically entered as default value in the **File Name** field. You can accept this file name or change it to a name of your choice. Save the file to a folder of your choice.
7) Once the **Download finished** dialog is displayed, click on **Close** to terminate the process.
8) In the **Sign Certificate Request (CSR)** dialog, click on **Continue**. The program goes back to the initial **Sign Certificate Request (CSR)** dialog, and you can select the next CSR to be signed, or end the process.
9) You may now import the signed, exported CSR into your web server.

Field Descriptions

Sign CSR

Sign Certificate Request (CSR) (Dialog)

Paste Certificate Request

Or Import Certificate Request from File

Browse (Button)

Password for Private Key of Root Certificate

Sign Certificate Request (Button)

Export signed Certificate into File (Button)

Continue (Button)

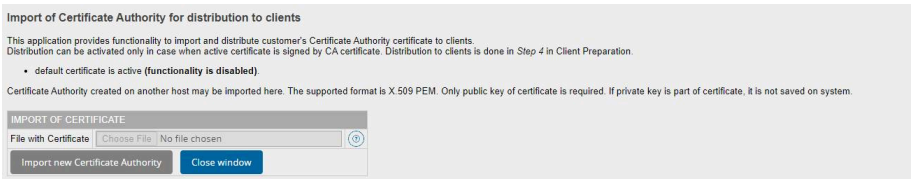
2.13.2.3 Import of Certificate Authority (CA) for distribution to clients

This application allows you to import and distribute the customer's Certificate Authority (CA) certificate to clients. The distribution can only be activated if the certificate active on this Web Sever is signed by a CA certificate. The application is disabled if a predefined or selfsigned certificate is active on the Web Server.

The distribution of an imported CA certificate to clients is done in Step 4 of Client Preparation. Only the public key of a CA certificate is stored on the system and provided for distribution.

Configuration:

1) Navigate to **Start Page -> Access Management -> Manage Web Server Certificates -> Certificate Network Management -> Import ort Certificate Authority for distribution**



2) Import the public key of the CA certificate you want to distribute to clients.
3) Enable the distribution by activating the checkbox and submit the change.
4) Go to Client Preparation and make sure that the certificate is provided for distribution.

A Certificate Authority created on another host may be imported here. The supported format is X.509 PEM. Only the public key of the certificate is required.

2.14 Security Mode Configuration

Start the application

Application is accessible only for administrator. The **Configuration** page for configuring security mode is accessible from the start page:

Security Mode Configuration

> **NOTICE:** The settings may differ on OpenScape 4000 Assistant and Manager.

Functionalities

The **Configuration** page for security mode settings is grouped in major sections to control:

Application access

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.14.1 Application access

Overview

In this section of the Security Mode Configuration page you can control access:

- Checkbox **Restricted access to Platform Portal**
  - Access can be restricted for all connections to Platform Portal (protocol https, port: 443) and ssh (port: 22)
  - Application access must be possible on the HHS as well as on AP-E. AP-E security configuration will be automatically overwritten by the HHS settings during the APE restore.
  - DUPLEX scenario: each Platform (including Quorum node for separated Duplex) will be automatically informed / restricted.
- Checkbox **Maintenance Mode**: Enable ssh and web access from Assistant and access from DLS.
  - Access can be granted for ssh and web access (to Platform Portal) for connections from Assistant
  - This is the new default starting with V11 R1. During Update to V11 R1 (or newer) from V11 R0 (or older) the Maintenance Mode will be activated automatically if “Restricted access” was not enabled before.

    NOTICE: If unrestricted access to the Platform Portal is required, it must be re-enabled after each RLC update.
- Checkbox **Restricted access of Comwin to ADP**
  - Access via ComWin to ADP is blocked.
  - ComWin will display a failure dialog ("Connection Refused" message) if the access is restricted.
- Checkbox **Restricted access to system shell from customer network**

  All connections to system shell from customer network are blocked
- Checkbox **Restrict SSH access to system and HG3550M from "SSH connection to Assistant" and "Gateway Dashboard" applications**
  - OpenScape 4000 provides a web based SSH terminal for access to the system and to HG3550M gateways with a single click.
  - Direct SSH access to the boards e.g. via Putty is still possible unless the Gateway Secure Mode is activated.
  - Web based SSH terminal to the system is accessible via *"Expert Mode --> SSH connection to Manager/Assistant*" application.

    NOTICE: When the checkbox is selected, the access over the web terminal is disabled.
  - Web based SSH terminal to HG3550M gateways is accessible via *"Gateway Dashboard*" application.

    NOTICE: When the checkbox is selected, the access over the web terminal is disabled.

- Checkbox **Restricted access to Security Management API from customer network**
  - Connection via Security Management API (secm.dll, secmcj.jar) is blocked
  - Should be only used to harden the standalone systems (not connected to Manager)
  - Remote communication between Assistant and Manager is blocked
    - collecting CDR data (COL)
    - remote login (Single Sign ON) to GUI / applications
    - batch jobs execution
    - remote connection to RMX / dipas batch
    - etc...

Manager only:

- Checkbox **Support legacy HiPath 4000 systems (enable port 102)**
  - Required for backward compatibility to older HiPath 4000 systems.
  - The default value is "switched off" (secured).

Enable/Disable Application Access

To enable/disable application access:

- Uncheck or check the corresponding checkbox.
- Click **Save changes**.

The following table shows the impact of "Restricted access to Security Management API from customer network" checkbox to features related with remote connection between Manager and Assistant. As you can see, this feature depends solely on the Assistant's setting. If restriction checkbox is checked there, this error is displayed when using Direct Access buttons in System Management:

"Error: Automatic logon at target server into account ERROR_FATAL_ERROR:cookie=non%20valid via NSL level

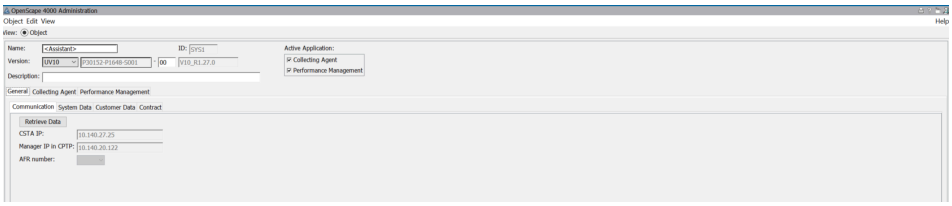
ERROR_FATAL_ERROR:cookie=non%20valid failed."

Table 1: System Management Direct Access overview

Restricted access to Security Management API from customer network Mgr. V6R2 & V7 and newer	Restricted access to Security Management API from customer network Assi. V6R2 & V7 and newer	Remote connection from the Mgr. to the Assi.
		OK
	x	Not OK
x		OK
x	x	Not OK

The Direct Access feature is affected by NSL accounts configuration. NSL accounts must be unlocked and passwords properly set. NSL accounts' password change is mandatory and affects both the Manager and the cooperating Assistant (see also OpenScape 4000 Assistant Security Checklist).

Direct Access GUI in System Management



The following table shows the impact of "SSL for Comwin" checkbox in combination with "Restricted access of Comwin to ADP" checkbox in Assistant V6 R2 & V7 to the Comwin (Expert Access) encryption. Expert Access through Manager consists of the connection from Desktop application to the Manager and second connection from the Manager to the Assistant. Both are listed in this table for all supported Assistant versions. The control connections, which go over ports 7777 or 7778 are always plain text. The payload (AMO commands and their output) is mpcid based connection and follows the same principles as described before.

Table 2: Comwin encryption overview

SSL for Comwin Manager V6R2 & V7	Expert Access client <-> Mgr. control connection encryption	Expert Access client <-> Mgr. control payload encryption	Restricted access of Comwin to ADP Assi. V6R2 & V7	mpcid based connection to Assi. V6R2 & V7	mpcid based connection to Assi. V5 & V6R1
	plain text	plain text		SSL	Proprietary
			x	SSL	
x	plain text	SSL		SSL	
			x	SSL	

See also

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.14.2 Remote Database Connectivity

In this section of the **Security Mode Configuration** page you can enable/disable the not encrypted remote ODBC/JDBC access to the system. Web server and OpenScape 4000 daemons will be restarted during change in this configuration.

Enable/Disable Database Connectivity

To enable/disable unencrypted database access:

- Uncheck or check the corresponding checkbox for the desired database type.
- Click **Save changes**.

See also

Application access

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.14.3 Authentication Mode

In this section of the **Security Mode Configuration** page you can control PKI authentication and Kerberos authentication of the system.

Detailed configuration of PKI authentication is done in Configuration of PKI Authentication.

Enable/Disable PKI Authentication Mode

To enable/disable PKI Authentication:

- Select one of the authentication modes:
  - **Only password authentication**
  - **Only PKI authentication**
  - **Password and PKI authentication**
- Click **Save changes**.

WARNING: Enable both authentication modes during system setup to prevent problems with authentication. Access to system can be blocked when configuration is not done properly and only PKI authentication is enabled.

Enable Kerberos Authentication

To enable the Kerberos Authentication:

- Select the respective checkbox
- Click **Save changes**.

For more details regarding Kerberos Authentication, please see Chapter 2.16, "Single Sign On".

See also

Application access

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.14.4 Gateway Security

In this section of the **Security Mode Configuration** page you can control the switching of all gateways to secure mode.

Selection of the Enable Gateway Secure Mode checkbox disables HTTPS, SSH and DLS access for IP Gateways.

- If the IP gateways are to avoid clear text protocols, the Signaling Payload Encryption (SPE) feature needs to be configured additionally.
- For Standalone Simplex SoftGate and Survivable SoftGate, "Restricted access to Platform Portal" also needs to be activated under "Application Access" entry.

To enable/disable Gateway Secure Mode:

- Uncheck or check the **Enable** Gateway Secure Mode checkbox.
- Click **Save changes**.

See also

Application access

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.14.5 TLS Protocol Selection

In this section of the **Security Mode Configuration** page you can select the protocol for the HTTPS communication with the web server.

The default configuration of the web server in V10 enables communication in TLSv1.3 with fallback to TLSv1.2

Assistant only:

The same configuration of TLS protocols is automatically set on the platform and CSTA. If the configuration is changed, the platform and CSTA are automatically reconfigured with the same configuration as used by the Assistant.

Available protocols:

- In Openscape 4000 V10, TLSv1.0 is not offered anymore. The only option available in Assistant will be TLSv1.3 with fallback to TLSv1.2

The web server and OpenScape 4000 daemons will be restarted during any change in this configuration.

See also

Application access

Remote Database Connectivity

Authentication Mode

Gateway Security

TLS Protocol Selection

2.15 Configuration of PKI Authentication

Overview

Configuration of PKI Authentication is the central application for configuration of PKI authentication and validation method.

Start the application

The **Configuration** page for configuring PKI Authentication is accessible from the start page:

Account Management -> Configuration of PKI Authentication

The following actions can be configured in the **Configuration of PKI Authentication**:

- Import of Trust Anchor (Root CA) certificate
- Import/Delete of Intermediate CA certificates
- Display description of all imported certificates
- Download all imported certificates
- Switch between CRL and OCSP certificate revocation management. Only one scenario is active at the time.

Revocation mode based on Certificate Revocation List (CRL) is always active. Revocation mode based on Online Certificate Status Protocol (OCSP) can be additionally enabled.

The validity of all imported certificates is checked. When certificate is going to expire, administrator is informed about this expiration and an alarm message is created.

Functionalities

The **Configuration** page for PKI settings is grouped in major sections for customizing:

Certificate Validation

OCSP - Online Certificate Status Protocol Management

Certificate Revocation List Management

Test of Connection with Current PKI Certificates

2.15.1 Certificate Validation

Certificates used for TLS sessions must be properly validated. The contents of the certificates as well as the certificates themselves must be checked for revocation status. A revocation status check involves one or both of the following mechanisms:

- Verification of the certificate revocation status from a downloaded Certificate Revocation List (CRL).
- Verification of the certificate revocation status with an OCSP responder.

OpenScape 4000 provides both mechanisms for certificate validation. The mechanism for certificate validation can be chosen in the **Configuration of Certificate Revocation Mode** section and only one scenario can be activated by one of the radio buttons:

- **Certificate Revocation List (CRL)**or
- **Online Certificate Status Protocol (OCSP)**When scenario with OCSP Responder is selected, the certificate is automatically checked with CRL as well.

Communication with OCSP Responder is handled via OpenSSL API/CLI.

The OpenSSL interface for CRL is part of web server (Apache, mod_ssl). mod_ssl contains required configuration for CRL, however it does not support the automatic download of said CRL. Download of actual CRL will be done via periodic job. Configuration of frequency for download of actual CRL is done in section **Configuration of Certificate Revocation List (CRL)**; see Certificate Revocation List Management.

See also

Configuration of PKI Authentication

OCSP - Online Certificate Status Protocol Management

Certificate Revocation List Management

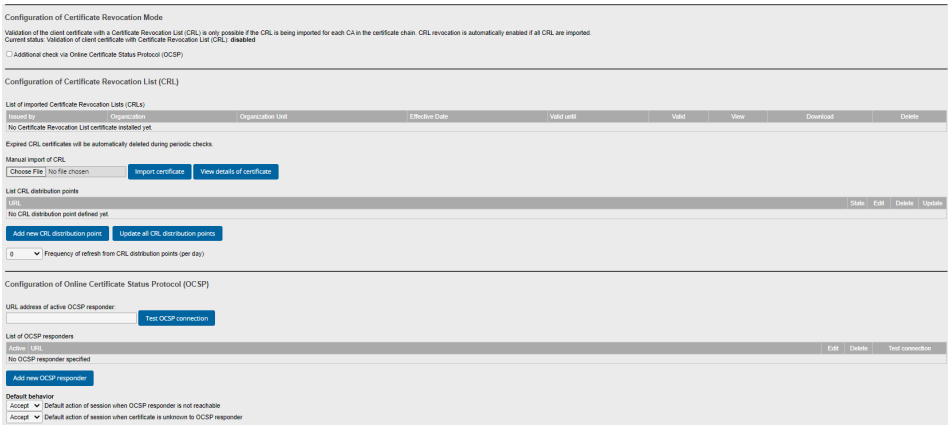
Test of Connection with Current PKI Certificates

2.15.2 OCSP - Online Certificate Status Protocol Management

The Configuration of PKI Authentication Application is responsible for configuration of an OCSP Responder. OCSP Responder is to be contacted in order to check the revocation status of the client certificate.

OCSP Responder is contacted on base of the following information:

- The preconfigured address of the OCSP Responder
- (optional) The OCSP Responder location identified in the OCSP field of the AIA (Au-thority Information Access) extension of the certificate



If both of the above are available: The OpenScape 4000 is configurable to provide preference for one over the other.

In OCSP Management's part of Configuration of PKI Authentication can be configured:

- Configuration of IP address or FQDN of OCSP Responder
- IP address or FQDN of OCSP Responder is identified from OCSP field of the AIA in Root CA certificate (if present)
- Preferred OCSP Responder server
- Default action for session establishing when OCSP Responder does not respond (Accept/Reject session request)
- Default action for session establishing when client certificate is unknown to OCSP Responder

During the establishment of a SSL/TLS connection, the OpenScape 4000 system validates the client Certificate by sending verification to online OCSP responder. If the OCSP Responder does not respond in a specified time, the SSL/TLS session is accepted or rejected based on configuration

The following alarms/logging messages shall be generated:

- OCSP Responder could not be contacted because of network issues.
- OCSP request is not finished in time.
- OCSP respond format is invalid.

See also

Certificate Validation

Certificate Revocation List Management

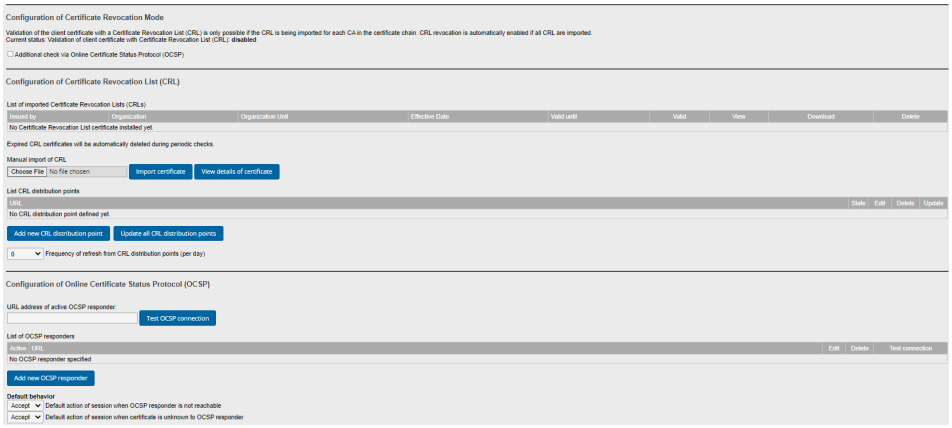
Configuration of PKI Authentication

Test of Connection with Current PKI Certificates

2.15.3 Certificate Revocation List Management

The Configuration of PKI Authentication Application is responsible for the certificate revocation lists (CRLs) configuration. It downloads the lists upon request and shall keep the lists up-to-date.

The Configuration of PKI Authentication accepts only CRL download requests for certificates whose certificate's chain lead to a specific (configured) Root CA.



The following is presented in the **Configuration of Certificate Revocation List (CRL)** section:

- List of imported/downloaded CRL
- Manual import CRL certificates
- View/delete CRL certificates
- Configuration of IP address or FQDN of CRL servers
- IP address or FQDN of CRL server identified from installed certificates (if presented)
- **CRL Download frequence of CRL**: Drop-down list for maximum count of automatic CRL downloads per day. If this interval is set to 0, no automatic CRL downloads is done.
- Button **Download actual CRL** to download current version of CRLs.

Each time a CRL is downloaded for which the 'CRL Number' is different from the 'CRL Num-ber' in the previous CRL, all Security Management sessions are checked about the potential change in revocation status.

See also

Configuration of PKI Authentication

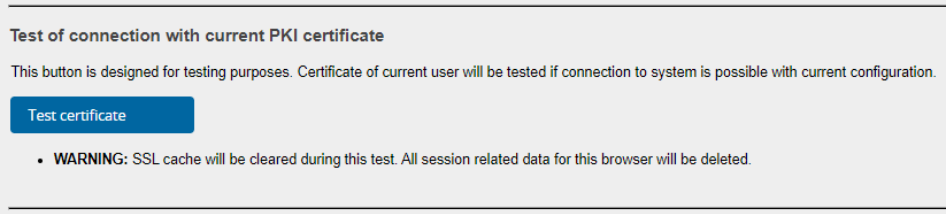
OCSP - Online Certificate Status Protocol Management

Certificate Validation

Test of Connection with Current PKI Certificates

2.15.4 Test of Connection with Current PKI Certificates

Clicking the button **Test certificate** the certificate of the currently active user can be tested, provided that a connection to the system is possible with the current configuration.



WARNING: Th SSL cache will be cleared and all session related data for this browser will be deleted during the test!

See also

Configuration of PKI Authentication

OCSP - Online Certificate Status Protocol Management

Certificate Validation

Certificate Revocation List Management

2.16 Single Sign On

Introduction

OpenScape 4000 Manager or Assistant supports a "Single Sign On" with Active Directory. This feature provides authenticated domain users with seamless sign on at OpenScape 4000 Manager or Assistant by just a single click. It is based on Kerberos credentials (authentication token), which that are automatically provided by client web browser.

Authentication is possible for a Kerberos account that is assigned to an existing OpenScape 4000 user account in Access Management - User Account Administration.

Schema of authentication

Figure 3: Schema of Kerberos authentication

Step 0: Periodic retrieval of Kerberos Ticket-Granting Ticket (TGT)

Step 1: User logs on to the domain on client PC.

Step 2: The Kerberos Key Distribution Center (KDC) verifies user credentials, authenticates the user and sends a Ticket-Granting Ticket to the client PC.

Step 3: User connects to OpenScape 4000 system and uses Kerberos authentication option. Kerberos credentials (Service Ticket) are automatically provided by browser.

Step 4: If Kerberos credentials are OK and user's domain account is assigned to an OpenScape 4000 user account, OpenScape 4000 system authenticates user and provides a session cookie.

NOTICE: Steps 0, 3 and 4 require configuration of OpenScape 4000 system and the Domain Controller.

2.16.1 Requirements

- OpenScape 4000 Assistant/Manager - V8 and newer
- Client PC with Windows assigned to domain
- Server OS with Domain Controller (DC) with Active Directory (AD), Kerberos Server (KDC) and DNS server functionality

List of Supported Client OS

- Windows XP and newer client OS

NOTICE: Alternatively, Windows server OS can be used as client as well.

List of Supported Server OS

All servers with Windows based server system are supported:

- Windows 2000 Server
- Windows 2003 Server
- Windows 2008 Server
- Windows 2012 Server

2.16.2 OpenScape 4000 Configuration

Global Kerberos configuration for SLES on OpenScape 4000 system is not affected. For authentication on OpenScape 4000, a dedicated set of configuration files is used.

2.16.2.1 Enabling of Kerberos authentication

Application for Kerberos configuration is accessible via the Access Management folder (Figure 3).

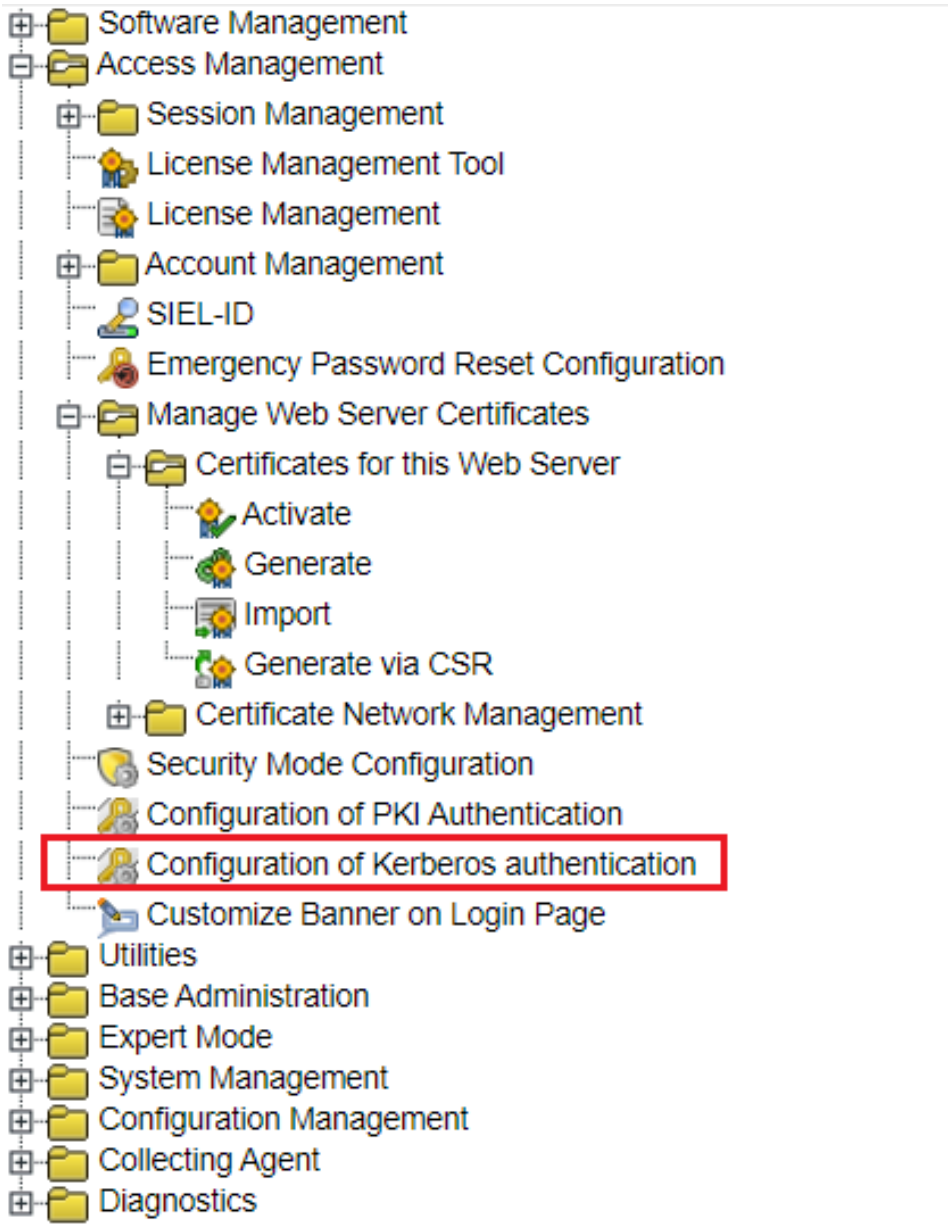


Figure 4: Access to the Configuration of Kerberos Authentication

Kerberos authentication is **disabled by default** after the installation of OpenScape 4000 (see the notification on Figure 4). Therefore, you have to enable it first. Click the Security Mode Configuration link in the notification to access the Security Mode Configuration application.

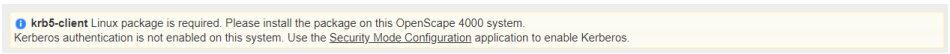


Figure 5: Default Kerberos authentication notification

In the Security Mode Configuration application, search for the Authentication Mode section, where you select the "Enable Kerberos Authentication" checkbox (Figure 5). Press the "**Save changes**" button to store the settings.

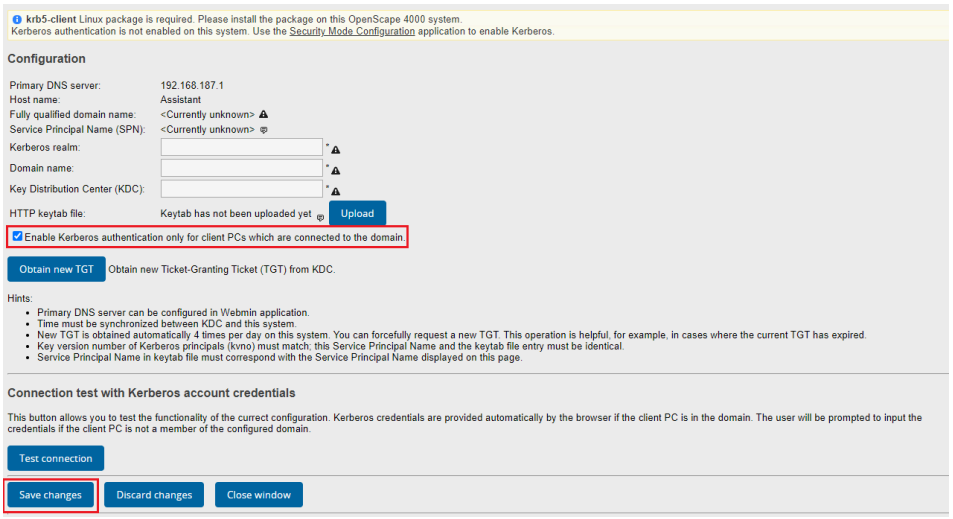


Figure 6: "Enable Kerberos Authentication" checkbox

2.16.2.2 Configuration of Kerberos authentication

Prerequisites

Installation of **krb5-client** Linux package on SLES. This package is pre-installed on Assistant automatically. On Manager, it has to be installed manually. The user is notified to do so (Figure 6).

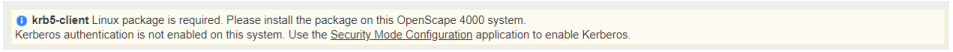


Figure 7: krb-5 client package installation notification

Further, **Kerberos authentication** must be **enabled** in the Security Mode Configuration application (see Chapter 2.16.2.1, "Enabling of Kerberos authentication").

Configuration items

Following items has to be configure:

- **Primary DNS Server** can be configured in Webmin application. Recommended value is a DNS server which is running on Windows domain controller.
- **Hostname** of the current system can be configured in Webmin application.
- **Fully qualified domain name (FQDN)** consists of a host name and a domain name. Since domain name must be configured, the complete FQDN is unknown after installation.
- **Service Principal Name (SPN)** is an identifier for a service offered by a particular host within an authentication domain. The common value is: *<service>/<FQDN>@<REALM>* (for example: HTTP/mgr-V8.os4k-kerb.com@OS4K-KERB.COM).

  SPN must be registered in the REALM's Key Distribution Center (KDC). The service principal name is calculated as soon as the required parameters are configured.

- **Kerberos Realm**. In the Windows environment, the Kerberos realm is equivalent to a Windows Domain written in capital letters, for example: OS4K-KERB.COM.
- **Domain name** of the Windows Domain, for example os4k-kerb.com.
- **Key Distribution Center (KDC)** is a service running on every domain controller that provides authentication services for clients, as well as for the servers and services.

  The value is: *dc.<name of domain controller>* (for example dc.os4k-kerb.com).
- **HTTP keytab file** contains the shared secret key of the SPN. This file is created on domain controller via the ktpass tool. The keytab file must be transferred from the domain controller and uploaded to OpenScape 4000 (see Service account for OpenScape 4000 system on page 179).
- **Enable Kerberos authentication only from client PCs which are connected to the domain** checkbox: when selected, Basic Authentication is disabled (see Chapter 2.16.5, "Authentication scenario").

  Note: Basic Authentication (displaying a dialog window with input for domain's username and password) takes place, if the client PC is NOT connected to the domain.

  If the client PC is connected to the domain, user's Kerberos credentials are automatically provided by browser during the authentication attempt (Negotiate authentication).
- **Obtain new TGT** (Ticket-Granting Ticket) button downloads immediately the actual version of the Ticket to OpenScape 4000. Use this function after the Kerberos configuration is finished.

Any change of Kerberos Realm, Domain Name, KDC or the keytab file requires restart of the web server in order to apply the change. The user can do it by clicking the "Restart Web Server" button which is displayed in case the restart is needed.

Configuration test

Use the **Test connection** button to check whether the configuration is set properly. A pop-up window with name of Kerberos account of current user is displayed if the configuration is correct.

2.16.2.3 Assignment of Kerberos account to OpenScape 4000 account

List of OpenScape 4000 user accounts is available in **User Account Administration** application. You can assign the Kerberos account to any OpenScape 4000 user account. This is possible either during account creation, options marked with solid line) or later via right configuration panel of User Account Administration window, options marked with dashed line).

One Kerberos account can be assigned to only one OpenScape 4000 account.

NOTICE: Assigning of Kerberos account to OpenScape 4000 **system accounts** is **NOT** possible.

The general format of a Kerberos account is: *<username>@<REALM>*

2.16.3 Active Directory Domain Controller and Kerberos Key Distribution Center configuration

Domain controller is running on Window Server based operating system.

DNS Server

1) Open "DNS Manager".
2) Add a record of OpenScape 4000 into DNS:

   DNS -->Forward Lookup zones --> Your zone --> New host with OpenScape 4000 record. Check "Create associated pointer record."
3) Check if the reverse record of OpenScape 4000 system is created:

   DNS --> Reverse Lookup zones --> Your zone --> PTR with OpenScape 4000 record

Service account for OpenScape 4000 system

One service account is required for each OpenScape 4000 system.

1) Open "Active Directory Users and Computers".
2) Create a service account in the domain (<USERNAME>). This account will be used for mapping of Service Principal Name (SPN) to domain account. After the account is created and you run the ktpass in the next step - a new tab named "Delegation" will appear in the User Properties.
3) Generate the keytab file with the configuration of SPN for OpenScape 4000 system and with shared secret key of SPN. The keytab file needs to be created in CMD on a server in the domain. The <USERNAME> should be the service account you created in the previous step.

   The ktpass command-line tool allows non-Windows services supporting Kerberos authentication to use the interoperability features provided by the Kerberos Key Distribution Center (KDC) in the Windows server.

   General format:

```
ktpass -princ <SPN> -mapuser <USERNAME>@<REALM> -crypto
 all -
ptype KRB5_NT_PRINCIPAL -pass <PASSWORD> -out
 http.keytab
```

   An example:

```
ktpass princ HTTP/mgr-V8.os4k-kerb.com@OS4K-KERB.COM -
mapuser
<USERNAME>@OS4K-KERB.COM -crypto all -ptype
 KRB5_NT_PRINCIPAL
-pass <PASSWORD> -out http.keytab
```

> **NOTICE:** The user will store a key version number (kvno). In case that the keytab is recreated, the new keytab must be uploaded to OpenScape 4000 system. Kvno stored in keytab must be the same as kvno obtained in OpenScape 4000.

Hints:

- Mapped SPN to service account can be listed with:

```
setspn <USERNAME>
```

```
setspn - reads, modifies and deletes the SPN directory
 property for an Active Directory (AD) service account.
```

- Maps SPN and AD service account:

  ```
  setspn -A <SPN> <USERNAME>
  ```

  For example:

  ```
  setspn -A HTTP/mgr-V8.os4k-kerb.com@OS4K-KERB.COM
   <USERNAME>
  ```

- In case that the same record existed from before, for example for different service account, you will get a duplicate message. Delete mapping with:

  ```
  setspn -D <SPN> <OLD_USERNAME>
  ```

2.16.4 Client configuration

OS configuration

The preferred way of authentication with Kerberos is an access from the client PC with following options:

- Client PC is connected to domain
- Client PC is configured to use DNS server running on domain controller

Browser configuration

Please check that the following requirements are fulfilled:

- "**Windows Integrated Authentication**" option is enabled in Browser --> Internet Options --> Advanced.
- OpenScape 4000 system is accessed **via hostname** (for example: mgr-v8) or **FQDN** (for example: mgr-v8.os4k-kerb.com) in browser. Hostname of OpenScape 4000 system is defined in Webmin application. Appropriate DNS record has to be configured in DNS server.
- Make sure that OpenScape 4000 system is accessed **via Local intranet zone** in browser. The list of intranet systems can be configured in Browser --> Internet Options --> Security. Usually, they are predefined by the administrator.

2.16.5 Authentication scenario

Login page of OpenScape 4000 system is extended with Single Sign On "Login" button. Authentication token which identifies the domain user, is automatically provided by browser to OpenScape 4000 system if the client PC is connected to domain (**Negotiate authentication**).

If the client PC is NOT connected to domain, the **Basic authentication** window is displayed. User must enter his credentials (domain username and password) to continue with Kerberos login.

NOTICE: Basic authentication with Kerberos can be **disabled** on the Configuration page (see Chapter 2.16.2.2, "Configuration of Kerberos authentication").

User is informed about the result of authentication and is automatically redirected to the main page of the OpenScape 4000 system.

NOTICE: If password change is required, the user will be notified with the following message: "*Your password expired. Please login to the system with the username/password and change your password.*"

2.17 Access Management tab sheet in System Management

The **Access Management** tab sheet in **System Management** is used to set or change the **security level passwords for network single logon (NSL)** to subordinated OpenScape 4000 servers. To make use of the NSL feature, the passwords entered here must match the passwords as set on the given target system. See **System Account Administration** on the selected system.

On OpenScape 4000 Manager and RSP (Remote Service Platform), an **Access Management** tab sheet is offered as a plug-in in the **System Management** application.

This additional **Access Management** tab sheet is only displayed in **System Management** if the user selects a OpenScape 4000 server as system type and if the **Access Management** application checkbox is checked in the **Active Application** area in **System Management**.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

Changes made in the **Access Management** tab sheet in the **System Management** application are saved in **System Management**..

The right of a user to define and/or change NSL passwords depends on the user account level and on the access rights associated with this user level.

Related Topics

Access Management tab sheet in System Management, User Interface

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.17.1 Access Management tab sheet in System Management, User Interface

The **Access Management** tab sheet in **System Management** is used to set or change the security level passwords for network single logon (NSL) to subordinated OpenScape 4000 servers. To make use of the NSL feature, the passwords entered here must match the passwords as set on the given target system. See **System Account Administration** on the selected system.

This additional **Access Management** tab sheet is only displayed in **System Management** if the user selects a OpenScape 4000 server as system type and if the **Access Management** application checkbox is checked in the **Active Application** area in **System Management**.

Changes made in the **Access Management** tab sheet in the **System Management** application are saved in **System Management**..

The right of a user to define and/or change NSL passwords depends on the user account level and on the access rights associated with this user level. Depending on the user account used to log on, only coequal and subordinate user levels are displayed. Higher-ranking user levels are not displayed, and passwords of higher-ranking user levels can therefore not be edited.

The user interface of the **Access Management** tab sheet is made up of three areas allowing you to set and change NSL password for three different areas of user accounts:

- Access for Service area, Access Management tab sheet

  This area contains the NSL accounts for service administrators.
- Access for Customer area, Access Management tab sheet

  This area contains the NSL accounts for customer administrators.
- System Access (Server-Server Communication) area, Access Management tab sheet

  This area contains the NSL account for server-server communication.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

Related Topics

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.17.1.1 Access for Service area, Access Management tab sheet

The **Access for Service** area in the **Access Management** tab sheet in **System Management** administers the NSL accounts and passwords for Service administrators.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

The **Access for Service** area contains the following NSL accounts:

- Expert level (nsl-engr)
- Second level service (nsl-rsta)
- First level service (nsl-rsca)

To set one (identical) password for all NSL accounts in the Service area, check the check box Same values for all service passwords.

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

For more information about NSL accounts and passwords please refer to:

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Field Descriptions

engr (Access for Service area)

rsta (Access for Service area)

rsca (Access for Service area)

Same value for all service passwords (Access for Service area)

cusa (Access for Customer area)

cust (Access for Customer area)

Same value for all customer passwords (Access for Customer area)

syst (System Access (Server-Server Communication) area)

Save (button)

Discard (button)

New (button)

Delete (button)

See Also

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.17.1.2 Access for Customer area, Access Management tab sheet

The **Access for Customer** area in the **Access Management** tab sheet in **System Management** administers the NSL accounts and passwords for Customer administrators.

On the RSP this area is not displayed, since the NSL access for customer accounts is not supported by the service tool (RSP).

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

The **Access for Service** area contains the following NSL accounts:

- Customer administrator (nsl-cusa)
- Customer (nsl-cust)

To set one (identical) password for all NSL accounts in the Service area, check the check box Same values for all service passwords.

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

For more information about NSL accounts and passwords please refer to:

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Field Descriptions

engr (Access for Service area)

rsta (Access for Service area)

rsca (Access for Service area)

Same value for all service passwords (Access for Service area)

cusa (Access for Customer area)

cust (Access for Customer area)

Same value for all customer passwords (Access for Customer area)

syst (System Access (Server-Server Communication) area)

Save (button)

Discard (button)

New (button)

Delete (button)

See Also

Access for Service area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.17.1.3 System Access (Server-Server Communication) area, Access Management tab sheet

The **System Access (Server-Server Communication)** area in the **Access Management** tab sheet in **System Management** administers the NSL accounts and passwords for server-server communication.

On the RSP this area is not displayed, since the NSL access for customer accounts is not supported by the service tool (RSP).

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

The **System Access (Server-Server Communication)** area contains the **syst** NSL account for server-server communication.

The **syst** NSL account is only used on the System level for internal server-server communication of OpenScape 4000 components like System Management, Expert Access/MPCID, Logging Management.

NOTICE: .NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

For more information about NSL accounts and passwords please refer to:

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Field Descriptions

engr (Access for Service area)

rsta (Access for Service area)

rsca (Access for Service area)

Same value for all service passwords (Access for Service area)

cusa (Access for Customer area)

cust (Access for Customer area)

Same value for all customer passwords (Access for Customer area)

syst (System Access (Server-Server Communication) area)

Save (button)

Discard (button)

New (button)

Delete (button)

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

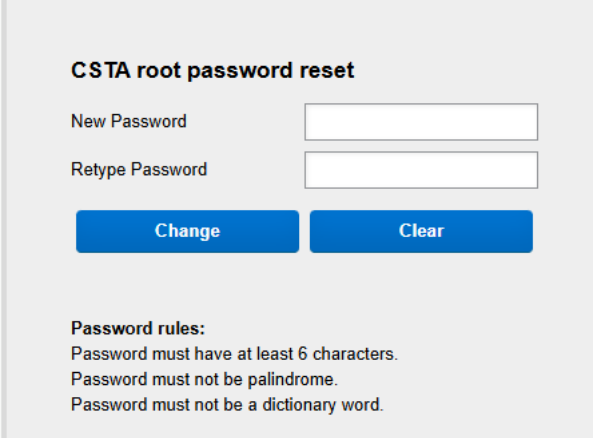
Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

2.18 CSTA Root Password Reset

This section describes the process of changing the **CSTA root password reset**.



Buttons

Change	Clicking on this button will apply the changes made, and the new password will become valid for future sessions.
Clear	Clicking on **Clear** deletes the contents of the entry fields, leaving them blank for new entries.

Password Rules

The rules for entering valid passwords are displayed in the **CSTA root password reset** dialog:

- Password must have at least 6 characters.
- Password must not be palindrome.
- Password must not be a dictionary word.

Field Descriptions

Old Password

New Password

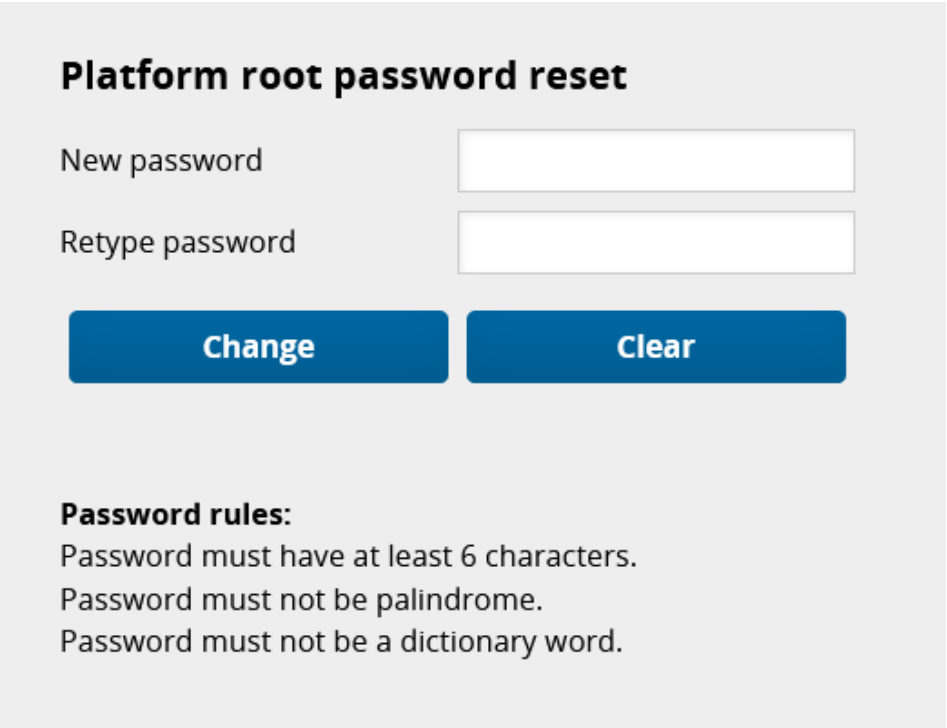
Retype Password

Change

Clear

2.19 Platform Root Password Reset

This section describes the process of changing the **Platform root password reset**.



Buttons

Change	Clicking on this button will apply the changes made, and the new password will become valid for future sessions.
Clear	Clicking on **Clear** deletes the contents of the entry fields, leaving them blank for new entries.

Password Rules

The rules for entering valid passwords are displayed in the **CSTA root password reset** dialog:

- Password must have at least 6 characters.
- Password must not be palindrome.
- Password must not be a dictionary word.

Field Descriptions

Old Password

New Password

Retype Password

Change

Clear

2.20 Automatic lock of OpenScape 4000 Linux accounts

Starting with V11 R1 the main OpenScape 4000 Linux accounts:

- root on Platform (any deployment inclusive Manager)

- TRM on STMIX and STMIY
- root on CSTA (central host and Survivable SoftGate and Enterprise Gateway)
- `engr/rsta/rsca`
  on Assistant and Manager

are locked temporarily after entering 5 times in a row the wrong password via SSH to prevent brute force security attacks via SSH.

After 5 minutes the account will be unlocked automatically.

The messages about locking can be found in `/var/log/messages`

Field Descriptions

Old Password

New Password

Retype Password

Change

Clear

3 Access Management Field Descriptions

This section contains the Access Management Field Help, sorted by topics.

3.1 Web Session Manager - Field Descriptions

Session Settings

Inactive sessions timeout value.

- **The current value of the session inactivity timeout is xx minute(s)/ hour(s)/day(s)/week(s)/month(s).** The dropdown list box displayed here allows you to select and set/change the timeout value for inactive sessions. Inactive sessions will become invalid (and will automatically be deleted) when the timeout value is reached. Only administrators with appropriate access rights are allowed to change this value. When the value is changed, all running sessions or all users are deleted immediately; for all new sessions, the new value is valid.

  Values: 15 minutes (smalles value) to 1 month (largest value).

  Only administrators with appropriate access rights are allowed to change this value.

  Concurrent sessions: maximum value 250.

- **The maximum count of concurrent sessions for one user is: xx**.
  This setting determines the current value set for the maximum number of concurrent sessions allowed for one user account.

  Only administrators with appropriate access rights are allowed to change this value.
- **The maximum count of concurrent sessions for your user account is: xxx** This setting determines the current value set for the maximum number of concurrent sessions.

  Only administrators with appropriate access rights are allowed to change this value.
- **Save session configuration**

  Clicking this button saves the session settings

 # (Sequential Number)

The first column (from left) displays the sequential (consecutive) number assigned to each session.

Kill

In the **Kill** column, klick the **Kill** icon to terminate and delete, respectively, the session displayed in the selected row.

To terminate multiple sessions at once, first select all sessions you want to terminate by checking the checkbox of each session in the **Mark** column, and then click the **Kill all marked sessions** button located beneath the table. See also next item, **Mark**, as well as Check Boxes and Buttons.

Mark

Check this check box to mark the session displayed in this row for future termination/deletion.

Account

Displays the user account of the currently logged-on user, e.g. **cusa**.

Click on the column title to sort the table by this column.

An arrow adjacent to the column title indicates the column by which the table is currently sorted, and also shows whether the table is currently sorted in ascending or descending order. Clicking on the column title again inverts the sorting order, e.g. from ascending to descending order, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

This column can be sorted, but not edited.

Displaying NSL accounts during Network Single Logon using the NSL account

Using the **Network Single Logon** access method you have the possibility to log on without a password from an OpenScape Manager or RSP system. Sessions of this type are displayed as e.g. **htsadm@218.1.16.35** in the **Account** column. As you can see, not only the account name **htssvc0** or **htsadm** is displayed, but also the IP address **account@IP_address** of the server from which the

access originated, i.e. of the server on which the user actually logged in. The solution provided up to now for NSL access performed a kind of "session re-mapping" to an existing account. The new solution creates a dynamic account composed of **account@IP_address**. In the **Logging Management** application this account is displayed accordingly as **account@IP_address** in the **User** column. The **Details** column in Logging Management shows the complete path and the mapping of the Network Single Logon.

See Also: Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

Session

This column displays a unique reference number for every session. If a user has multiple logins (multiple sessions running), each session is assigned a unique reference number and displayed accordingly in this column. The session reference number is also helpful in creating a cross reference to the activities in the **Logging Management** application. In the Logging Management application the session reference number is displayed as **Session Ref**.

Click on the column title to sort the table by this column.

An arrow adjacent to the column title indicates the column by which the table is currently sorted, and also shows whether the table is currently sorted in ascending or descending order. Clicking on the column title again reverts the sorting order, e.g. from ascending to descending order, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

This column can be sorted, but not edited.

Client

This column displays the IP address of the client system from which the user logged on.

Click on the column title to sort the table by this column.

An arrow adjacent to the column title indicates the column by which the table is currently sorted, and also shows whether the table is currently sorted in ascending or descending order. Clicking on the column title again reverts the sorting order, e.g. from ascending to descending order, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

This column can be sorted, but not edited.

Logon Time

This column displays the date and time when a user logged on to the server, e.g. 2003-07-16 12:44.

This value remains unchanged for the whole duration of the session.

Click on the column title to sort the table by this column.

An arrow adjacent to the column title indicates the column by which the table is currently sorted, and also shows whether the table is currently sorted in ascending or descending order. Clicking on the column title again reverts the sorting order, e.g. from ascending to descending order, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

This column can be sorted, but not edited.

Last Access

This column displays the date and time of the last browser access within a session. With each new access this value is updated accordingly. All other values remain unchanged for the complete duration of a session.

The value displayed in this column allows you to find out which user performed the most recent access, and at what date/time this last access occurred. Administrators who are administering a large number of sessions can sort by the **Last Access** column to find out which session becomes invalid at what date/time - depending on the value set in "Session Inactivity Timeout".

Click on the column title to sort the table by this column in ascending or descending order.

An arrow adjacent to the column title indicates the column by which the table is currently sorted, and also shows whether the table is currently sorted in ascending or descending order. Clicking on the column title again reverts the sorting order, e.g. from ascending to descending order, or vice versa, respectively.

Default setting for table sorting: By default, the table is sorted by the **Last Access** column, with the "oldest" entry on the top, i.e. the session with the longest inactivity time duration.

This column can be sorted, but not edited.

Kill all marked sessions

Clicking this button terminates all sessions, which are marked (see checkbox **Mark**) for killing in the **Existing Session** table.

3.2 Change Password - Field Descriptions

Old Password

New Password

Retype Password

Change

Clear

Old Password

In order to change the password, the old password has to be entered into this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Minumum length is 6 characters, maximal length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **Old Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

New Password

The new password has to be entered into this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **New Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

Retype Password

The new password has to be re-typed in this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **Retype Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

Change

Click this button to apply the password changes and to make the new password valid for all sessions from now on.

Clear

Click this button to delete the contents from all entry fields. The blank fields are then ready to accept new values.

3.3 Password Distribution (OpenScape 4000 Manager only) - Field Descriptions

Old Password

In order to change the password, the old password has to be entered into this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Minumum length is 6 characters, maximal length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **Old Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

New Password

The new password has to be entered into this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **New Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

Retype Password

The new password has to be re-typed in this field. Password entries are case-sensitive.

This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).

The **Retype Password** entry field is only displayed if the user has "Change Password" privileges, i.e. if he/she has the right to change passwords.

Change the password also on Assistants (Password Distribution)

If you do **not** check the checkbox **Change the password also on Assistants (Password Distribution)**, the password change only effects the local Manager.

If you check the checkbox **Change the password also on Assistants (Password Distribution)**, all passwords on the Assistants assigned are also changed.

Change

Click this button to apply the password changes and to make the new password valid for all sessions from now on.

Clear

Click this button to delete the contents from all entry fields. The blank fields are then ready to accept new values.

3.4 Account and Password Policy - Field Descriptions

Use extended password handling rules

Enable duty hours

Account is locked after: xx days of inactivity

Password must expire after: xx days

Use extended password handling rules

To enable the use of extended password rules, check the "Use extended password handling rules" checkbox and set the values for:

- **Minimum length of the password: xx characters**

  This input field determines the minimum length of the password. Possible values: 6 to 20.
- **Password must contain at least: xx upper case letters**

  This input field determines the minimum number of upper case letters the password must contain. Possible values: 0 to 20.
- **Password must contain at least: xx lower case letters**

  This input field determines the minimum number of lower case letters the password must contain. Possible values: 0 to 20.
- **Password must contain at least: xx numbers**

  This input field determines the minimum number of digits the password must contain. Possible values: 0 to 20.
- **Password must contain at least: xx special characters**

  This input field determines the minimum number of special characters the password must contain. Possible values: 0 to 20.
- **Password history length: xx passwords**

  This input field determines the minimum number of password changes after which the same password (i.e. the first one in the series) can be re-used. Possible values: 0 to 10.
- **Minimum time between password changes: xx days**

  This input field determines the number of days after which a password can be changed. Possible values: 0 to 30
- **Password must differ from the previous at least: xx characters**

  This input field determines the minimum number of digits, letters or special character the password must be different from the previous password when it is changed. Possible values: 0 to 20.

Enable duty hours

To enable the use of a time-defined account validity, i.e. to set the times of day (=duty hours) when an account is allowed to be used, check this checkbox and set the values for:

- **Work day begins**

  Start time of day when the account can be used.
- **Work day ends**

  End time of day when the account can be used.
- **Work week days**

  Only on checked week days the account can be used.

Account is locked after: xx days of inactivity

To enable the use of time-restricted account validity, check this checkbox and set the number of idle days, i.e. number of days within no login is done, after which the account will be locked completely.

Password must expire after: xx days

To enable the use of a time-defined password validity, i.e. the number of days after which the password must be changed, check this checkbox and set the number of valid days for the password.

3.5 User Account Administration and System Account Administration - Field Descriptions

User Name

Read-only field for user account name in the **Identification** field area, **User Account Administration** and **System Account Administration** dialog.

See also Toolbar Icons - User Account Administration dialog.

Description

Entry field for user name description in the **Identification** field area, **User Account Administration** and **System Account Administration** dialog. This entry field accepts alphanumeric and special characters. The description cannot be changed for predefined accounts listed in the **System Account Administration** dialog.

Security Profile

Displays the security profile of the user account: engr, rsca, rsta, cusa or cusa

New Password

Entry field in the **Actions** area, **User Account Administration** and **System Account Administration** dialog. The new password for the selected user(s) has to be entered into this field. Password entries are case-sensitive. This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).

Retype Password

Entry field in the **Actions** area, **User Account Administration** and **System Account Administration** dialog. The new password for the selected users has to be re-entered into this field. This avoids unwanted typing errors, as passwords are never displayed on the screen.

Delete Password

Checkbox in the **Actions** area, **User Account Administration** and **System Account Administration** dialog. If this checkbox is activated (checked), the **New password** and **Retype password** fields are greyed out. Also, the **Force password change** checkbox will automatically be activated and greyed out. If the existing password is deleted for a user or set of users, this user or set of users will not need to enter any password when they log on the next time. But since Force password change is always automatically activated together with Delete password, the user(s) who log on will be prompted to enter a new password when they log on. This checkbox is not available for system accounts and NSL accounts in the **System Account Administration** dialog: they must always have a password set.

Force password change

Checkbox in the **Actions** area, **User Account Administration** and **System Account Administration** dialog. If this checkbox is active, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time. This checkbox is automatically activated if **Delete password** is activated. This checkbox is not available for system accounts and NSL accounts in the **System Account Administration** dialog: forced password change is only supported for interactive logons.

Max. password validity

Entry field in the **Properties** area, **User Account Administration** and **System Account Administration** dialog. The value entered defines the maximum number of days for a password being valid. When the password becomes invalid, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time. This entry field is not available for system accounts and NSL accounts in the **System Account Administration** dialog: forced password change is only supported for interactive logons.

Password never expires

Checkbox in the **Properties** area, **User Account Administration** and **System Account Administration** dialog. This property can be turned on or off. If it is turned on (checked) the user password will never become invalid, and the entry field **Max. password validity** is deactivated. This checkbox is always checked for system accounts and NSL accounts in the **System Account Administration** dialog.

Lock user account

Checkbox in the **Properties** area, **User Account Administration** and **System Account Administration** dialog. This property can be turned on or off. If it is turned on (checked) the user cannot log on.

Allowed to change password

Checkbox in the **Properties** area, **User Account Administration** dialog. This feature can be turned on or off. If it is turned on (checked) the user is allowed to change the own password, i.e. the user has access to the **Change Password** dialog.

Access through Network Single Logon only

For RSP only, a new checkbox Access through Network Single Logon only has been added in the **Properties** area.

Checked - If this check box is **checked**, the selected user/s can no longer log on directly to the server, but only via NSL from a higher-ranking RSP (SIRA) server.

Unchecked - If this check box is **unchecked**, the selected user/s can log on directly to the server.

Lock account automatically

Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the number of unsuccessful logons after which the account will automatically be locked.

If a user account is locked due to unsuccessful logons, a corresponding error message will be displayed after entering the correct password.

See also Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts.

Possible values: Never; 1 to 15 (max.) unsuccessful logons.

occurring during

Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period within which the unsuccessful logons must happen to activate the automatic locking of the account.

If a user account is locked due to unsuccessful logons, a corresponding error message will be displayed after entering the correct password.

See also Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts.

Possible values: any time; 30 seconds to (max.) 1 week.

Unlock it automatically

Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period after which the locked account will be unlocked.

If a user account is locked due to unsuccessful logons, a corresponding error message will be displayed after entering the correct password.

See also Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts.

Possible values: Never; 30 seconds to (max.) 1 month.

Apply (Button)

Clicking on the **Apply** button in the lower right part of the screen applies the selected properties to the selected user(s). This command has the same function as the **Apply** entry in the **Edit** menu and the **Apply modifications** icon in the toolbar.

See also:

Edit menu - User Account Administration

Edit menu - System Account Administration

Toolbar Icons - User Account Administration dialog

Discard (Button)

Clicking on the **Discard** button in the lower right part of the screen discards the applied changes made to the selected user(s). This command has the same function as the **Discard** entry in the **Edit** menu and the **Discard modifications** icon in the toolbar.

S:ee also

Edit menu - User Account Administration

Edit menu - System Account Administration

Toolbar Icons - User Account Administration dialog

Reload

Clicking on **Reload** in the **Edit** menu updates the contents of the **User Account Administration** and **System Account Administration** dialogs by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions.

This command has the same function as the **Reload data from server** icon in the Toolbar.

See also

Edit menu - User Account Administration

Edit menu - System Account Administration

Toolbar Icons - User Account Administration dialog

3.6 Add new user - Field Descriptions

New username

Description

New username

Entry field for new user (account) name.

A user name must start with an alphabetic character (a-z or A-Z) and must consist of alphanumeric characters (a-z, A-Z, 0-9), underscores (_) and hyphens (-) only.

Description

Entry field for user (account) name description.

This entry field accepts alphanumeric and special characters.

3.7 List of User Accounts, Export User Reports window

The data displayed in this list is identical with the data in the **User Account Administration** area.

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: List of User Accounts

User Name

Description

Locked

Max. Password Validity

Change Password Allowed

 # eur.cgi v1.0

This line is always the first line and shows the version number of the output format of the list. A changed version number indicates that the output format has changed, e.g. it may contain additional or changed columns. The following description refers to version "v1.0".

"**eur**" stands for "Export User Reports".

Export User Reports: List of User Accounts

This is the title of the list. It indicates the type of data exported, in this case a list of user accounts. Next to the title, this line also contains the following information:

- Creation date and time of the data list
- Name of the server as configured on the system
- Server software version number, e.g. **0.520**

User Name

This column contains the user name. The data displayed here is defined and maintained in the **Identification** area of the **User Account Administration** dialog in **Access Management**.

The **#0** entry at the bottom of the **User Name** column indicates that the data export was successful, and completed without errors. Any other value than 0 indicates an error during data export.

See also

User Account Administration dialog - User Interface Description.

Description

This field contains a short description of the user name. The description displayed here is defined and maintained in the **Identification** area of the **User Account Administration** dialog in **Access Management**.

See also

User Account Administration dialog - User Interface Description.

Locked

This field displays the current status of the **Lock User Account** check box in the **Properties** area of the **User Account Administration** dialog in **Access Manangement**. "Yes" indicates that the user is currently not allowed to log on.

See also

User Account Administration dialog - User Interface Description.

Max. Password Validity

The current value of the **Max. Password Validity** field in the **Properties** area of the **User Account Administration** dialog is displayed here. The value defines the maximum time period of password validity (in number of days). A value of "-1" indicates that the password never expires.

See also

User Account Administration dialog - User Interface Description.

Change Password Allowed

This field displays the current status of the **Change Password Allowed** check box in the **Properties** area of the **User Account Administration** dialog in **Access Manangement**. "Yes" indicates that the user is allowed to change his/her own password.

See also

User Account Administration dialog - User Interface Description.

3.8 List of Users and Assigned Access Right Groups , Export User Reports window

The data displayed in this list is identical with the data in the **Access Right Configuration** area.

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: Liste of Users and Assigned Access Right Groups

User Name

Description

ID of Access Right Group

Description of Access Right Group

 # eur.cgi v1.0

This line is always the first line and shows the version number of the output format of the list. A changed version number indicates that the output format has changed, e.g. it may contain additional or changed columns. The following description refers to version "v1.0".

"**eur**" stands for "Export User Reports".

Export User Reports: Liste of Users and Assigned Access Right Groups

This is the title of the list. It indicates the type of data exported, in this case a list of user accounts and associated access right groups. Next to the title, this line also contains the following information:

- Creation date and time of the data list
- Name of the server as configured on the system
- Server software version number, e.g. **0.520**

User Name

This column contains the user name. The data displayed here is defined and maintained in the **Users** area of the **Access Right Configuration** dialog in **Access Management**.

The **#0** entry at the bottom of the **User Name** column indicates that the data export was successful, and completed without errors. Any other value than 0 indicates an error during data export.

See also

Access Right Configuration dialog - User Interface Description.

Description

This field contains a short description of the user name. The description displayed here is defined and maintained in the **Users** area of the **Access Right Configuration** dialog in **Access Management**.

See also

Access Right Configuration dialog - User Interface Description.

ID of Access Right Group

This field displays the internal ID of an access right group, e.g. **arg3** for a manually created group, or **All-SysM** for a pre-defined group.

See also

Access Right Configuration dialog - User Interface Description.

Description of Access Right Group

This field contains a short description of the access right group, e.g. "All access rights of "Configuration Management"", or the name as it has been defined for a manually created group.

See also

Access Right Configuration dialog - User Interface Description.

3.9 List of Manually Created Access Right Groups, Export User Reports window

The data displayed in this list is identical with the data in the **Access Right Group Configuration** area. However, manually created access right groups are exported only. Predefined groups are not exported, as they are preinstalled in the system and not changeable.

Description of the table rows and columns

eur.cgi v1.0

Export User Reports: Liste of Manually Created Access Right Groups

ID of Access Right Group

Description of Access Right Group

ID of Component

Description of Component

ID of Access Right

Description of Access Right

eur.cgi v1.0

This line is always the first line and shows the version number of the output format of the list. A changed version number indicates that the output format has changed, e.g. it may contain additional or changed columns. The following description refers to version "v1.0".

"**eur**" stands for "Export User Reports".

Export User Reports: Liste of Manually Created Access Right Groups

This is the title of the list. It indicates the type of data exported, in this case the list of manually created access right groups. Next to the title, this line also contains the following information:

- Creation date and time of the data list
- Name of the server as configured on the system
- Server software version number, e.g. **0.520**

ID of Access Right Group

This field displays the internal ID of a manually created access right group, e.g. **arg3**.

The **#0** entry at the bottom of this column indicates that the data export was successful, and completed without errors. Any other value than 0 indicates an error during data export.

See also

Access Right Group Configuration dialog - User Interface Description.

Description of Access Right Group

This field contains the name as it has been defined for a manually created group.

See also

Access Right Group Configuration dialog - User Interface Description.

ID of Component

This field contains the internal ID of the software component, e.g. "HBR" for "Backup & Restore".

See also

Access Right Group Configuration dialog - User Interface Description.

Description of Component

This field contains a short description of the component ID, e.g. "Direct Access" for "DA".

See also

Access Right Group Configuration dialog - User Interface Description.

ID of Access Right

Each individual access right within an access right group has its own internal ID displayed in this column, e.g. "HBR-Backup" for the Backup feature of Backup & Restore or "sendBroadcast" for the "Broadcast Message" feature of the Start Page (LAP).

See also

Access Right Group Configuration dialog - User Interface Description.

Description of Access Right

This field contains a short description of the access right ID listed in the previous column, e.g. "Network Single Logon" for "nsl-own" or "Install License Data" fÃ¼r "storeLicData".

See also

Access Right Group Configuration dialog - User Interface Description.

3.10 Manage Web Server Certificates -- Field Descriptions

Certificates for this Web Server -> Activate

3.10.1 Certificates for this Web Server -> Activate

Activate (Link on Start Page of Access Management)

Navigation: **Start Page -> Access Management -> Manage Web Server Certificates -> Certificates for this Web Server -> Activate**

Click or double-click on the **Activate** link to open the **Activate Server Certificate** dialog.

The following types of SSL security certificates are displayed in this dialog:

- Currently Active Certificate (Table in Activate Server Certificate dialog)

- Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

Currently Active Certificate (Table in Activate Server Certificate dialog)

The currently active SSL security certificate, i.e. the certificate currently used by the HTTP server is displayed in a table with the following **columns**:

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Shows the mode of creation of the currently active SSL certificate.

Possible modes/values: **Pre-installed**, **Generated**, **Imported**, **Generated via CSR**.

NOTICE: The software is shipped with a pre-installed security certificate by default. A password is not required with pre-installed certificates. The **Password** entry field is not displayed with pre-installed certificates.

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

In the **Server Name** column, click the server name displayed as a **Link** in order to display additional details of the currently active certificate. The complete list of detail data of this certificate is then displayed in the browser in the **Certificate Information** table.

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

In the **Server Name** column, click on the name (displayed as a link) of the currently active certificate. The complete list of detail data of the currently active certificate is then displayed in the browser in the **Certificate Information** table, grouped by the following categories:

- **Name and Validity**
  - Version of Certificate
  - Serial Number of Certificate
  - Signature Algorithm
  - Start of Validity / End of Validity

- **Issuing CA**
  - Name of CA
  - Country
  - Organisation
  - Organizational Unit
- **Server**
  - Server Name
  - Country
  - Organisation
  - Organizational Unit
  - Mail Address
- **Encryption Information**
  - Encryption Algorithm
  - Elliptic curve for ECDSA
  - Key Length
  - MD5 Fingerprint
  - SHA1 Fingerprint

Delete Certificate (Button in Certificate Information view, Display Certificate dialog)

The **Delete certificate** button is displayed in red color in the **Certificate Information** table.

Click on this button to delete this certificate, the data of which is currently being displayed in the **Certificate Information** table.

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Name of Certificate Authority that verified and signed the certificate.

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Shows the validity period of the currently valid certificate.

Distribute active certificate (Button beneath Currently Active Certificate table, Activate Server Certificate dialog)

This button is only displayed if there is at least one HG3550 v2 board with an independently running Web Server installed.

Click on **Distribute active certificate** to distribute the active certificate to all existing HG3550 v2 boards.

You will then be prompted to enter the password for the private key of the certificate and to continue your action by clicking on the **Distribute certificate** button.

The **Activate Server Certificate** dialog will then display one of the following messages:

- the confirmation message regarding the successful distribution of the certificate,

or

- an error message informing you that an error occurred during the distribution of the active server certificate to the HG3550 v2 boards.

  The error message is displayed on the screen and you are prompted to repeat the process, and -- if the error should occur again -- to verify the configuration using the HG3550 v2 Manager, to update the board list, and to establish a connection to all boards listed.

  If the error still persists, you should send the displayed error message to your system administrator or to the service department.

Overview of all certificates that can be activated (Table in Activate Server Certificate dialog)

This list displays all certificates that can be activated. You may select a new certificate for activation from this list, provided that you previously created and imported such a certificate. The selected certificate will then be displayed for verification purposes.

Only signed certificates can be activated.

NOTICE: HG35xx boards that are not based on Linux (STMI and NCUI) support only RSA certificates for web based administration. If the selected certificate type is ECDSA, it will not be distributed to these types of boards. All SoftGate based boards support ECDSA.

NOTICE: The software is shipped with a pre-installed security certificate by default. A password is not required with pre-installed certificates. The **Password** entry field is not displayed with pre-installed certificates.

The table of all certificates that can be activated contains the following columns:

Origin (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Server Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Certificate Information (Display Certificate dialog; click on link in Server Name column to open)

CA Name (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Validity (from / until) (Column in Currently Active Certificate and Overview of All Certificates That Can Be Activated tables, Activate Server Certificate dialog)

Activate (Radio Button in Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog**)**

Activate (Radio Button in Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Click this radio button in the **Activate** column to select the certificate to be activated.

Only signed certificates can be activated.

Distribute the selected certificate to all available HG35xx boards as well (Checkbox beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

If this checkbox is checked (default: checked), the selected certificate is activated on the server as usual by clicking the **Activate selected certificate** button, and distributed to all available HG35xx boards at the same time.

This checkbox is only displayed if there is at least one HG35xx board with an independently running Web Server installed on this system.

Only signed certificates can be activated.

Default value: checked.

See Also

Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only

---

NOTICE: HG35xx boards that are not based on Linux (STMI and NCUI) support only RSA certificates for web based administration. If the selected certificate type is ECDSA, it will not be distributed to these types of boards. All SoftGate based boards support ECDSA.

Activate selected certificate (Button beneath Overview of All Certificates That Can Be Activated table, Activate Server Certificate dialog)

Click this button to activate the certificate marked by checking the radio button in the **Activate** column, and to proceed to the next process step.

In the **Activate Server Certificate** dialog, **Overview of all certificates that can be activated** table, **Activate** column, select the radio button of the certificate you want to activate, and click on **Activate selected certificate**.

The certificate details of the selected certificate are then displayed in the **Activate Server Certificate** dialog.

See Also

Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only

and

Activate - HG35xx Board NOT Installed

Activate certificate (Button, Activate Server Certificate dialog)

Button located next to the table showing the detail data in the **Activate Server Certificate** dialog.

1) In the **Activate Server Certificate** dialog, **Overview of all certificates that can be activated** table, **Activate** column, check the radio button of the certificate you want to activate.

   Only signed certificates can be activated.

2) Click on **Activate selected certificate**.

   The certificate details are then displayed in the **Activate Server Certificate** dialog, and the program prompts you to enter the password for the private key.

   Entering a password is not required with pre-installed certificates. Therefore, the password prompt and the password entry field are not displayed with pre-installed certificates.

3) Enter the **Password** for the private key - if required - and click on **Activate certificate**.

   NOTICE: The Web Server always needs to be restarted after activating a new certificate. All currently running sessions, including your own session, will be terminated upon restart.

   A warning message is displayed, alerting you that the Web Server needs to be restarted after activating a new certificate, and that all currently running sessions, including your own session, will be terminated on the server.

   The selected certificate is activated and displayed as new **Currently active Certificate** in the **Activate Server Certificate** dialog.

   or

4) Click on **Back** in the **Activate Server Certificate** dialog if you do not want to activate the new certificate.

See Also

Activate - HG35xx Board IS INSTALLED - On OpenScape 4000 Assistant Only

and

Activate - HG35xx Board NOT Installed

Back (Button, Activate Server Certificate dialog)

Button located beneath the table showing the detail data, in the **Activate Server Certificate** dialog.

Click this button to go back to the previous process step.

3.10.2 Certificates for this Web Server -> Generate

Server Name

Mail Address

Organizational Unit

Organization

Location

State

Country

Subject Alternative Name (subjectAltName)

Signature Algorithm

Key Length - for RSA only

Validity

Password for Private Key

Password Confirmation

Server Name

The server name is mandatory and must correspond to the real unique host name of the server (DNS name). This is the name used in the address bar of the browser, without http:// or https://. Wildcards (e.g. *.domain.com), IP addresses and port numbers are not allowed.

Example: openscape4k.company_name.com

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Mail Address

Optional mail address, e.g. of the Web Server administrator.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organizational Unit

Optional organizational unit within your organisation, e.g. Department.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organization

Optional name of your organisation, e.g. company.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Location

Optional name of the city in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

State

Optional name of the state in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Country

Optional 2-letter country code, e.g. DE for Germany, US for United States of America.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Subject Alternative Name (subjectAltName)

The Subject Alternative Name is an extension to X.509 that allows you to add various values which describe the server, e.g. IP addresses, URLs, DNS names.

Assistant will automatically add the IP addresses of Assistant, CSTA GUI, and Platform Portal to the subjectAltName field.

Standalone Appliances Portal/YAST IPs are also added by default. DNS names are also added for all IP addresses by default if found by query in the DNS servers of the system.

In addition, you can add your own addresses for servers, which shall be provided with the certificate.

Include Gateway addresses

Add the list of all Gateway IP addresses to subjectAltName. For web server certificate, the Management IP addresses shall be added. For SPE certificate the Voice IP addresses shall be added.

Signature Algorithm

Specifies the cryptographic hash function used for certificate signature.

The number in the name of the function represents the length of the hash values in bits.

The dropdown list allows you to select the desired value.

Possible values: SHA-1, SHA-256 (recommended), SHA-384, SHA-512.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Key Length - for RSA only

Specifies the encryption level as a key length (in bits) .

2048 bit is the recommended value, since some browsers may have problems with higher encryption levels, i.e. with longer keys.

The dropdown list in the second column allows you to select the desired value.

Possible values: 2048 bits (recommended); 4096 bits.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Elliptic Curve - for ECDSA only

For ECDSA, the elliptic curve must be specified. All openssl supported elliptic curves for ECDSA algorithm are listed here. Most popular curves are

NIST-approved Suite B, e.g. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Validity

Certificates are always generated with a restricted duration. After expiration of the validity period the browser will issue a corresponding notification. The dropdown list in the second column allows you to select the desired value. The minimum duration value is 1 week, the maximum duration is 3 years.

Possible values: 1 week, 2 weeks, 1 month, 3 months, 6 months, 1 year, 2 years, 3 years.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Password for Private Key

The private key is stored in encrypted format and can only be decrypted with the password.

NOTICE: Attention: This password is not saved anywhere! Therefore, it has to be entered again when activating this certificate, even if this is done days or months later. Losing the password causes the private key and the certificate to be unusable.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Password Confirmation

Confirming your password avoids typing errors.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Continue (Button)

Use this button to get to the next process step.

After having created a new certificate the program goes back to the **Activate Server Certificate** dialog. The newly created certificate is displayed and is already preselected (highlighted) as a rule. In the **Origin** column the entry **Generated** is displayed in this case.

See also the generic feature description under Generate**.**

3.10.3 Certificates for this Web Server -> Import

File with Key and Certificate (Entry Field)

Password for Private Key (Entry Field)

Import Certificate (Button)

File with Key and Certificate (Entry Field)

Entry field in the **Import Server Certificate and Key** dialog. It serves for entering the path and file name of a certificate and private key created on a different host. The supported file format is X.509 PEM and PKCS #12. You need to enter the password (see next field) in order to decode the encoded private key.

Importing a certificate and private key created on a different host is possible under the following conditions:

- Supported file format: X. 509 PEM and PKCS #12. If the file extension is *.p12, it is treated as a PKCS #12, otherwise X.509 PEM format is used.
- Private key and password for decoding are required and exist.

Password for Private Key (Entry Field)

To decrypt the encrypted private key you need to enter the password.

Importing a certificate and private key created on a different host is possible under the following conditions:

- Supported file format: X. 509 PEM and PKCS #12. If the file extension is *.p12, it is treated as a PKCS #12, otherwise X.509 PEM format is used.
- Private key and password for decoding are required and exist.

Import Certificate (Button)

The program goes back to the **Activate Server Certificate** dialog. The imported certificate is displayed and is already preselected (highlighted) as a rule. In the **Origin** column the entry **Imported** is displayed in this case. The imported certificate can now be activated.

The **Status** of the selected certificate is additionally indicated by a **color**. The colors have the following meaning:

red = signed certificate, active on server

green = signed certificate available, ready for activation.

See also the generic feature description under Import**.**

3.10.4 Certificates for this Web Server -> Generate via CSR

Server Name (Table Column)

CA Name (Table Column**)**

Validity (from / until) (Table Column**)**

Generated (Table Column)

Exported (Table Column)

Imported (Table Column)

Action (Table Column)

Test (Button)

Export (Button)

Server Name (Table Column)

In the **Server Name** column, click the server name displayed as a **Link** in order to display additional details of the currently active certificate. The complete list of detail data of this certificate or CSR, respectively, is then displayed in the browser in the **Display Certificate / Certificate Information** table. The Delete Certificate button in the Display Certificate dialog allows you to delete the currently displayed certificate or CSR, respectively.

CA Name (Table Column)

Name of Certificate Authority that verified and signed the certificate.

Validity (from / until) (Table Column)

Start and end date of validity period (from: YYYY-MM-DD - until: YYYY-MM-DD) of the currently active certificate.

Generated (Table Column)

Specifies the user (account) who generated this certificate, e.g. **by: rsta**, and the date and time of creation in the following format YYYY-MM-DD HH:MM, e.g. **at: 2004-02-11 10:07**.

Exported (Table Column)

Specifies the user (account) who exported this certificate, e.g. **by: rsta**, and the date and time of export in the following format YYYY-MM-DD HH:MM, e.g. **at: 2004-02-11 10:07**.

Imported (Table Column)

Specifies the user (account) who imported this certificate, e.g. **by: rsta**, and the date and time of import in the following format YYYY-MM-DD HH:MM, e.g. **at: 2004-02-11 10:07**.

Action (Table Column)

Contains the icon buttons **Test**, **Export**, **Import**, **Activate**.

Depending on the current status of a certificate can the action be executed or not executed (greyed-out), respectively.

Test (Button)

Icon button in **Action** column; serves for testing the newly created, self signed certificate.

Depending on the current status of a certificate can the action be executed or not executed (greyed-out), respectively.

Export (Button)

Icon button in **Action** column; serves for exporting the newly created, self signed certificate.

Depending on the current status of a certificate can the action be executed or not executed (greyed-out), respectively.

Import (Button)

Icon button in **Action** column; serves for importing the newly created, self signed certificate.

Depending on the current status of a certificate can the action be executed or not executed (greyed-out), respectively.

Activate (Button)

Icon button in **Action** column; serves for activating the newly created, self signed certificate.

Depending on the current status of a certificate can the action be executed or not executed (greyed-out), respectively.

Certificate Information

In the **Server Name** column, click on the name (displayed as a link) of the currently active certificate. The complete list of detail data of the currently active certificate is then displayed in the browser in the **Certificate Information** table, grouped by the following categories:

- **Name and Validity**
  - Version of Certificate
  - Serial Number of Certificate
  - Signature Algorithm
  - Start of Validity / End of Validity

- **Issuing CA**
  - Name of CA
  - Country
  - Organisation
  - Organizational Unit
- **Server**
  - Server Name
  - Country
  - Organisation
  - Organizational Unit
  - Mail Address
- **Encryption Information**
  - Encryption Algorithm
  - Elliptic curve for ECDSA
  - Key Length
  - MD5 Fingerprint
  - SHA1 Fingerprint

Delete Certificate (Button)

Click on this button in the **Certificate Information** table, in order to delete the current certificate/CSR displayed in the **Certificate Information** table. The button is displayed in red color.

Server Name (Entry Field)

The server name is mandatory and must correspond to the real unique host name of the server (DNS name). This is the name used in the address bar of the browser, without http:// or https://. Wildcards (e.g. *.domain.com), IP addresses and port numbers are not allowed.

Example: openscape4k.company_name.com

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Mail Address

Optional mail address, e.g. of the Web Server administrator.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organizational Unit

Optional organizational unit within your organisation, e.g. Department.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organization

Optional name of your organisation, e.g. company.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Location

Optional name of the city in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

State

Optional name of the state in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Country

Optional 2-letter country code, e.g. DE for Germany, US for United States of America.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Signature Algorithm

Specifies the cryptographic hash function used for certificate signature.

The number in the name of the function represents the length of the hash values in bits.

The dropdown list allows you to select the desired value.

Possible values: SHA-1, SHA-256 (recommended), SHA-384, SHA-512.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Key Length - for RSA only

Specifies the encryption level as a key length (in bits) .

2048 bit is the recommended value, since some browsers may have problems with higher encryption levels, i.e. with longer keys.

The dropdown list in the second column allows you to select the desired value.

Possible values: 2048 bits (recommended); 4096 bits.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Elliptic Curve - for ECDSA only

For ECDSA, the elliptic curve must be specified. All openssl supported elliptic curves for ECDSA algorithm are listed here. Most popular curves are

NIST-approved Suite B, e.g. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Validity

Certificates are always generated with a restricted duration. After expiration of the validity period the browser will issue a corresponding notification. The dropdown list in the second column allows you to select the desired value. The minimum duration value is 1 week, the maximum duration is 3 years.

Possible values: 1 week, 2 weeks, 1 month, 3 months, 6 months, 1 year, 2 years, 3 years.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

You can **renew a certificate by extending its validity**. Please proceed as follows:

Renewing a Certificate or CSR, respectively, by Extending its Validity

1) In the **Validity** column, move the mouse pointer to the end date of the certificate.

   The tooltip text **Renew Certificate** is displayed.
2) Click on the displayed end date.

   The **Generate Certificate via CSR** dialog is displayed. The certificate data are already present in the fields. Please take over the existing values unchanged, if possible, and onlyy change the validity period, because changed values need to be verified and confirmed by the Certificate Authority (CA).

   Using this method you create a new CSR that you can later send to a CA for signing purposes. The signed certificate can then be imported and activated on the server. The new CSR is automatically turned into a self signed certificate for testing purposes. You may then test and export this self signed certificate in order to send it to the CA.

Password for Private Key

The private key is saved in encrypted format and can only be decrypted and read by providing the password.

NOTICE: Attention: This password is not saved anywhere! Therefore, it has to be entered again when activating this certificate, even if this is done days or months later. Losing the password causes the private key and the certificate to be unusable.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Password Confirmation

Confirming your password avoids typing errors.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Continue (Button)

Use this button to get to the next process step.

After having created a new certificate the program goes back to the **Activate Server Certificate** dialog. The newly created certificate is displayed and is already preselected (highlighted) as a rule. In the **Origin** column the entry **Generated via CSR** is displayed in this case.

Back (Button)

Click this button in the **Generate Certificate via CSR** dialog to go back to the previous process step.

See also the generic feature description under Generate via CSR.

3.10.5 Certificate Network Management-> Root Certificate

Root Certificate (link)

This allows you to import the certificate to the Trusted Root CA Store of the client browser and to the Java Runtime Environment. Afterwards you are also able to distribute this Root CA certificate to all other clients which need access to the Managers and Assistants using this same Root certificate.

The advantage of this, in contrast to a self-signed certificate, is that the certificate may be used for all Managers and Assistants. So each client, having access to this certificate, needs to import this root certificate only once, instead of importing an individual certificate for each Manager and Assistant.

New Root Certificate (Button)

Button in the **Root Certificate** dialog.

1) Click on the **New Root Certificate** button in the **ROOT CERTIFICATE** dialog if you want to create a new Root Certificate.

   If no Root Certificate has been created for this server yet, the empty **Root Certificate** dialog will open.

   If a self signed Root Certificate has already been created for this server, the data of the existing certificate will be displayed together with a corresponding note in the **Root Certificate** dialog in the browser.

   NOTICE: Warning: If you create a new root certificate although a self signed root certificate already exists for this server, the existing root certificate will be overwritten.

   ---

2) If you want to use the existing root certificate for signing CSRs, click on Sign CSR.

   You can use this root certificate to sign external CSRs.
3) If you want to create a new root certificate and overwrite the existing root certificate, click on **New Root Certificate**.

   The **Generate Root Certificate** dialog opens.

Name of Certificate Authority (entry field)

The name of your Certificate Authority is mandatory.

Enter a name for your Certificate Authority here.

Mandatory fields are flagged with a red asterisk (*).

Mail Address

Optional mail address, e.g. of the Web Server administrator.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organizational Unit

Optional organizational unit within your organisation, e.g. Department.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Organization

Optional name of your organisation, e.g. company.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Location

Optional name of the city in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

State

Optional name of the state in which your organization is located.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Country

Optional 2-letter country code, e.g. DE for Germany, US for United States of America.

Do not use accented characters (e.g. "umlauts" like "Ã¤" or "Ã¼") or other special characters.

Optional.

Signature Algorithm

Specifies the cryptographic hash function used for certificate signature.

The number in the name of the function represents the length of the hash values in bits.

The dropdown list allows you to select the desired value.

Possible values: SHA-1, SHA-256 (recommended), SHA-384, SHA-512.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Key Length - for RSA only

Specifies the encryption level as a key length (in bits) .

2048 bit is the recommended value, since some browsers may have problems with higher encryption levels, i.e. with longer keys.

The dropdown list in the second column allows you to select the desired value.

Possible values: 2048 bits (recommended); 4096 bits.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Elliptic Curve - for ECDSA only

For ECDSA, the elliptic curve must be specified. All openssl supported elliptic curves for ECDSA algorithm are listed here. Most popular curves are NIST-approved Suite B, e.g. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Validity

Certificates are always generated with a restricted duration. After expiration of the validity period the browser will issue a corresponding notification. The dropdown list in the second column allows you to select the desired value. The minimum duration value is 1 week, the maximum duration is 3 years.

Possible values: 1 week, 2 weeks, 1 month, 3 months, 6 months, 1 year, 2 years, 3 years.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

You can **renew a certificate by extending its validity**. Please proceed as follows:

Renewing a Certificate or CSR, respectively, by Extending its Validity

1) In the **Validity** column, move the mouse pointer to the end date of the certificate.

The tooltip text **Renew Certificate** is displayed.

2) Click on the displayed end date.

The **Generate Certificate via CSR** dialog is displayed. The certificate data are already present in the fields. Please take over the existing values unchanged, if possible, and onlyy change the validity period, because changed values need to be verified and confirmed by the Certificate Authority (CA).

Using this method you create a new CSR that you can later send to a CA for signing purposes. The signed certificate can then be imported and activated on the server. The new CSR is automatically turned into a self signed certificate for testing purposes. You may then test and export this self signed certificate in order to send it to the CA.

Password for Private Key

The private key is saved in encrypted format and can only be decrypted and read by providing the password.

NOTICE: Attention: This password is not saved anywhere! Therefore, it has to be entered again when activating this certificate, even if this is done days or months later. Losing the password causes the private key and the certificate to be unusable.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Password Confirmation

Confirming your password avoids typing errors.

Mandatory field.

Mandatory fields are flagged with a red asterisk (*).

Continue (Button)

Use this button to get to the next process step.

After having created a new root certificate the program displays the new root certificate data in the Root Certificate window together with the following message:

"The certificate has been created as displayed below. With this Root Certificate you can now sign externally generated certificate requests."

You may now click on the Sign CSR link in this dialog in order to sign external CSRs with the newly created root certificate.

See also the generic feature description under Root Certificate**.**

3.10.6 Certificate Network Management-> Sign CSR

Sign CSR

Link on Start Page of **Access Management**, and also in **Root Certificate** dialog.

Click on **Sign CSR** to sign an external Certificate Signing Request (CSR) for a system within an OpenScape/HiPath network.

The prerequisite is that you have previously created a self signed Root Certificate of your own.

The aim of this feature is to have all Certificate Signing Requests (CSRs) for all systems within an OpenScape/HiPath 4000 network signed and certified by just one local Certificate Authority (CA) using a self signed root certificate of your own.

If no Root Certificate has been created for this server yet, the following error message will be displayed on the empty screen:

Error : Create Root Certificate first.

In this case you first need to create a new root certificate. Then, click on Sign CSR again. The **Sign Certificate Request (CSR)** dialog opens.

Sign Certificate Request (CSR) (Dialog)

This dialog is displayed when you click on the Sign CSR link on the Start Page of **Access Management** or in the **Root Certificate** dialog.

You can either use Copy&Paste to copy the content of the signed certificate from a text file to the **Paste Certificate Request** dialog area, or import the certificate from a file by clicking on **Browse** and selecting the <filename.csr> file name.

NOTICE: Important: Only BASE64 encoded PKCS#10 requests are accepted. Please make sure to also copy the delimiter lines (BEGIN and END)!

Paste Certificate Request

Display area for content of a signed certificate copied from a text file using Copy&Paste.

You can either use Copy&Paste to copy the content of the signed certificate from a text file to the **Paste Certificate Request** dialog area, or import the certificate from a file by clicking on **Browse** and selecting the <filename.csr> file name.

NOTICE: Important: Only BASE64 encoded PKCS#10 requests are accepted. Please make sure to also copy the delimiter lines (BEGIN and END)!

Or Import Certificate Request from File

Entry field for file name of CSR in the **Sign Certificate Request (CSR)** dialog.

Click on the **Browse** button next to the entry field to open the **File Download** dialog. Select the desired path and file name (e.g. server.csr), and click on **Save**, **not** on **Open**.

Browse (Button)

Button in the **Sign Certificate Request (CSR)** dialog.

You can either use Copy&Paste to copy the content of the signed certificate from a text file to the **Paste Certificate Request** dialog area, or import the certificate from a file by clicking on **Browse** and selecting the <filename.csr> file name.

NOTICE: Important: Only BASE64 encoded PKCS#10 requests are accepted. Please make sure to also copy the delimiter lines (BEGIN and END)!

Password for Private Key of Root Certificate

Entry field in the **Sign Certificate Request (CSR)** dialog.

In the **Sign Certificate Request (CSR)** dialog, enter the **Password for the Private Key** of the root certificate, and click on **Sign Certificate Request**.

Sign Certificate Request (Button)

Once you have entered the **Password for the Private Key** of the root certificate and clicked on the **Sign Certificate Request** button, the program goes back to the **Display Certificate** dialog and displays the detail data of the signed certificate.

Click on **Continue** to go to the next step.

Export signed Certificate into File (Button)

Once you have imported and signed an external CSR you can export it to a file by clicking on **Export signed Certificate into File**.

The **File Download** dialog opens. Click on **Save**, and **not** on **Open** in this dialog.

The file name **server.crt** is automatically entered as default value in the **File Name** field. You can accept this file name or change it to a name of your choice. Save the file to a folder of your choice.

Once the **Download finished** dialog is displayed, click on **Close** to terminate the process.

In the **Sign Certificate Request (CSR)** dialog, click on **Continue**. The program goes back to the initial **Sign Certificate Request (CSR)** dialog, and you can select the next CSR to be signed, or end the process.

You may now import the signed, exported CSR into your web server.

Continue (Button)

Use this button to get to the next process step.

See also the generic feature description under Sign CSR.

3.11 Access Management tab sheet in System Management

engr (Access for Service area)

Enter the password for the **engr** NSL account for service administrators into this field.

The **engr** NSL account is used for remote access of service technicians at expert level for emergency cases.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

rsta (Access for Service area)

Enter the password for the **rsta** NSL account for service administrators into this field.

The **rsta** NSL account is used for remote access of service technicians at upper service level.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

---

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

---

rsca (Access for Service area)

Enter the password for the **rsca** NSL account for service administrators into this field.

The **rsca** NSL account is used for remote access of service technicians at lower service level..

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

---

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

Same value for all service passwords (Access for Service area)

This check box is only displayed if at least 2 fields in this area contain an entry.

Check this box to set one (identical) password for all NSL accounts in the **Access for Service** area.

If this box is checked and you enter a value into the top level editable field in this area, then the values in the other editable fields in this area will automatically be changed as well.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

cusa (Access for Customer area)

The **Access for Customer** area is not displayed on RSP servers.

Enter the password for the **cusa** NSL account for customer administrators into this field.

The **cusa** NSL account is used for remote access of customer security administrators.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

---

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

---

cust (Access for Customer area)

The **Access for Customer** area is not displayed on RSP servers.

Enter the password for the **cust** NSL account for customer administrators into this field.

The **cust** NSL account is used for remote access of standard (cust-level) users.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

---

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

Same value for all customer passwords (Access for Customer area)

This check box is only displayed if at least 2 fields in this area contain an entry.

Check this box to set one (identical) password for all NSL accounts in the **Access for Customer** area.

If this box is checked and you enter a value into the top level editable field in this area, then the values in the other editable fields in this area will automatically be changed as well.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

syst (System Access (Server-Server Communication) area)

Enter the password for the **syst** NSL account for server-server communication into this field.

The **syst** NSL account is used for internal server-server communication of OpenScape 4000 components like System Management, Expert Access/ MPCID, Logging Management.

NOTICE: Important: Setting the password of these accounts avoids illegal access to this server via Network Single Logon (NSL). Communicate the passwords only to administrators of master systems (e.g. OpenScape 4000 Manager or RSP (Remote Service Platform) for remote service access), where access via NSL is accepted from.

See Also

Access for Service area, Access Management tab sheet

Access for Customer area, Access Management tab sheet

System Access (Server-Server Communication) area, Access Management tab sheet

System Accounts and Accounts for Network Single Logon (NSL)

System Accounts List, System Account Administration dialog

Edit menu - System Account Administration

Access Management Security Levels and User Accounts

Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

---

NOTICE: NSL password changes are only valid for the currently selected object! For other objects you need to perform the step of applying the changes in the same way again.

Save (button)

The **Save** button is activated once you enter or change a value in one of the editable fields in the **Access Management** tab sheet in **System Management**.

Clicking on the **Save** button applies and saves the settings and/or changes you made to the NSL passwords. The new or changed passwords become valid at once for all future sessions.

Changes made to other settings in System Management will be saved as well.

Discard (button)

The **Discard** button is activated once you enter or change a value in one of the editable fields in the **Access Management** tab sheet in **System Management**.

Clicking on the **Discard** button revokes the changes made and displays the initial values in the entry fields again.

Changes made to other settings in System Management will be revoked as well.

New (button)

Click the **New** button in the **Access Management** tab sheet in **System Management**, to enter new values for NSL passwords.

Then click the **Save** button to apply your changes and activate the new NSL passwords.

Changes made to other settings in System Management will be saved as well.

Delete (button)

Click the **Delete** button to remove the entries from the fields, allowing you to enter new values.

4 Reference Information

The following topics are covered:

4.1 User Account Administration dialog - User Interface Description

4.1.1 Toolbar Icons - User Account Administration dialog

Reload data from server

Show Help Topics

Show start page

Logoff

Add new user account

Creates a new user account. Same function as **Add** in the **User** menu.

See also Add New User for more details.

Delete selected user account(s)s

Deletes the selected user account(s). Same function as **Delete** in the **User** menu.

See also Delete User Accounts for more details.

Apply modifications for selected user account(s)

The modifications made are applied to the selected user account(s). Same function as **Apply** in the **Edit** menu. See also Edit menu - User Account Administration.

Discard modifications

The modifications made are not applied, but discarded. All entry fields and checkboxes are reset to their initial state. Same function as **Discard** in the **Edit** menu. See also Edit menu - User Account Administration.

Reload data from server

Updates the contents of the **User Account Administration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. Same function as **Reload** in the **Edit** menu. See also Edit menu - User Account Administration.

Show Help Topics

Opens the online help and displays the Help Topics. Same function as **Help Topics** in the **Help** menu. See also Help menu - User Account Administration.

Show start page

Opens a new browser window to display the Start Page of OpenScape 4000 Assistant/Manager, where all applications are listed that the current user is allowed to access. Same function as **Start** in the **View** menu. See also View menu, User Account Administration.

Logoff

Logs you off, closing the current session for all associated browser windows, and brings you back to the Logon screen. Same function as **Logoff** in the **Action** menu. See also Action menu, User Account Administration.

Columns in the User Account Administration dialog

Username	Displays the user account name as entered when adding a new user.
Security Profile	Displays the security profile of the user account: engr, rsca, rsta, cusa or cusa
Certificate name	Displays the certificate name assigned to the user. Matches to the common name written in client certificate of the specific user.
Description	Displays the description of the user as entered into the **Description** field in the **Identification** area.
Max. Password Validity	Displays the current value entered into the **Max. password validity** field in the **Properties** area. The value defines the maximum number of days for a password being valid.
Never Expires	The read-only checkbox in this column displays the current status of the **Password never expires** checkbox in the **Properties** area. If it is turned on (checked) the user password will never become invalid.
Locked	The read-only checkbox in this column displays the current status of the **Lock user account** checkbox in the **Properties** area. If it is turned on (checked) the user cannot log on.
Change Password Allowed	The read-only checkbox in this column displays the current status of the **Allowed to change password** checkbox in the **Properties** area. If it is turned on (checked) the user is allowed to change the own password, i.e. the user has access to the "Change Password" dialog.
Autolock	Displays the current value of the **Lock account automatically** field in the **Autolock** area. This value defines after how many unsuccessful logons the user account will be automatically locked.
Access through Network Single Logon only	For RSP only, a new checkbox Access through Network Single Logon only has been added in the **Properties** area. **Checked** - If this check box is **checked**, the selected user/s can no longer log on directly to the server, but only via NSL from a higher-ranking RSP (SIRA) server. **Unchecked** - If this check box is **unchecked**, the selected user/s can log on directly to the server.

Areas in the User Account Administration dialog

Identification area

User Name	Displays the user account name as entered when adding a new user.
Security Profile	Displays the security profile of the user account: engr, rsca, rsta, cusa or cusa
Certificate name	Input field for the certificate name to be assigned to the user. Must matche the common name written in client certificate of the specific user.
Description	Entry field for a description of the user(s) selected in the left part of the dialog. This entry field accepts alphanumeric and special characters.

Actions area

New password	Entry field for a new password for the user(s) selected in the left part of the dialog. Password entries are case-sensitive. This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).
Retype password	Entry field to retype the new password for the selected user(s). This avoids unwanted typing errors, as passwords are never displayed on the screen.
Delete password	Checkbox to delete the password of the selected user(s). If this checkbox is activated (checked), the **New password** and **Retype password** fields are greyed out. Also, the **Force password change** checkbox will automatically be activated and greyed out. If the existing password is deleted for a user or a set of users, this user or set of users will not need to enter any password when they log on the next time. But since Force password change is always automatically activated together with Delete password, the user(s) who log on will be prompted to enter a new password when they log on.
Force password change	Checkbox used to force a password change. If this checkbox is active, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time. This checkbox is automatically activated if **Delete password** is activated.

Properties area

Max. password validity	Entry field for the maximum number of days for a password being valid. When the password becomes invalid, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time.

Password never expires	Checkbox to define unlimited validity of a password. This property can be turned on or off. If it is turned on (checked) the user password will never become invalid and the entry field **Max. password validity** is deactivated.
Lock user account	Checkbox to lock the selected user(s). This feature can be turned on or off. If it is turned on (checked) the user cannot log on.
Allowed to change password	Checkbox to control access to the **Change Password** dialog. This property can be turned on or off. If it is turned on (checked) the user is allowed to change the own password, i.e. the user has access to the **Change Password** dialog.
Access through Network Single Logon only	For RSP only, a new checkbox Access through Network Single Logon only has been added in the **Properties** area. **Checked** - If this check box is **checked**, the selected user/s can no longer log on directly to the server, but only via NSL from a higher-ranking RSP (SIRA) server. **Unchecked** - If this check box is **unchecked**, the selected user/s can log on directly to the server.

Autolock area

Lock account automatically	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the number of unsuccessful logons after which the account will automatically be locked. Possible values: Never; 1 to 15 (max.) unsuccessful logons.
occurring during	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period within which the unsuccessful logons must happen to activate the automatic locking of the account. Possible values: any time; 30 seconds to (max.) 1 week.
Unlock it automatically	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period after which the locked account will be unlocked. Possible values: Never; 30 seconds to (max.) 1 month.

Controls and Buttons in the User Account Administration dialog

Apply	The modifications made in the areas above are applied to the selected user account(s). Same function as **Apply** in the **Edit** menu. See Edit menu - User Account Administration.

Discard	The modifications made in the areas above are not applied, but discarded. All entry fields and checkboxes are reset to their initial state. Same function as **Discard** in the **Edit** menu. See Edit menu - User Account Administration.

4.2 System Account Administration dialog - User Interface Description

4.2.1 Toolbar Icons - System Account Administration dialog

Apply modifications for selected user account

The modifications made are applied to the selected user account(s). Same function as **Apply** in the **Edit** menu. See also Edit menu - System Account Administration.

Discard modifications

The modifications made are not applied, but discarded. All entry fields and checkboxes are reset to their initial state. Same function as **Discard** in the **Edit** menu. See also Edit menu - System Account Administration.

Reload data from server

Updates the contents of the **System Account Administration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. Same function as **Reload** in the **Edit** menu. See also Edit menu - System Account Administration.

Show Help Topics

Opens the online help and displays the Help Topics. Same function as **Help Topics** in the **Help** menu. See also Help menu - System Account Administration.

Show start page

Opens a new browser window to display the Start Page of OpenScape 4000 Assistant/Manager, where all applications are listed that the current user is allowed to access. Same function as **Start** in the **View** menu. See also View menu, System Account Administration.

Logoff

Logs you off, closing the current session for all associated browser windows, and brings you back to the Logon screen. Same function as **Logoff** in the **Action** menu. See also Action menu, System Account Administration.

Columns in the System Account Administration dialog

User Name	Displays the user account name.
Description	Displays the description of the user account.
Max. Password Validity	Displays the current value entered into the **Max. password validity** field in the **Properties** area. The value defines the maximum number of days for a password being valid.
Never Expires	The read-only checkbox in this column displays the current status of the **Password never expires** checkbox in the **Properties** area. If it is turned on (checked) the user password will never become invalid.
Locked	The read-only checkbox in this column displays the current status of the **Lock user account** checkbox in the **Properties** area. If it is turned on (checked) the user cannot log on.
Change Password Allowed	The read-only checkbox in this column displays the current status of the **Allowed to change password** checkbox in the **Properties** area. If it is turned on (checked) the user is allowed to change the own password, i.e. the user has access to the "Change Password" dialog.
Autolock	Displays the current value of the **Lock account automatically** field in the **Autolock** area. This value defines after how many unsuccessful logons the user account will be automatically locked.

Areas in the System Account Administration dialog

Identification area

User Name	Displays the user account name.
Description	Displays the description of the user.

Actions area

New password	Entry field for a new password for the user(s) selected in the left part of the dialog. Password entries are case-sensitive. This entry field accepts alphanumeric and special characters. Min. length is 6 characters, max. length is 16 characters. The password must contain at least one special character (neither digit nor letter).
Retype password	Entry field to retype the new password for the selected user(s). This avoids unwanted typing errors, as passwords are never displayed on the screen.
Delete password	Checkbox to delete the password of the selected user(s). If this checkbox is activated (checked), the **New password** and **Retype password** fields are greyed out. Also, the **Force password change** checkbox will automatically be activated and greyed out. If the existing password is deleted for a user or a set of users, this user or set of users will not need to enter any password when they log on the next time. But since Force password change is always automatically activated together with Delete password, the user(s) who log on will be prompted to enter a new password when they log on. This checkbox is not available for system accounts and NSL accounts: they must always have a password set.

Force password change	Checkbox used to force a password change. If this checkbox is active, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time. This checkbox is automatically activated if **Delete password** is activated. This checkbox is not available for system accounts and NSL accounts: forced password change is only supported for interactive logons.

Properties area

Max. password validity	Entry field for the maximum number of days for a password being valid. When the password becomes invalid, the system will force a password change prompting the user(s) to enter a new password when they try to log on the next time. This entry field is not available for system accounts and NSL accounts: forced password change is only supported for interactive logons.
Password never expires	Checkbox to define unlimited validity of a password. This property can be turned on or off. If it is turned on (checked) the user password will never become invalid and the entry field **Max. password validity** is deactivated. This checkbox is always checked for system accounts and NSL accounts.
Lock user account	Checkbox to lock the selected user(s). This feature can be turned on or off. If it is turned on (checked) the user cannot log on.

Autolock area

Lock account automatically	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the number of unsuccessful logons after which the account will automatically be locked. Possible values: Never; 1 to 15 (max.) unsuccessful logons.

occurring during	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period within which the unsuccessful logons must happen to activate the automatic locking of the account. Possible values: any time; 30 seconds to (max.) 1 week.
Unlock it automatically	Entry field in the **Autolock** area, **User Account Administration** and **System Account Administration** dialog. Click on the dropdown list in this field to select the time period after which the locked account will be unlocked. Possible values: Never; 30 seconds to (max.) 1 month.

Controls and Buttons in the System Account Administration dialog

Apply	The modifications made in the areas above are applied to the selected user account(s). Same function as **Apply** in the **Edit** menu. See Edit menu - System Account Administration.
Discard	The modifications made in the areas above are not applied, but discarded. All entry fields and checkboxes are reset to their initial state. Same function as **Discard** in the **Edit** menu. See Edit menu - System Account Administration.

4.3 Access Right Configuration dialog - User Interface Description

4.3.1 Toolbar Icons - Access Right Configuration dialog

Assign group(s) to selected user account(s)

Assigns the access right group(s) selected in the right area to the user(s) selected in the left area. Same function as **Assign** in the **Edit** menu. See also Edit menu - Access Right Configuration.

You can also use the Context Menu or the Toolbar to execute this command.

Withdraw group(s) from selected user account(s)

Removes access right group(s) selected in the left area from the associated user(s). Same function as **Withdraw** in the **Edit** menu.

You can also use the Context Menu or the Toolbar to execute this command.

Note: The **Withdraw** command is only executed after an additional security prompt and confirmation.

See also Edit menu - Access Right Configuration.

Replace groups of selected user account(s)

Select the required user(s) in the left hand side area, and the access right groups that should replace the existing access right groups in the right hand side area. Click on **Replace** in the **Edit** menu to replace the previously assigned access right groups with the currently selected access right groups. The previously assigned access right groups will be overwritten during this process. Difference to **Assign**: In the case of **Assign** the newly selected access right groups are appended (added) to the already existing assigned access right groups, which are not overwritten. Alternative ways to execute this command: Via the Context Menu or the Toolbar.

NOTICE: The **Replace** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Withdraw all groups from selected user account(s)

In the left hand side area, select the user(s) to which you want to apply this command. Click on **Withdraw All** in the **Edit** menu to withdraw all assigned access rights from the selected user(s). Alternative ways to execute this command: Via the Context Menu or the Toolbar. **Note:** The **Withdraw All** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Reload data from server

Updates the contents of the **Access Right Configuration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. Same function as **Reload** in the **Edit** menu. See also Edit menu - Access Right Configuration.

Show Help Topics

Opens the online help and displays the Help Topics. Same function as **Help Topics** in the **Help** menu. See also Help menu - Access Right Configuration.

Show start page

Opens a new browser window to display the Start Page of OpenScape 4000 Assistant/Manager, where all applications are listed that the current user is allowed to access. Same function as **Start** in the **View** menu. See also View Menu - Access Right Configuration.

Logoff

Logs you off, closing the current session for all associated browser windows, and brings you back to the Logon screen. Same function as **Logoff** in the **Action** menu. See also Action menu, Access Right Configuration.

Areas and Preview Panes in the Access Right Configuration dialog

Areas

Users (left hand side area)

Shows a two-level tree containing all users (first level) and all access right groups assigned to the users (second level). Each user is represented by a folder. Each folder contains the access right groups assigned to the user. Each user folder can be opened to view the access right groups assigned to it. See also Access Right Configuration, Assigning/Withdrawing Access Right Groups To/From Users, and Preview Panes - Access Right Configuration.

Access Right Groups (right hand side area)

Shows all available access right groups that can be assigned to a user. See also Access Right Configuration, Assigning/Withdrawing Access Right Groups To/From Users, and Preview Panes - Access Right Configuration.

Preview Panes

Both areas of the **Access Right Configuration** dialog have a small **Preview Pane** attached at the bottom. The Preview Panes - Access Right Configuration list all access rights that are currently part of the selected access right group. If - in the left hand area - a user is selected instead of an access right group, the preview pane on the left hand side lists all access rights currently assigned to this user. The Preview Panes can be shown and hidden, respectively, using the **Show Access Right Preview Panes** option in the View Menu - Access Right Configuration. See also Access Right Configuration dialog - User Interface Description, Assigning/Withdrawing Access Right Groups To/From Users, and Preview Panes - Access Right Configuration.

Access Rights of the Selected User (preview pane on left hand side)

Shows the list of access rights assigned to a user.

Access Rights of the Selected Access Right Group (preview pane on right hand side)

Shows the list of access rights within the selected access right group.

4.4 Access Right Group Configuration dialog - User Interface Description

Toolbar Icons - Access Right Group Configuration dialog

Areas and Preview Panes in the Access Right Group Configuration dialog

4.4.1 Toolbar Icons - Access Right Group Configuration dialog

Create a new access right group

Copy the selected access right group to a new one

Rename the selected access right group

Remove the selected access right group

Assign access rights to selected group(s)

Withdraw access rights from selected group(s)

Replace access rights of selected group(s)

Withdraw all access rights from selected group(s)

Reload data from server

Display/Hide predefined access right groups

Display/Hide manually created access right groups

Display/Hide access right groups for dynamic applications

Display access rights as a component tree

Display access rights as an application tree

Show Help Topics

Show start page

Logoff

Create a new access right group

Opens the dialog Add new group. Same function as **Add new group** in the **Group** menu. See Edit menu - User Account Administration.

Copy the selected access right group to a new one

Opens the dialog Copy the selected access right group. Same function as **Copy selected group** in the **Group** menu. See Edit menu - User Account Administration.

Rename the selected access right group

Opens the dialog Rename the selected access right group. Same function as **Rename selected group** in the **Group** menu. See Edit menu - User Account Administration.

Remove the selected access right group

Deletes the selected access right group(s). Same function as **Delete selected groups** in the **Group** menu. See Edit menu - User Account Administration.

Assign access rights to selected group(s)

The access right(s) selected in the right area are assigned to the access right group(s) selected in the left area. Same function as **Assign access rights** in the **Edit** menu. See Edit menu - User Account Administration.

Withdraw access rights from selected group(s)

The access right(s) selected in the left area are withdrawn from the associated access right group(s). Same function as **Withdraw access rights** in the **Edit** menu. See Edit menu - User Account Administration.

Replace access rights of selected group(s)

Select the batch of manually created access right groups (this feature only works with MANUALLY CREATED access right groups) in the left hand side area, and the batch of individual access rights or higher-ranking folders in the right hand side area. Click on **Replace Access Rights** in the **Edit** menu to replace the previously assigned access rights with the currently selected access rights. The previously assigned access rights will be overwritten during this process. Difference to **Assign**: In the case of **Assign** the newly selected access rights are appended (added) to the already existing assigned access rights, which are not overwritten. Alternative ways to execute this command: Via the Context Menu or the Toolbar.

NOTICE: The **Replace Access Rights** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Withdraw all access rights from selected group(s)

Select the batch of manually created access right groups (this feature only works with MANUALLY CREATED access right groups) in the left hand side area. You can hide the other categories of access right groups, thus only displaying the manually created access right groups. Click on **Withdraw All Access Rights** in the **Edit** menu to withdraw all assigned access rights from the selected access right group(s). Alternative ways to execute this command: Via the Context Menu or the Toolbar.

NOTICE: The **Withdraw All Access Rights** command is only executed after you explicitly confirm the action a second time, as requested by the system security prompt issued.

Reload data from server

Updates the contents of the **Access Right Group Configuration** dialog by loading the current data from the server and displaying the recently applied changes of concurrent administrator sessions. Same function as **Reload** in the **Edit** menu. See Edit menu - User Account Administration.

Display/Hide predefined access right groups

Turns the display of predefined access right groups on and off. Same function in **View** menu. See also View menu - Access Right Group Configuration.

Display/Hide manually created access right groups

Turns the display of manually created access right groups on and off. Same function in **View** menu. See also View menu - Access Right Group Configuration.

Display/Hide access right groups for dynamic applications

Turns the display of access right groups for dynamic applications on and off. Same function in **View** menu. See also View menu - Access Right Group Configuration.

Display access rights as a component tree

Displays the access rights below the components they belong to, hiding the corresponding applications. Same function as **Access Rights - Show Component Tree** in **View** menu. See also View menu - Access Right Group Configuration.

Display access rights as an application tree

Displays the access rights below the corresponding applications. (Available components may consist of more than one application offered in the user's start page.) Same function as **Access Rights - Show Application Tree** in **View** menu. See also View menu - Access Right Group Configuration.

Show Help Topics

Opens the online help and displays the Help Topics. Same function as **Help Topics** in the **Help** menu. See also Help menu - Access Right Group Configuration. Â¨

Show start page

Opens a new browser window to display the Start Page of OpenScape 4000 Assistant/Manager, where all applications are listed that the current user is

allowed to access. Same function as **Start** in the **View** menu. See also View menu - Access Right Group Configuration.

Logoff

Logs you off, closing the current session for all associated browser windows, and brings you back to the Logon screen. Same function as **Logoff** in the **Action** menu. See also Action menu, Access Right Group Configuration.

Areas and Preview Panes in the Access Right Group Configuration dialog

Access Right Groups tree (left hand side area)	Displays a two-level tree containing all available access right groups (ARGs, first level) and their assigned access rights (second level).
Access Rights - Component/Application Tree (right hand side area)	Displays a tree showing all access rights that can be assigned to manually created access right groups. You can toggle between two view modes: **Component Tree** and **Application Tree**.
Information on Access Right - (preview panes, left and right hand side area)	Displays a short description of the currently selected access right.

The **Preview Panes** at the bottom of the two dialog areas can be shown and hidden, respectively, by activating or deactivating the **Display Info on Access Right** option in the View menu - Access Right Group Configuration.

4.5 Error Messages displayed in case of Incorrect NSL Logon and Locked NSL Accounts

When logging on to a system using an NSL account, error messages are displayed in the following situations:

No permission (access right not assigned) for Network Single Logon (NSL)

Password for NSL access level is incorrect

NSL level is locked

NSL level is locked automatically

Account on target server does not exist

Internal error during automatic logon

Error when connecting to target server

Internal system error on target server

The error messages are self-explanatory.

No permission (access right not assigned) for Network Single Logon (NSL)

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: You don't have the permission for Network Single Logon.
Automatic logon to a target server is denied, if the access right for *Network Single Logon* is not assigned.
Please contact your system administrator to add this access right to your account.

Password for NSL access level is incorrect

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: The password for the NSL level is incorrect.
Automatic logon to a target server is denied, if the transmitted password (aka secret) and that one configured for this NSL level at the target server do not match.
Please contact your system administrator to configure the correct password in System Management.

NSL level is locked

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: The NSL level is locked.
Automatic logon is denied, if the associated NSL level is locked at the target server.
Please contact your system administrator to unlock NSL access at the target server.

NSL level is locked automatically

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: The NSL level has been locked automatically.
Automatic logon is denied, if the associated NSL level is locked automatically at the target server.
This happens, if a wrong NSL secret is used too often at the target server.

Account on target server does not exist

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: The account on the target server does not exist.
Automatic logon to a target server is denied, if the associated account does not exist on the target server.
Please contact your system administrator to create and configure this account at the target server.

This situation will normally only happen only when accessing from SIRA to the RSP or to the Manager.

It is, however, possible to configure an arbitrary system (e.g. an Assistant) in such a way that it only accepts NSL logons if the corresponding profile (in this example the account 'mark') exists on the target system.

Internal error during automatic logon

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

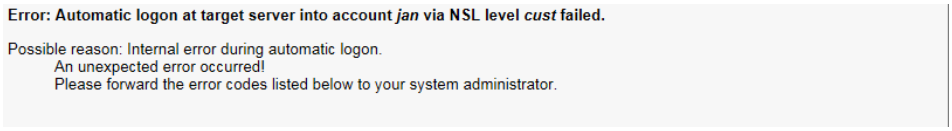
Possible reason: Internal error during automatic logon.
An unexpected error occurred!
Please forward the error codes listed below to your system administrator.

Error when connecting to target server

Error: Automatic logon at target server into account *jan* via NSL level *cust* failed.

Possible reason: Internal error during automatic logon.
An unexpected error occurred!
Please forward the error codes listed below to your system administrator.

Internal system error on target server



Index

K

L

M

N

O

P

R

S

T

U

V

W