A MITEL
PRODUCT
GUIDE

Unify OpenScape 4000 Assistant/Manager

Access Management

Administratordokumentation
10/2025

A31003-H34B0-M121-03-00A9

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.

Inhalt

1 Zugangsverwaltung – Übersicht

In diesem Abschnitt werden folgende Themen behandelt:

Siehe auch

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

1.1 Einführung

Die Zugangsverwaltung ist die Zugriffssteuerungskomponente für OpenScape 4000-Server. Diese Komponente bestimmt, welche Benutzer auf einen bestimmten Server zugreifen dürfen und welche Anwendungen oder Zugriffsrechte diese Benutzer nutzen können. Mögliche Benutzergruppen sind Kundenadministratoren und Servicetechniker, deren Aufgabe es ist, die OpenScape-Systeme zu verwalten.

Für diese Benutzer richtet die Zugangsverwaltung Benutzerkennungen (Accounts) ein und verwaltet alle zugehörigen Passwörter, Passwort-Attribute sowie sonstige kennungsbezogene Daten. Ferner überwacht die Zugangsverwaltung den Benutzerzugang via Web-Browser und ermöglicht das Verwalten von Web-Server-Zertifikaten

Weitere Leistungsmerkmale der Zugangsverwaltung:

- **Sitzungsverwaltung (Session Management)**
  - Kontrolle bzw. Überwachung aller momentan angemeldeten Benutzer.
  - Web-Sitzungen werden nach einer frei definierbaren Zeitspanne ohne Benutzeraktivität automatisch beendet.
  - Web-Sitzungen können außerdem explizit über die Schaltfläche **Abmelden** oder den Web Session Manager beendet werden.
- **Netzwerk-Einzelanmeldung (Network Single Logon, NSL)**
  - Benutzer brauchen sich nur einmalig bei einem OpenScape 4000-Netzwerkserver anzumelden und können anschließend ohne weitere Authentifizierung auf alle angeschlossenen OpenScape 4000-Systeme zugreifen.
  - Die Verwaltung der Sicherheitsfunktionalität und Zugriffssicherung erfolgt über die NSL-Passwort-Konfiguration sowie eine zweckentsprechende Zugriffsrecht-Konfiguration auf den OpenScape 4000-Systemen.
- **Integration von Windows(TM) Client/Server-Programmen**
  - Windows(TM)-Programme sind ebenfalls in das OpenScape 4000-Authentifizierungs- und Sitzungskonzept integriert.

    Zwei Verfahren werden angeboten:
  - Integration in die Startseite von OpenScape 4000 Assistant/Manager: Ausführung des Windows(TM)-Clients im Anschluss an die web-basierte Authentifizierung über die Startseite von OpenScape 4000 Assistant/Manager
  - Einsatz einer von der Zugangsverwaltung bereitgestellten Authentifizierungsbibliothek (kein Browser für Anmeldung erforderlich)

- **Emergency Password Reset (EPR)**
  - Mit Emergency Password Reset (EPR) kann das Passwort des Administrators (Benutzer "engr") zurückgesetzt werden, falls es verloren gegangen ist oder Systemfehler vorliegen.
- **Konfiguration für Passwortchronik**
  - Im Dialogfenster Password History Configuration können erweiterte Passwort-Regeln festgelegt werden.
- **Steuerung/Kontrolle der Systemkennungen**
  - Aus technischen Gründen richten OpenScape 4000-Server eine vordefinierte Gruppe von Linux-Accounts für verschiedene interne Anwendungen ein (beispielsweise für den Datenbankzugang mit bestimmten Zugriffsrechten bzw., um die Anbindung eventuell angeschlossener Systeme zu ermöglichen).
  - Die Zugriffssteuerung für diese Systemkennungen kann auch über die Zugangsverwaltung erfolgen. Eine detaillierte Liste der Systemkennungen finden Sie in Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen.
- **Verwalten von Web-Server-Zertifikaten (ab Version 2.0)**
  - Erstellen von Zertifikatsanforderungen (CSRs) für SSL-Sicherheitszertifikate.
  - Generieren, Aktivieren und Importieren von SSL-Sicherheitszertifikaten für den aktuellen Server.
  - Generieren, Aktivieren und Importieren von SSL-Sicherheitszertifikaten für die Netzverwaltung.

1.2 Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Folgende Themen werden hier behandelt:

Sicherheitsebenen und vordefinierte Benutzerkennungen

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Siehe auch

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

1.2.1 Sicherheitsebenen und vordefinierte Benutzerkennungen

Die Zugangsverwaltung unterstützt fünf verschiedene **Sicherheitsebenen**.

Jeder Benutzer, der sich bei einem OpenScape 4000-Server anmeldet, wird einer dieser Ebenen zugeordnet.

Bei vier dieser Sicherheitsebenen werden vordefinierte Benutzerkennungen mit Vorgabe-Passwörtern eingerichtet, um einen sofortigen Zugang auf den OpenScape 4000-Server zu ermöglichen.

Aus Sicherheitsgründen muss das Vorgabe-Passwort geändert werden, sobald sich der Benutzer erstmalig anmeldet.

Die nachfolgende Tabelle bietet einen Überblick über die verschiedenen Sicherheitsebenen und vordefinierten Benutzerkennungen der Zugangsverwaltung.

Sicherheitsebenen

Sicherheit	Vordefinierte Benutzerkennung	Initialen Kennwort	Linux-Shell-Zugang	Eigentür	Anmerkungen
engr 	engr(1)	4K-admin	ja	Dienst	Engineer (umfassende Systemverwaltungsprivilegien für "Techniker"). Kommt nur in Notfällen zur Anwendung. Umfasst alle anderen Sicherheitsebenen. Nur auf dem Assistant: Zugang zur Linux-Shell mit Superuser-Rechten (uid 0).
rsta 	rsta	4K-admin	ja	Dienst	Remote Service Technical Assistance (eingeschränkte Systemverwaltungsprivilegien). Für "Upper Level"-Servicetechniker. Enthält die Sicherheitsebene rsca.
rsca 	rsca	4K-admin	ja	Dienst	Remote Service Customer Assistance (eingeschränkte Systemverwaltungsprivilegien). Für "Lower Level"-Servicetechniker.
cusa 	cusa	c.u.s.a	nein	Kunde	CUstomer Security Adminstrator (eingeschränkte Systemverwaltungsprivilegien für "Kundensicherheitsadministratoren"). Für "Master"-Administratoren auf der Kundenseite. Enthält die Sicherheitsebene cust.
cust 	--	--	nein	Kunde	CUSTomer (Standardbenutzer). Individuelle Kennungen für die jeweilige Kundenumgebung können zur Laufzeit eingerichtet werden.

(1) Nur auf dem Assistant: Standardmäßig ist die Anmeldung als root gesperrt und kann nur über engr freigegeben werden.

Verwandte Themen

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Systemkennungen

Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

1.2.2 Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Zusätzlich zu den vordefinierten Kennungen für interaktive Anmeldung verwaltet die Zugangsverwaltung zwei weitere Arten von Kennungen, die nicht für interaktive Anmeldung verwendet werden:

- Systemkennungen

und

- Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Diese beiden Kennungstypen sind in den nachstehenden Tabellen dargestellt und beschrieben.

Systemkennungen

Kennung / Kategorie	Symbol	Beschreibung
Systemkennungen		
syst		Linux-Kennungen für verschiedene Einsatzbereiche. Über diese Kennungen wird die korrekte Funktion der OpenScape 4000-Leistungsmerkmale und die Kommunikation zu den Partnersystemen sichergestellt. Diese Kennungen werden nicht für interaktive Anmeldung verwendet.

Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Kennung / Kategorie	Symbol	Beschreibung
Netzwerk-Einzelanmeldung (Network Single Logon, NSL) Kennungen		Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.
nsl-syst		Systemebene - für die interne Server-Server-Kommunikation von OpenScape 4000-Komponenten wie z.B. Systemverwaltung, OpenScape 4000 Expert Access/MPCID, Logging Management.
nsl-engr		Netwerkeinzelanmeldung für den Fernzugriff von Servicetechnikern auf Expertenebene für Notfallsituationen (engr).
nsl-rsta		Netwerkeinzelanmeldung für den Fernzugriff von "Upper level" Servicetechnikern (rsta).
nsl-rsca		Netwerkeinzelanmeldung für den Fernzugriff von "Lower level" Servicetechnikern (rsca).
nsl-cusa		Netwerkeinzelanmeldung für den Fernzugriff von Kundensicherheitsadministratoren (cusa).

Kennung / Kategorie	Symbol	Beschreibung
nsl-cust		Netwerkeinzelanmeldung für den Fernzugriff von Standardbenutzern (cust-Ebene).

Verwandte Themen

Systemkennungen

Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2 Funktionalität

In diesem Abschnitt werden folgende Themen behandelt:

2.1 Zugriffssteuerung für Server und Anwendungen

Die Zugangsverwaltung gewährleistet, dass sich jeder Benutzer mit einer gültigen Kennung und gültigem Passwort bei einem OpenScape 4000-Server anmelden muss. Bei erfolgreicher Anmeldung wird eine Sitzung eingerichtet. Im Rahmen einer Sitzung kann der Benutzer nur OpenScape 4000-Anwendungen nutzen, die in seinem Benutzerprofil vereinbart wurden. Die Anwendung **Zugangsverwaltung** selbst unterliegt ebenfalls dieser Zugriffssteuerung. So sind beispielsweise Benutzer mit **rsca-, cusa-** oder höheren Zugriffsrechten berechtigt, das Leistungsmerkmal **Kennungsverwaltung** zu nutzen.

Bereich Sitzungsverwaltung

Der Bereich **Sitzungsverwaltung** umfasst folgende Leistungsmerkmale:

- Passwort ändern

  Standardmäßig ist jeder Benutzer berechtigt, sein Passwort mit der Funktion Passwort ändern zu ändern. Falls erforderlich, kann ein Benutzer mit höherer Berechtigungsebene die Berechtigung eines Benutzers, sein Passwort zu ändern, auch wieder sperren, um bestimmte Passwörter unverändert beizubehalten.

- Passwortverteilung (nur OpenScape 4000 Manager)

  Diese zusätzliche **Passwort ändern** Funktion für den Manager ermöglicht das einfache Verwalten und Verteilen von Passwörtern einzelner Benutzer vom Manager aus. Es kann nicht nur das Passwort des aktuellen Benutzers am Manager geändert werden, sondern auch auf allen ausgewählten Assistants.
- Web Session Manager

  Der Web Session Manager dient zum Verwalten und Löschen von laufenden Sitzungen auf dem Server. Je nach Berechtigungsebene werden dem angemeldeten Benutzer auch Sitzungen anderer Benutzer mit niedrigeren Berechtigungsebenen angezeigt. Hauptaufgabe des Session Managers ist das Löschen von verwaisten Sitzungen, die noch nicht abgelaufen sind. Eine Sitzung wird als verwaist bezeichnet, wenn z. B. ein Benutzer alle Browser-Fenster schließt, ohne sich explizit abzumelden.
- Emergency Password Reset (EPR)

  Mit Emergency Password Reset (EPR) kann das Passwort des Administrators (Benutzer "engr") zurückgesetzt werden, falls es verloren gegangen ist oder Systemfehler vorliegen.
- Im Dialogfenster Passwort-Einstellungen können erweiterte Passwort-Regeln aktiviert und konfiguriert werden.

Bereich "Kennungsverwaltung"

Der Bereich "Kennungsverwaltung" ist nur für Benutzer mit **rsca**-, **cusa**- oder höheren Zugriffsrechten freigegeben. Dieser Bereich umfasst folgende Leistungsmerkmale:

- Benutzerkennungsverwaltung

  Erstellen oder Löschen von Kennungen einzelner Benutzer und Verwalten ihrer Passwort-Eigenschaften.
- Systemkennungsverwaltung

  Ändern der Passwort-Eigenschaften von OpenScape 4000-Server-Systemkennungen, vordefinierten Administratorkennungen und Netzsicherheitsebenen (Network Security Levels, NSL).
- Zugriffsrechtekonfiguration

  Zuweisen oder Verweigern von Zugriffsrechten bzw. Zugriffsrechtegruppen für bestimmte Benutzer, und somit Erstellung individueller Benutzerprofile.
- Zugriffsrechtegruppen-Konfiguration

  Erstellung und Verwaltung von Zugriffsrechtegruppen durch Zuordnen individueller Anwendungszugriffsrechte zu diesen Gruppen.
- Export von Benutzerdaten

  Anzeige der aktuellen Benutzer- und Zugriffsrechtekonfigurationsdaten vom Server in einer HTML-Datei. Exportieren der angezeigten Daten in eine Textdatei. Übernahme der Daten in ein Tabellenkalkulationsprogramm zur weiteren Bearbeitung oder Auswertung.

Der Bereich "Verwalten von Web-Server-Zertifikaten"

- Erstellen von Zertifikatsanforderungen (CSRs) für SSL-Sicherheitszertifikate.
- Generieren, Aktivieren und Importieren von SSL-Sicherheitszertifikaten für den aktuellen Server.

- Generieren, Aktivieren und Importieren von SSL-Sicherheitszertifikaten für die Netzverwaltung.

Eine Übersicht über die Leistungsmerkmale der **Zugangsverwaltung** finden Sie unter Zugangsverwaltung – Übersicht on page 7.

Verwandte Themen

Benutzeroberfläche der Zugangsverwaltung page 19

Einführung page 7

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen page 10

Registerkarte "Zugangsverwaltung" in der Systemverwaltung page 237

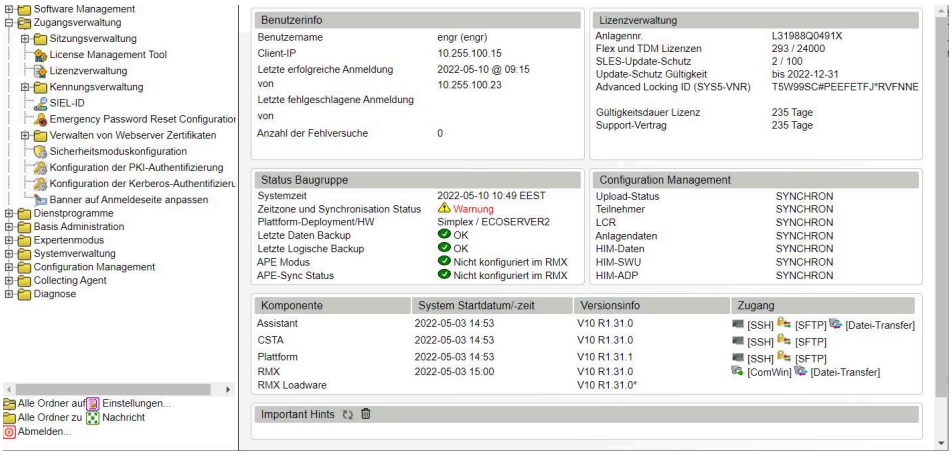
Siehe auch

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.2 Benutzeroberfläche der Zugangsverwaltung

Nach der Anmeldung beim Web-Server werden die Hauptfunktionsbereiche der Zugangsverwaltung auf der **Startseite** von **OpenScape 4000 Assistant/Manager** (im Folgenden kurz **Startseite** genannt) in Form eines Anwendungsbaums angezeigt. Wenn Sie im Anwendungsbaum auf einen Link klicken, wird das zugehörige Dialogfeld der Zugangsverwaltung aufgerufen. Die Startseiten von **OpenScape 4000 Assistant** und **OpenScape 4000 Manager** unterscheiden sich etwas in den Inhalten des Applikationsbaumes, nicht aber in der Funktionalität. Auf der Startseite werden nur diejenigen Applikationen angezeigt, für die Sie als angemeldeter Benutzer aufgrund Ihrer erworbenen Lizenz und Ihrer Zugriffsrechte über die entsprechenden Berechtigungen verfügen.

OpenScape 4000 Assistant-Startseite



Beschreibung der Benutzeroberfläche

Beschreibungen der Symbole, Steuerelemente und sonstigen Elemente der Benutzeroberfläche der **Zugangsverwaltung** finden Sie unter folgenden Links:

Inhalt der Startseite von OpenScape 4000 Assistant/Manager

Symbolleiste

Menüleiste

Kontextmenü

Web Session Manager

Passwort ändern

Passwortverteilung (nur OpenScape 4000 Manager)

Emergency Password Reset (EPR)

Konto- und Passwort-Einstellungen

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung"

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Verwandte Themen

Benutzerkennungsverwaltung

Systemkennungsverwaltung

Zugriffsrechtekonfiguration

Zugriffsrechtegruppen-Konfiguration

Export von Benutzerdaten

Bereich "Verwalten von Web-Server-Zertifikaten"

Registerkarte "Zugangsverwaltung" in der Systemverwaltung

Einführung

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Zugriffssteuerung für Server und Anwendungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.2.1 Inhalt der Startseite von OpenScape 4000 Assistant/Manager

Der Anwendungsbaum auf der **Startseite** enthält alle lizenzierten Anwendungen (von Benutzer erworbene Anwendungen), zu deren Benutzung der Anwender berechtigt ist. Damit grundsätzlich eine Lizenzüberprüfung

durchgeführt wird, wird für jede Anwendung eine Lizenz-ID gespeichert. (Diese Kennung muss registriert werden, bevor der Benutzer sie verwenden kann.) Für einige Anwendungen - beispielsweise für die Anwendungen in der Gruppe **Expertenmodus** (OpenScape 4000 Assistant) bzw. **Direktzugang** (OpenScape 4000 Manager) - ist keine Registrierung erforderlich.

Die **Startseite** erhält von der Lizenzverwaltung alle registrierten Anwendungen, und von der Zugangsverwaltung alle Anwendungen, zu deren Nutzung der Benutzer berechtigt ist. Auf Grundlage dieser Informationen sind im Anwendungsbaum nur die Anwendungen sichtbar, die lizenziert sind und mit denen zu arbeiten der Benutzer befugt ist. Wenn eine Anwendung ein Netzobjekt benötigt, muss mindestens eine Instanz des erforderlichen Netzobjekttyps im System vorhanden sein.

Folgende Bereiche werden im Anwendungsbaum der Zugangsverwaltung auf der Startseite von OpenScape 4000 Assistant/Manager angezeigt:

Bereich "Kennungsverwaltung"

Bereich Sitzungsverwaltung

Lizenzverwaltung

Bereich "Verwalten von Web-Server-Zertifikaten"

2.2.1.1 Lizenzverwaltung

Die Lizenzverwaltung (License Management) ist eine separate Software-Komponente mit eigener Online-Hilfe.

Verwandte Themen

Inhalt der Startseite von OpenScape 4000 Assistant/Manager

Symbolleiste

Menüleiste

Benutzeroberfläche der Zugangsverwaltung

2.2.1.2 Bereich Sitzungsverwaltung

Der Bereich **Sitzungsverwaltung** (Session Management) unterstützt folgende Leistungsmerkmale:

- Passwort ändern
- Passwortverteilung (nur OpenScape 4000 Manager)
- Web Session Manager
- Emergency Password Reset (EPR)
- Konto- und Passwort-Einstellungen

2.2.1.3 Bereich "Kennungsverwaltung"

Der Bereich **Kennungsverwaltung** ist in folgende Funktionsbereiche unterteilt:

- Benutzerkennungsverwaltung
- Systemkennungsverwaltung
- Zugriffsrechtekonfiguration
- Zugriffsrechtegruppen-Konfiguration
- Export von Benutzerdaten

2.2.1.4 Bereich "Verwalten von Web-Server-Zertifikaten"

Der Bereich **Verwalten von Web-Server-Zertifikaten** umfasst folgende Funktionsbereiche:

- Zertifikate für diesen Web-Server
  - Aktivieren - Bei NICHT INSTALLIERTER HG35xx-Baugruppe
  - Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant
  - Generieren
  - Import
  - Über CSR generieren
- Zertifikate für Netzverwaltung
  - Stammzertifikat
  - CSR signieren

2.2.2 Symbolleiste

Die Symbolschaltflächen in der **Symbolleiste** haben die gleichen Funktionen wie die entsprechenden Einträge in den Menüs. Beschreibungen der einzelnen Symbolschaltflächen finden Sie bei den einzelnen Komponenten, und zwar unter:

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung",

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung",

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration",

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

2.2.3 Menüleiste

Die **Menüleiste** wird bei allen Leistungsmerkmalen des Bereichs **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**, wo es keine Menüleiste gibt.

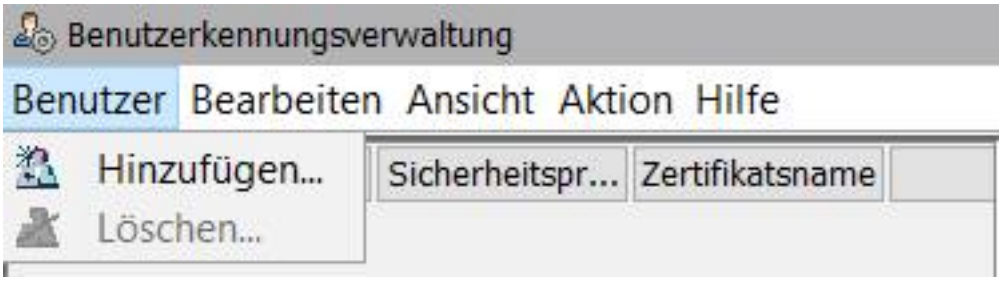
Der Inhalt der **Menüleiste** kann unterschiedlich sein. Je nachdem, welche Funktion und Komponente Sie gewählt haben, werden unterschiedliche Menüs angezeigt.

Die Menüs **Bearbeiten**, **Ansicht**, **Aktion** und **Hilfe** werden bei allen Leistungsmerkmalen des Bereichs **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**, wo es keine Menüleiste gibt.

Die Komponenten des Bereichs **Sitzungsverwaltung** haben keine Menüleiste.

Menü Benutzer

Das Menü Benutzer erscheint nur im Dialogfeld Benutzerkennungsverwaltung.



Das Menü "Bearbeiten"

Das Menü "Bearbeiten" enthält - je nach Software-Komponente - unterschiedliche Optionen. Siehe hierzu die Detailbeschreibungen der einzelnen Komponenten:

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

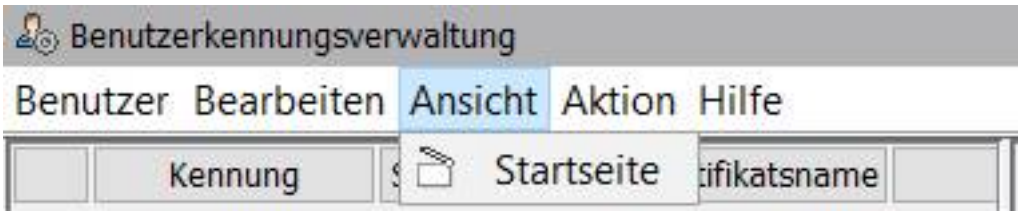
Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

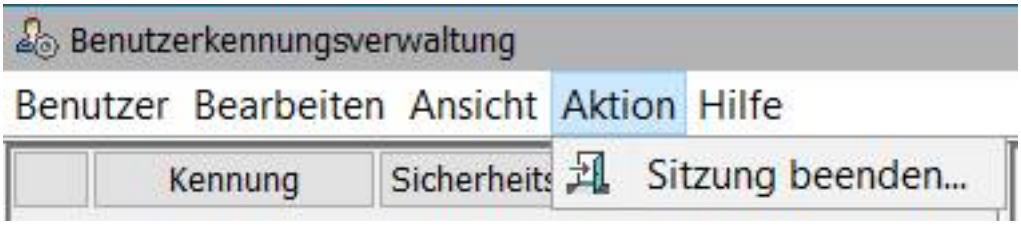
Menü Ansicht

Das Menü **Ansicht** enthält - je nach Software-Komponente - unterschiedliche Optionen. Bei den Komponenten Benutzerkennungsverwaltung und Systemkennungsverwaltung enthält des Menü **Ansicht** nur die Option **Startseite** von OpenScape 4000 Assistant/Manager. Bei den Komponenten Zugriffsrechtekonfiguration und Zugriffsrechtegruppen-Konfiguration dagegen werden spezifische Optionen angezeigt. Detailinformationen finden Sie bei der jeweiligen Komponente. Als Beispiel ist hier das Menü **Ansicht** der Zugriffsrechtegruppen-Konfiguration abgebildet.

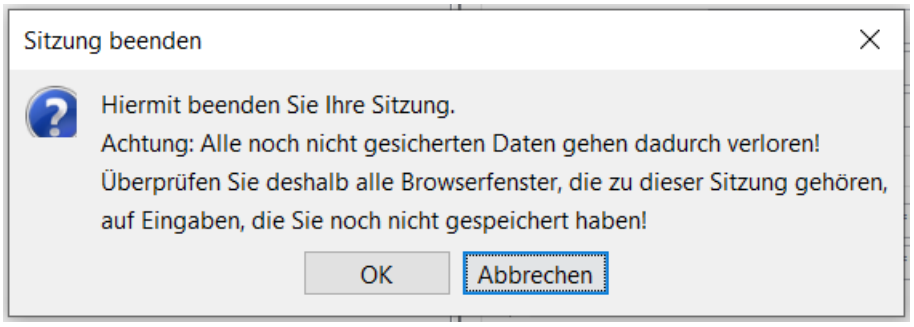


Menü Aktion

Das Menü **Aktion** enthält die Option **Sitzung beenden**. Diese hat die gleiche Funktion wie die Symbolschaltfläche **Sitzung beenden** in der Symbolleiste, Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung".



Sobald Sie auf **Sitzung beenden** klicken, erscheint eine Warnmeldung, die darauf hinweist, dass sämtliche nicht gespeicherten Sitzungsdaten verloren gehen. Sie werden aufgefordert, alle Sitzungsdaten zu speichern und das Verlassen der Sitzung zu bestätigen.

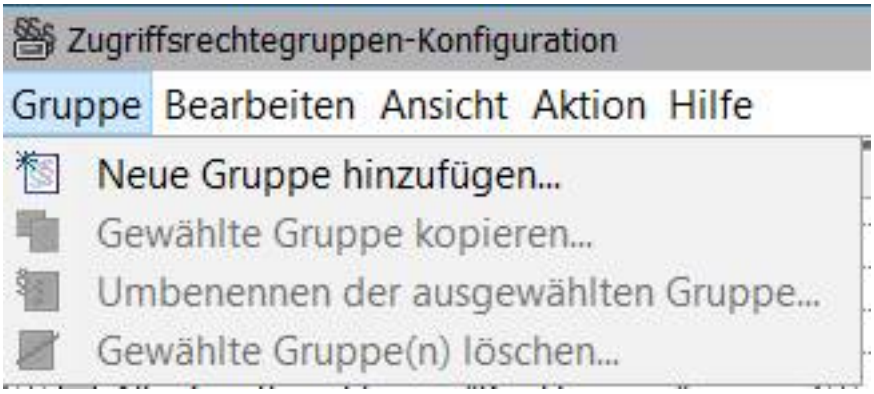


Das Menü "Hilfe"

Das Menü **Hilfe** wird bei allen Komponenten des Bereichs **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**. Das Menü **Hilfe** enthält bei allen Komponenten die gleichen Optionen, und zwar **Kontextsensitive Hilfe**, **Hilfethemen** und **Info**. Details hierzu finden Sie bei den einzelnen Komponenten, z. B. unter Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung".

Menü Gruppe

Das Menü **Gruppe** erscheint nur im Dialogfeld Zugriffsrechtegruppen-Konfiguration.



Symbole und Steuerelemente

Eine Beschreibung der Symbole, Steuerelemente und sonstigen Elemente der Benutzeroberfläche der Zugangsverwaltung finden Sie unter:

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung"

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Verwandte Themen

Zugriffssteuerung für Server und Anwendungen page 16

Benutzeroberfläche der Zugangsverwaltung page 19

Einführung page 7

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen page 10

2.2.4 Kontextmenü

Das **Kontextmenü** rufen Sie über die **rechte Maustaste** auf. Die im Kontextmenü angezeigten Befehle entsprechen immer der aktuellen Arbeitsumgebung. Die im Kontextmenü angezeigten Befehle entsprechen immer der aktuellen Arbeitsumgebung. Es werden immer nur Befehle angezeigt, die zum aktuellen Bereich der Benutzeroberfläche gehören und zur Bearbeitung der aktuellen Einstellungen eingesetzt werden. Nur die jeweils relevanten Befehle können gewählt werden; nicht relevante Befehle sind verblasst (grau) dargestellt.

Markieren von Elementen

Bevor Sie Befehle ausführen, müssen Sie die gewünschten Elemente (Benutzerkennungen) markieren.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Übersicht der im Kontextmenü angezeigten Befehle (Beispiele):

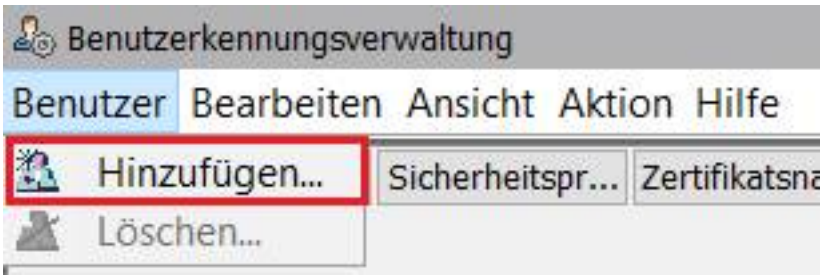


Figure 1: Benutzerkennungsverwaltung, Benutzerliste (Linker Bereich)

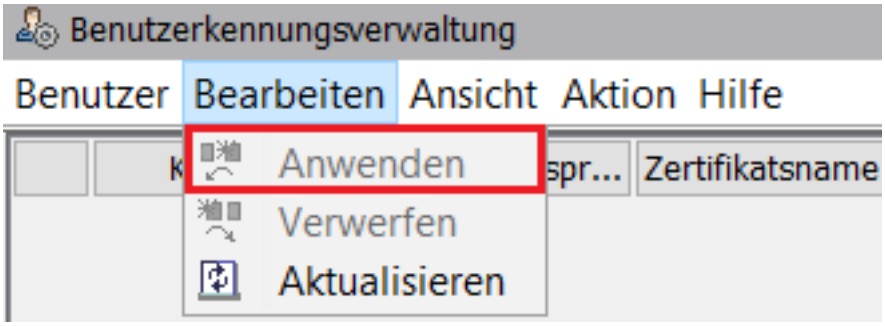


Figure 2: Benutzerkennungsverwaltung, Rechter Bereich

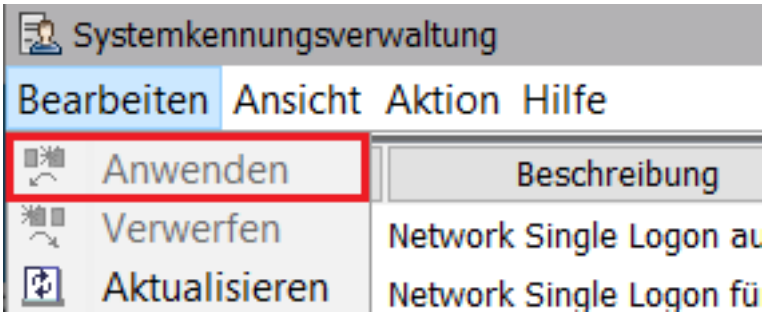


Figure 3: Systemkennungsverwaltung, linker und rechter Bereich

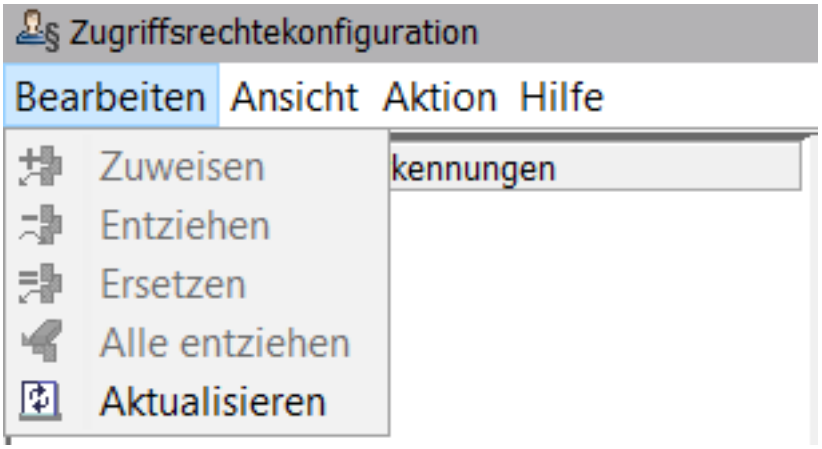


Figure 4: Zugriffsrechtekonfiguration, linker und rechter Bereich

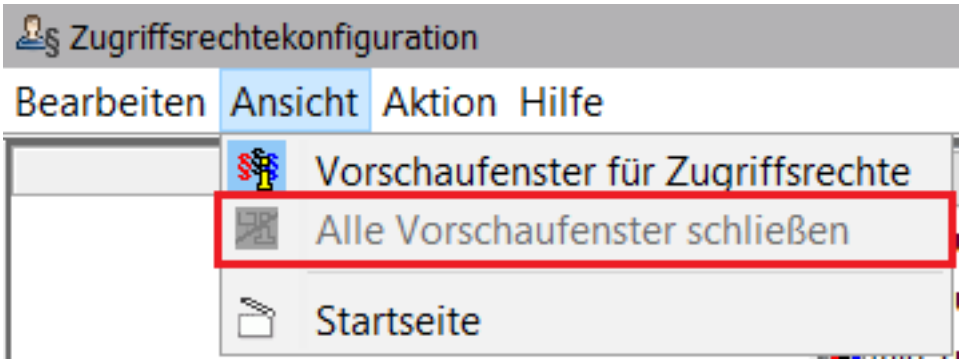


Figure 5: Zugriffsrechtekonfiguration, Vorschaubereich

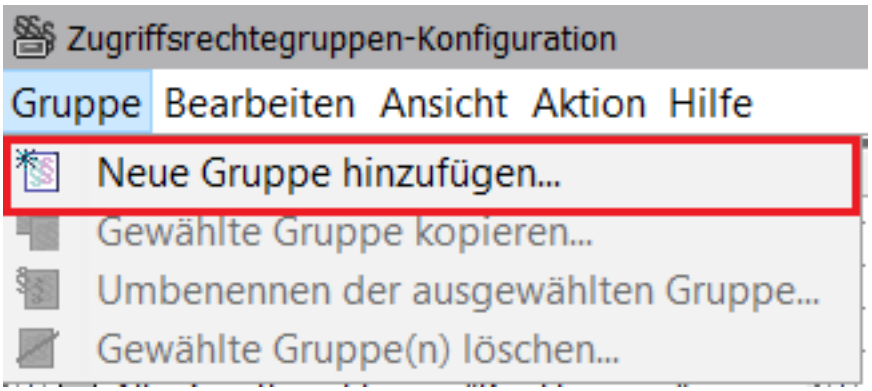


Figure 6: Zugriffsrechtegruppen-Konfiguration, linker Bereich

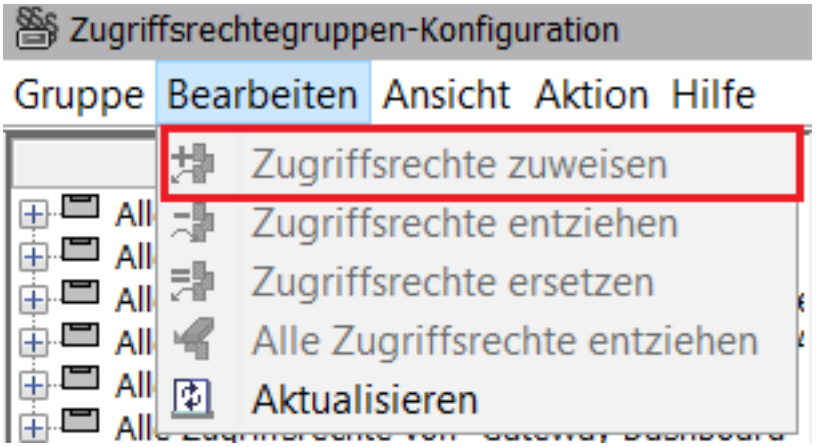
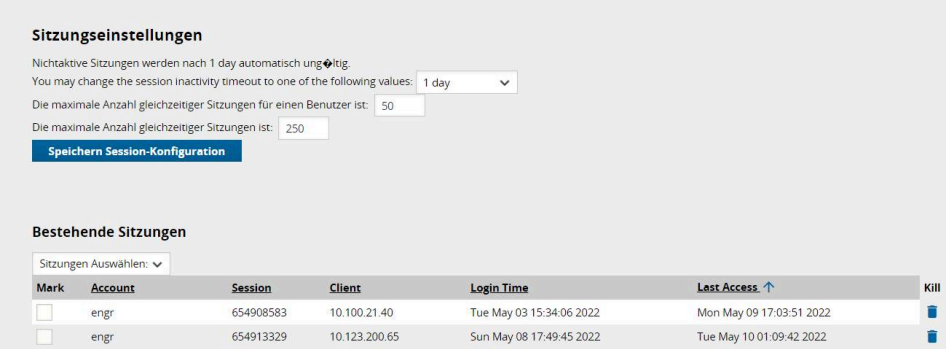


Figure 7: Zugriffsrechtegruppen-Konfiguration, linker Bereich

2.3 Web Session Manager

Das Dialogfeld **Session Manager** zeigt eine Liste aller laufenden Web-Sitzungen, die der momentan angemeldete Benutzer entsprechend seiner Berechtigungen verwalten darf. Angezeigt werden sämtliche dem aktuellen Benutzer zugeordneten Sitzungen sowie zusätzlich die Sitzungen aller Benutzer mit niedrigeren Zugriffssicherheitsebenen - siehe Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen. Hauptaufgabe des Session Managers ist das Löschen von verwaisten Sitzungen, die noch nicht abgelaufen

sind. Eine Sitzung wird als verwaist bezeichnet, wenn z. B. ein Benutzer alle Browser-Fenster schließt, ohne sich explizit abzumelden.



Der Session Manager umfasst folgende Funktionsbereiche:

Sitzungseinstellungen

Bestehende Sitzungen

2.3.1 Sitzungseinstellungen

Die folgenden Einstellungen werden angezeigt und können unter **Sitzungseinstellungen** eingegeben werden:

- **Nicht aktive Sitzungen werden nach xx Minute(n)/Stunde(n)/Tag(en)/ Woche(n)/Monat(en) automatisch ungültig.** Diese Einstellung gibt den eingestellten aktuellen Zeitüberschreitungswert an, nach dessen Ablauf nicht aktive Sitzungen ungültig (und damit automatisch gelöscht) werden.

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern. Wenn der Wert geändert wird, werden alle laufenden Sitzungen aller Benutzer sofort beendet; für alle danach eröffneten Sessions gilt der neue Wert.
- **Die maximale Anzahl gleichzeitiger Sitzungen pro Benutzer ist: xx**. Hier wird der aktuell eingestellte Wert für die maximal zulässige Anzahl gleichzeitiger Sitzungen pro Benutzerkennung angegeben.

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern.
- **Die maximale Anzahl gleichzeitiger Sitzungen pro Benutzer ist: xxx.** Hier wird der aktuell eingestellte Wert für die maximal zulässige Anzahl gleichzeitiger Sitzungen angegeben.

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern.

Feldbeschreibungen

Siehe Sitzungseinstellungen

Siehe auch

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.3.2 Bestehende Sitzungen

In der Tabelle **Bestehende Sitzungen** werden alle laufenden Sitzungen angezeigt, die ein Benutzer aufgrund seiner Zugriffsrechte sehen und bearbeiten darf. Jede Zeile der Tabelle entspricht einer Sitzung. Jede Sitzung ist durch folgende Sitzungseigenschaften eindeutig definiert : **# (Laufende Nummer)**, **Beenden**, **Markieren**, **Kennung**, **Sitzung**, **Client**, **Anmeldezeit**, **Letzter Zugriff**. Die eigene Sitzung ist durch ein Sternchen (*) gekennzeichnet. Wenn Sie die eigene Sitzung löschen, wechselt die Anwendung sofort und ohne Warnung zurück zum Anmeldebildschirm.

Feldbeschreibungen

(Laufende Nummer)

Beenden

Markieren

Kennung

Sitzung

Client

Anmeldezeit

Letzter Zugriff

Sortieren der Tabelle "Bestehende Sitzungen"

Sie können die Einträge in der Tabelle **Bestehende Sitzungen** sortieren (nach **Kennung**, **Sitzung**, **Client** (IP-Adresse**)**, **Anmeldezeit** und **Letzter Zugriff**), indem Sie auf die als Links angezeigten (unterstrichenen) Spaltenüberschriften klicken.

Klicken Sie auf den Spaltentitel, um die Tabelle nach dieser Spalte zu sortieren.

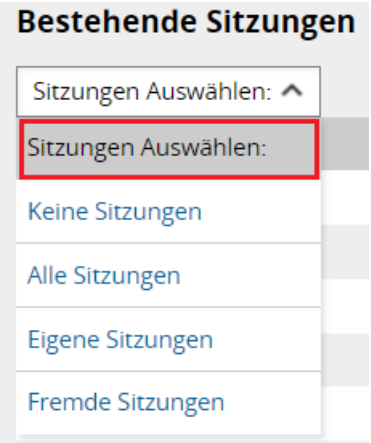
Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung der Tabelle: Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalten können sortiert, aber nicht editiert werden.

Dropdown-Menü "Sitzungen auswählen"

Die Dropdown-Box **Sitzungen auswählen** unterstützt das Auswählen und Anzeigen bestimmter Sitzungen. Klicken Sie einfach auf die gewünschte Option, um nur diejenigen Sitzungen anzuzeigen, die dem Auswahlkriterium entsprechen.



Sie haben die Wahl zwischen folgenden Kriterien für die Anzeige von Sessions:

Keine Sitzungen -> Alle Sessions abwählen

Alle Sitzungen -> Alle Sessions auswählen

Eigene Sitzungen -> Alle eigenen Sessions markieren

Fremde Sitzungen - Alle außer den eigenen Sessions auswählen

Anzeige von NSL-Kennungen bei Netzwerk-Einzelanmeldung mit NSL-Kennung

Über die **Netzwerk-Einzelanmeldung** (Network Single Logon) können Sie vom HTS oder vom OpenScape-Manager aus ohne Passwort auf eine Anlage zugreifen. Angezeigt wird eine solche Session im Session Manager in der Spalte **Kennung** beispielsweise als **htsadm@218.1.16.35**. Es wird also nicht nur die Kennung **htssvc0** oder **htsadm** angezeigt, sondern **Kennung@IP-Adresse** des Ausgangs-Servers, von dem aus der Zugriff erfolgte, d. h. des Servers, auf dem der Benutzer sich tatsächlich eingeloggt hat. Bei der bisher verwendeten Lösung wurde die Session bei solchen Zugriffen sozusagen auf eine existierende Kennung umadressiert bzw. "gemappt". Bei der neuen Lösung wird eine dynamische Kennung erzeugt, die sich aus **account@IP_address** zusammensetzt. Im **Logging Management** wird die Kennung in der Spalte **User** entsprechend als **Kennung@IP-Adresse** angezeigt. Unter **Details** wird im Logging Management der gesamte Pfad und das Mapping des Network Single Logon angezeigt.

Kontrollkästchen

Markieren	Markiert eine laufende Sitzung für die weitere Bearbeitung (z. B. für späteres Löschen mit **Alle markierten Sitzungen beenden**

Schaltflächen

Alle markierten Sitzungen beenden 	Wenn Sie auf die Schaltfläche **Alle markierten Sitzungen beenden** klicken, werden alle markierten Sitzungen beendet (gelöscht). Anschließend erscheint wieder der Bildschirm **Anmeldung**.

Beenden 	Ein Klick auf das Symbol  (Diese Session beenden) in der Spalte **Beenden** löscht die laufende Sitzung und es erscheint wieder der Bildschirm **Anmeldung**.

Feldbeschreibungen

(Laufende Nummer)

Beenden

Markieren

Kennung

Sitzung

Client

Anmeldezeit

Letzter Zugriff

Verwandte Themen

Passwort ändern

Passwortverteilung (nur OpenScape 4000 Manager)

Emergency Password Reset (EPR)

Konto- und Passwort-Einstellungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Zugriffssteuerung für Server und Anwendungen

Benutzerkennungsverwaltung

Systemkennungsverwaltung

Zugriffsrechtekonfiguration

Zugriffsrechtegruppen-Konfiguration

Export von Benutzerdaten

Registerkarte "Zugangsverwaltung" in der Systemverwaltung

Einführung

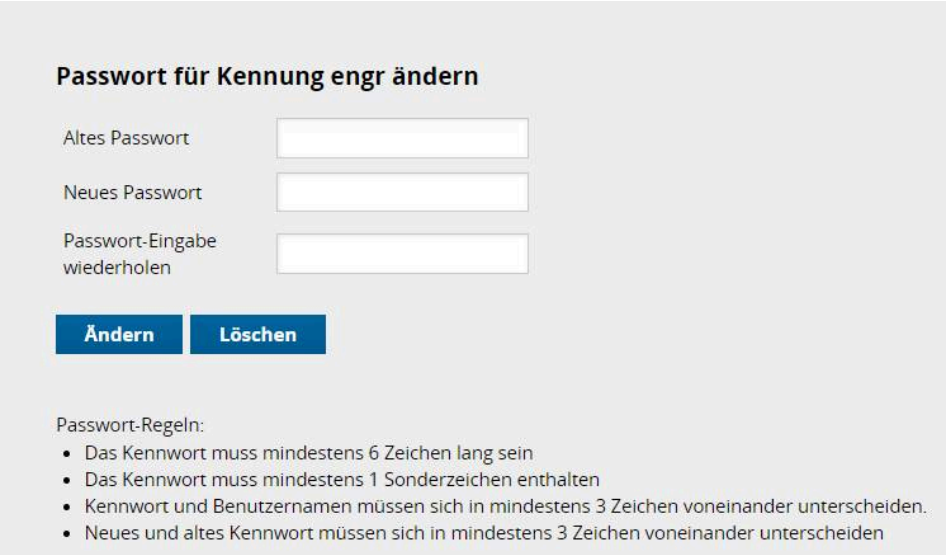
Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

2.4 Passwort ändern

NOTICE: Dieser Abschnitt beschreibt die für OpenScape 4000 Manager & Assistant identischen Bereiche der Funktion **Passwort ändern**. Die für den Manager zusätzlich zur Verfügung stehende Funktion **Passwortverteilung** wird im

Abschnitt Passwortverteilung (nur OpenScape 4000 Manager) beschrieben.

Das Dialogfeld **Passwort ändern** dient der Änderung des Benutzer-Passworts für die Zugangsverwaltung. Dieses Dialogfeld erscheint nur, wenn der Benutzer über die erforderlichen Zugriffsrechte für die Änderung des Passworts verfügt.



Schaltflächen

Ändern	Wenn Sie auf diese Schaltfläche klicken, werden die gewünschten Änderungen vorgenommen; das neue Passwort gilt ab sofort für alle weiteren Sitzungen.
Löschen	Wenn Sie auf **Löschen** klicken, wird der Inhalt der Eingabefelder entfernt und Sie können neue Werte eingeben.

Passwortregeln

Die Regeln für die Eingabe gültiger Passwörter werden im Dialogfeld **Passwort ändern** angezeigt:

- Passwort muss aus mindestens 6 Zeichen bestehen
- Passwort darf nicht länger als 16 Zeichen sein
- Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe)
- Passwort muss sich in mindestens drei Zeichen vom Benutzernamen unterscheiden
- Passwort muss sich in mindestens drei Zeichen vom alten Passwort unterscheiden

Erweiterte Passwort-Regeln wenn Password History Configuration aktiviert ist

Im Dialogfeld Konto- und Passwort-Einstellungen können zusätzliche im Dialogfeld spezifizierte Passwort- und Kontoregeln aktiviert werden.

Beachten Sie bitte, dass Addministratioren mit Superuser-Zugriffsrechten diese Regeln umgehen können. Dadurch kann es vorkommen, dass Ihr altes

Passwort diesen Regeln nicht entspricht, Sie aber bei Eingabe eines neuen Passworts die Regeln beachten müssen.

Feldbeschreibungen

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Ändern

Löschen

Verwandte Themen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Web Session Manager

Passwortverteilung (nur OpenScape 4000 Manager)

Emergency Password Reset (EPR)

Konto- und Passwort-Einstellungen

Zugriffssteuerung für Server und Anwendungen

Benutzerkennungsverwaltung

Systemkennungsverwaltung

Zugriffsrechtekonfiguration

Zugriffsrechtegruppen-Konfiguration

Export von Benutzerdaten

Registerkarte "Zugangsverwaltung" in der Systemverwaltung

Einführung

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

2.5 Passwortverteilung (nur OpenScape 4000 Manager)

Diese zusätzliche Funktion für den Managerermöglicht das einfache Verwalten und Verteilen von Passwörtern einzelner Benutzer vom Manager aus. Es kann nicht nur das Passwort des aktuellen Benutzers am Manager geändert werden, sondern auch auf allen ausgewählten Assistants. Dieses Leistungsmerkmal ist nur im OpenScape 4000 Manager verfügbar.

2.5.1 Konfiguration

2.5.1.1 Zuordnung der Assistants

Zuallererst müssen Assistants dem Benutzer zugeordnet werden. Auf diesen zugeordneten Assistants muss jeweils der Benutzer existieren, d. h. ein Benutzerkonto vorhanden sein. Die Passwörter aller Benutzerkonten auf den verschiedenen Assistants müssen identisch sein, und das Recht zum Ändern des Passworts gegeben sein. Hierfür muss im Dialogfenster Benutzerkennungsverwaltung das Kontrollkästchen **Passwort-Änderung erlaubt** markiert sein (siehe Benutzerkennungsverwaltung).

Die Zuordnung kann der Benutzer nicht selbst erledigen, sondern der Benutzer "**engr**" muss die Konfiguration am Manager vornehmen.

Hierfür wird in die zwei Dateien
`/var/secm/pwddist/<username>.cnf`
`/var/secm/pwddist/global.cnf`

in jeweils einer Zeile eine IP-Adresse mittels eines Textverarbeitungsprogramms eingefügt.

Natürlich kann als Textverarbeitungsprogramm der "vi" verwendet werden. Sind Sie mit dem "vi" nicht vertraut, wechseln Sie bitte in das Verzeichnis "**/var/secm/pwddist**" und verwenden folgendes Kommando pro Assistant bzw. pro IP-Adresse:
`echo "192.023.045.056" >> global.cnf`

Die Datei "**global.cnf**" wird für alle Benutzer verwendet, für die keine benutzerspezifische **<Benutzername>.cnf**-Datei angelegt ist.

Heißt der Benutzer zum Beispiel "Meier" und existiert die Datei "**Meier.cnf**", dann wird nur das Passwort derjenigen Assistants aktualisiert, die in der Datei "Meier.cnf" aufgelistet sind. Befinden sich keine Einträge in der Datei, wird das Passwort nur lokal am Manager geändert.

Existiert die Datei "**Meier.cnf**" nicht, werden die Benutzerkonten der Assistants aktualisiert, die in der Datei "**global.cnf**" aufgelistet sind.

NOTICE: Die Assistants, die hinter den IP-Adressen stehen, müssen nicht zwingend in der Systemverwaltung eingetragen sein. In der Praxis wird dies üblicherweise nicht vorkommen.

Des Weiteren werden die log-Dateien im Verzeichnis `/var/secm/pwddist/log angelegt.`

2.5.1.2 Hinweise zur Konfiguration

Beachten Sie bitte folgende Hinweise zur Konfiguration:

1) Die IP-Adressen der zugeordneten Assistants müssen existieren. Über diese IP-Adresse muss der entsprechende Assistant erreichbar sein. Ist das nicht der Fall, wir dies durch den Eintrag
   `"error while executing execurl: 10"`

   in der Protokolldatei dokumentiert.
2) Der Benutzer, dessen Passwort geändert werden soll, muss auf den zugeordneten Assistants Benutzerkonten gleichen Namens haben. Ist das

nicht der Fall, wird auf den Assistants, auf denen das Benutzerkonto nicht existiert, keine Änderung vorgenommen.
`"error while executing execurl: 11"`

in der Protokolldatei dokumentiert.

3) Alle Benutzerkonten eines Benutzers müssen auf allen zugeordneten Assistants das gleiche Passwort haben. Ist das nicht der Fall, wird auf den Assistants, auf denen das Passwort verschieden ist, keine Änderung vorgenommen.
`"error while executing execurl: 11"`

in der Protokolldatei dokumentiert.

4) Der Benutzer muss auf jedem Assistant das Recht zum Ändern seines Passworts haben. Ist das nicht der Fall, wird auf den Assistants, auf denen das Recht nicht gegeben ist, keine Änderung vorgenommen. Man würde sich eine Fehlermeldung erwarten, in der Protokolldatei ist aber folgende Erfolgsmeldung zu lesen:
`successfully reset password for user [User]`
5) Der Benutzer muss am Manager das Zugriffsrecht zum Ändern seines Passworts haben.

2.5.2 Vorgehensweise

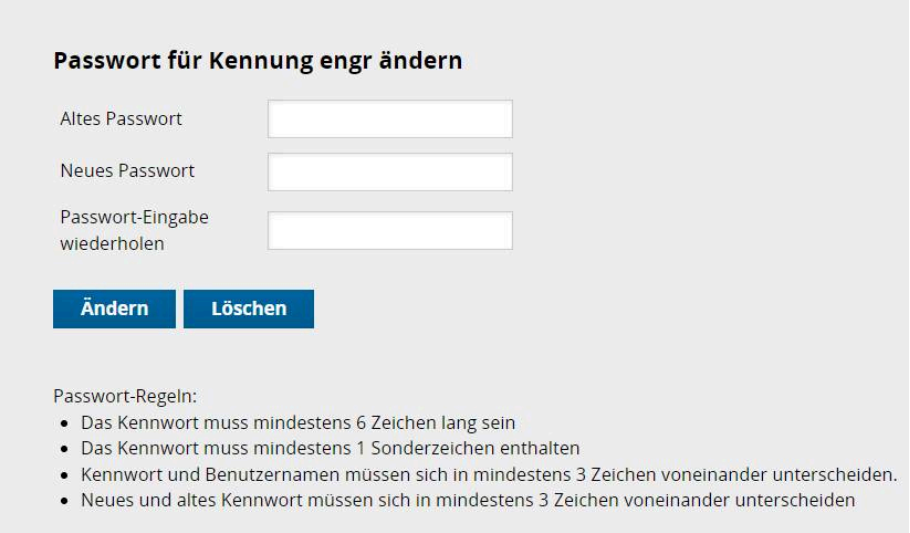
2.5.2.1 Hinweise

1) Die Änderungen werden von eben diesem Benutzer vorgenommen, nicht durch einen Administrator.
2) Der Benutzer ist selbst für die Änderung des Passworts in regelmäßigen Zeitintervallen verantwortlich.
3) Ein neues Benutzerkonto plus Passwort muss "per Hand" vom Administrator direkt am Assistant angelegt werden.
4) Jede Änderung auf einem zugeordneten Assistant erfolgt für sich und beeinflusst die Änderungen auf den anderen Assistants nicht. D.h. schlägt die Änderung auf einen Assistant fehl, stoppt der Prozess nicht, sondern es wird beim nächsten Assistant fortgefahren. So kann es natürlich sein, dass auf allen außer einem Assistant die Passwörter geändert worden sind. Hier muss, um wieder ein konsistentes System zu erlangen, der Benutzer "von Hand" die Änderungen direkt am Assistant vornehmen.
5) Die Änderungen der Passwörter erfolgt hintereinander. Beim Ändern mehrerer Passwörter auf verschiedenen Assistants kann einige Zeit in Anspruch genommen werden. Erst nachdem alle Passwörter geändert worden sind, kann eine weitere Änderung durchgeführt werden.

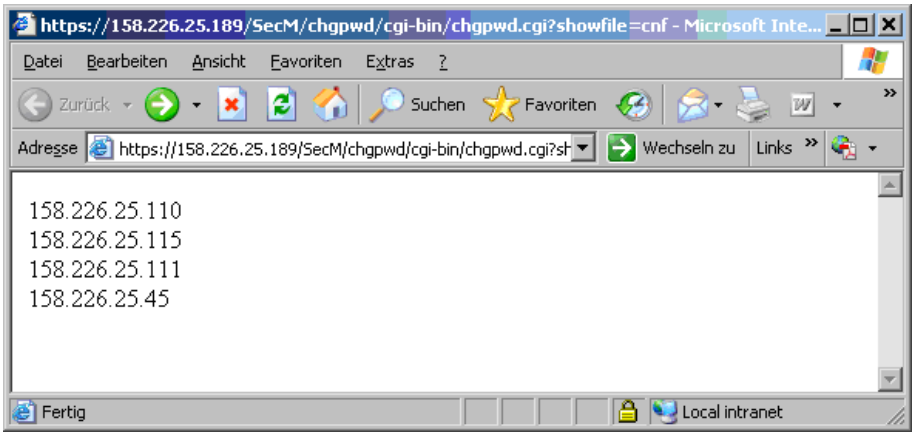
2.5.2.2 Schritt für Schritt

1) Loggen Sie sich am Manager ein.

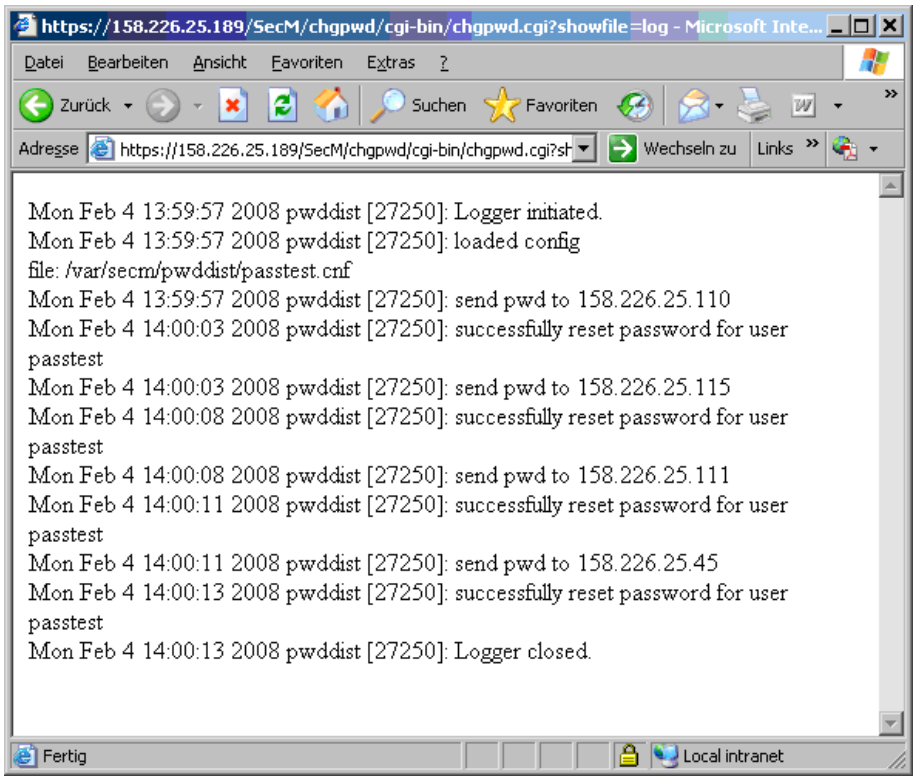
2) Wählen Sie über den Menübaum nacheinander **Zugangsverwaltung**, **Sitzungsverwaltung** und **Passwort ändern**. Es erscheint die Manager-Version der **Passwort ändern** Eingabemaske.



3) Geben Sie nacheinander das alte Passwort, das neue Passwort und die Passwortbestätigung in die Textfelder ein (siehe Passwort ändern).
4) Wenn Sie das Kontrollkästchen **Passwort auch ändern am Assistant(s) (Passwortverteilung) nicht** markieren, wird die Passwortänderung nur lokal am Manager angestoßen.
5) Wenn Sie das Kontrollkästchen **Passwort auch ändern am Assistant(s) (Passwortverteilung)** markieren, werden auch alle Passwörter auf den zugeordneten Assistants geändert.
6) Wenn Sie auf den Link **Assistants** klicken, öffnet sich ein Fenster, in dem die zugeordneten Assistants aufgelistet sind.



7) Wenn Sie auf den Link **Protokolldatei** klicken, öffnet sich ein Fenster, in dem das Ergebnis des letzten Änderungsvorganges angezeigt wird.



Feldbeschreibungen

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Passwort auch ändern am Assistant(s) (Passwortverteilung)

Ändern

Löschen

Verwandte Themen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Web Session Manager

Passwort ändern

Emergency Password Reset (EPR)

Konto- und Passwort-Einstellungen

Zugriffssteuerung für Server und Anwendungen

Benutzerkennungsverwaltung

Systemkennungsverwaltung

Zugriffsrechtekonfiguration

Zugriffsrechtegruppen-Konfiguration

Export von Benutzerdaten

Registerkarte "Zugangsverwaltung" in der Systemverwaltung

Einführung

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

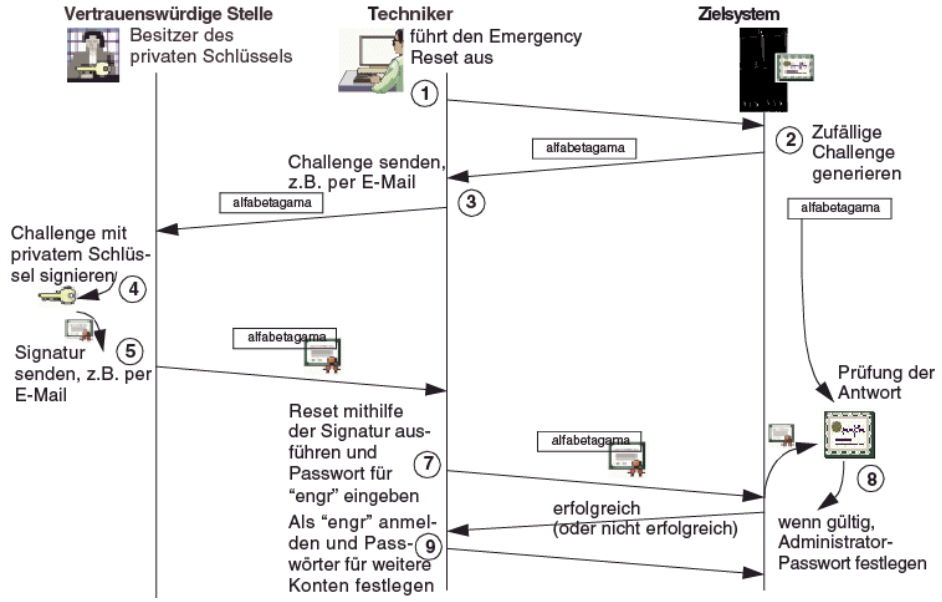
2.6 Emergency Password Reset (EPR)

Mit Emergency Password Reset (EPR) kann das Administrator-Passwort des Assistant, der Host-Plattform oder von CSTA zurückgesetzt werden, falls es verloren gegangen ist oder Systemfehler vorliegen.

Vor der Verwendung dieses Leistungsmerkmals muss das System richtig konfiguriert sein, und das Leistungsmerkmal muss vom System-Administrator aktiviert werden.

Damit das Leistungsmerkmal funktionsfähig ist, muss bei der Konfiguration ein Zertifikat von einer für das System vertrauenswürdigen Stelle importiert werden. Das Zertifikat wird im X.509 PEM-Format erwartet. Der Benutzer wird authentifiziert und darf sein Passwort ändern, indem er seine Fähigkeit beurteilt, eine vom System ausgestellte zufällige Meldung mit dem privaten Schlüssel des Zertifikatsinhabers zu signieren. Die Signaturantwort muss ein SHA512 Meldungsdigest sein; andere Algorithmen werden nicht unterstützt. Das System kann die eingereichte Antwort mit dem öffentlichen Schlüssel des installierten Zertifikats verifizieren. Nach der erfolgreichen Verifizierung darf der Initiator des Emergency Resets das Administrator-Passwort ändern.

Das Arbeitsflusskonzept des Merkmals lautet wie folgt:



2.6.1 EPR - Konfiguration

Vorbereitung des Systems auf den Emergency Reset:

- Der Administrator aktiviert das Merkmal und konfiguriert die allgemeinen Einstellungen (siehe EPR-Allgemeine Konfiguration),

  und
- Importiert ein Zertifikat - öffentlicher Schlüssel (siehe Installation eines Zertifikats)

Der private Schlüssel des Zertifikats muss von einer vertrauenswürdigen Behörde sicher gespeichert werden. Es ist nicht relevant, wenn das Zertifikat von einer dritten Zertifizierungsbehörde (CA) ausgestellt wird oder es ein selbstsigniertes Kundenzertifikat ist. Beide werden akzeptiert und weder die Authentizität des Zertifikats noch der Widerruf werden während des Imports überprüft.

Beispiel für die Generierung eines selbstsignierten Zertifikats:

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

Dieser Befehl beinhaltet ein Dialogfeld zum Erstellen des selbstsignierten RSA 2048-Bit-Zertifikats. Die Passphrase für den privaten Schlüssel (epr-self.key) und die Zertifikat-Eigenschaften müssen eingegeben werden. Die Passphrase und der private Schlüssel müssen von der vertrauenswürdigen Behörde sicher an verschiedenen Orten gespeichert werden.

Variante für ECDSA-Zertifikat:

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

Während des Emergency Password Resets

- **Schritt 1:** Der Benutzer initiiert das Passwortreset über eine öffentliche Seite oder eine Terminal-Anmeldung.
- **Schritt 2:** Der Benutzer fordert eine zufällige Herausforderung (zufällige 32-Byte-Lange Zeichenfolge) aus dem System an (siehe Anfrage einer neuen Herausforderung).
- **Schritt 3:** Der Benutzer fordert die vertrauenswürdige Behörde an, die zufällige Herausforderung mit dem privaten Schlüssel des Zertifikats zu signieren.
- **Schritt 4-5:** Die vertrauenswürdige Behörde signiert die zufällige Herausforderung und sendet sie an den Administrator zurück. Die Signatur

muss eine SHA512-Digest sein. Es werden keine anderen Digest-Algorithmen akzeptiert.

Die Herausforderung kann von der vertrauenswürdigen Behörde mit dem folgenden Befehl signiert werden:

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

wobei

- `Private.key` ist der private Schlüssel des importierten Zertifikats.
- `Challenge` ist die Datei mit der Herausforderung.

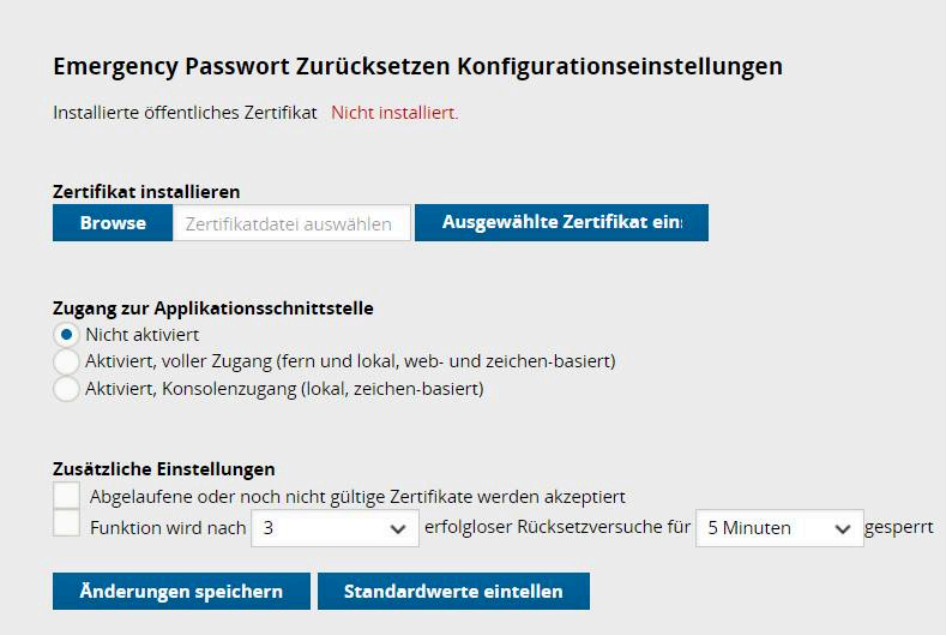
  Bitte beachten Sie, dass die Datei mit Herausforderung das Zeilenende-Zeichen **NICHT** enthalten darf.
- `Response.sha` ist die Datei mit der signierten Herausforderung.

Die Umwandlung der signierten Challenge in das BASE64-Format (PEM) kann mit folgendem Befehl durchgeführt werden:

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

- **Schritt 6:** Der Benutzer sendet eine signierte Herausforderung an das System (siehe Herausforderung).
- **Schritt 7:** Das System verifiziert die Herausforderung gegen den öffentlichen Schlüssel des installierten Zertifikats.
- **Schritt 8:** Wenn die Überprüfung erfolgreich ist, darf der Benutzer das Verwaltungspasswort der Assistant, Plattform oder CSTA ändern (siehe Passwortreset ausführen).

2.6.1.1 EPR - Allgemeine Konfiguration



Aufruf des Fensters für die allgemeine EPR Konfiguration

- Dieses Fenster ist nur dem Systemadministrator verfügbar, z. B. zum Benutzerkonto "engr".

- Das Fenster wird von der **Startseite** aus über das Menü **Zugangsmanagement**> **Notfallpasswort zurücksetzen Konfigurationseinstellung**aufgerufen

EPR Konfigurationsfenster - Symbolleiste

Die Symbolleiste enthält die folgenden Schaltflächen:

Hilfe => Öffnet die Online-Hilfe und zeigt den Hilfeindex an

Startseite => Links zum Launchpad

Start => Öffnet ein neues Browser-Fenster, das die Startseite von OpenScape 4000 Manager anzeigt.

Abmelden=> Meldet den aktuellen Benutzer ab, schließt die laufende Sitzung für alle zugehörigen Browser-Fenster und kehrt zum Anmeldebildschirm zurück.

Installieren eines Zertifikats

- Klicken Sie auf **Durchsuchen**, um eine Datei, die das von der vertrauenswürdigen Behörde verwaltetes Zertifikat enthält, auszuwählen.

  Anmerkung: Es werden nur Zertifikate im X.509 PEM-Format akzeptiert.

- Klicken Sie auf **Ausgewähltes Zertifikat anzeigen**, um Details zum ausgewählten Zertifikat anzuzeigen.

  Siehe Zertifikatsdetails, Seite 44.
- Klicken Sie auf **Änderungen einreichen**, um die aktuellen Einstellungen zu speichern.

  Oder
- Klicken Sie auf **Standardwerte einstellen**, um die Änderungen zu verwerfen und die Einstellungen auf die Standardwerte zurückzusetzen. Das Zertifikat bleibt unverändert.

Optionen für den Zugriff auf die Schnittstelle zum Zurücksetzen des Notfallpassworts

Der Zugriff auf Emergency Password Reset kann mit den folgenden Optionen konfiguriert werden:

- **Deaktiviert:** Merkmal Deaktiviert (kein EPR möglich)
- **Aktiviert, Vollzugriff:** EPR über Browser und Terminal-Anmeldung möglich
- **Aktiviert, Konsolenzugriff:** EPR über Terminal-Anmeldung möglich

Zusätzliche Einstellungen

- **Abgelaufene oder nicht mehr gültige Zertifikate werden akzeptiert:** Die Gültigkeitsdauer wird bei der Installation nicht überprüft
- **Aussetzen:** Ein Merkmal nach bestimmten ungültigen Versuchen für eine bestimmte Zeit aussetzen.

2.6.1.2 Zertifikatdetails

Zweck dieses Fensters

Die Seite mit den **Zertifikatdetails** zeigt die Details der ausgewählten Zertifikate.

- Klicken Sie auf **Zurück zu den Konfigurationseinstellungen**, um das Fenster zu schließen und zur Konfigurationsseite zurückzukehren.
- Siehe EPR - Allgemeine Konfiguration, page 51.

2.6.2 EPR - Zurücksetzen

2.6.2.1 Anfordern einer neuen Challenge

NOTICE: Eine Challenge ist eine 32 Byte lange zufällige alphanumerische Zeichenkette. Diese muss beim Speichern in einer Datei unverändert übernommen werden: keine Zeichencodierung, keine Zeilenschaltungen usw.

Um eine neue Challenge zu generieren:

- Öffnen Sie zuerst das Fenster Emergency Passwort Zurücksetzen, indem Sie auf den Link **Emergency Passwort Zurücksetzen** des Anmeldebildschirms klicken.
- Klicken Sie auf **Neue Challenge**, um eine neue zufällige Challenge zu generieren. Daraufhin wird die Seite **Zurücksetzen** angezeigt (sh. Zurücksetzen des Passworts).

2.6.2.2 Zurücksetzen des Passworts

Herausforderung

Die generierte Herausforderung wird im Textfeld **Herausforderung** angezeigt.

- Klicken Sie auf **Neue Herausforderung**, um die aktuelle Herausforderung zu verwerfen und eine neue anzufordern
- Klicken Sie auf **Herausforderung abbrechen**, um die aktuelle Herausforderung zu verwerfen

Anmerkung: Eine gültige Antwort ist eine SHA512-Meldungsdigest, die von der vertrauenswürdigen Behörde des installierten Zertifikats generiert wurde. Dabei handelt es sich um eine 256 Byte lange Binärdatei. Andere Methoden für Nachrichten-Digests werden nicht unterstützt.

Antwort

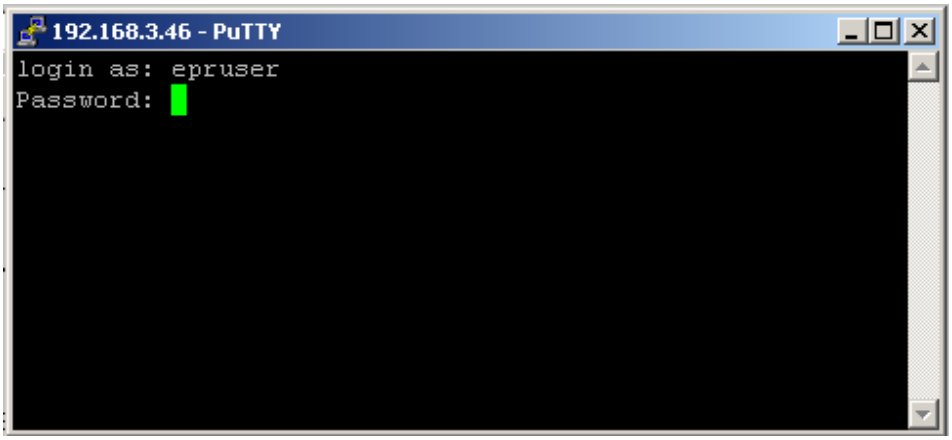
- Geben Sie im Textfeld **Antwort** eine BASE64-codierte Antwort ein,

  oder
- Klicken Sie auf **Durchsuchen**, um binäre oder BASE64-codierte Antwortdatei auszuwählen.
- Klicken Sie auf **Passwort setzen**, um das Administrator-Passwort zurückzusetzen.

Festlegen eines neuen Administrator-Passworts

- Im Feld **Neues Passwort**, geben Sie das neue Administrator-Passwort ein
- Im Feld **Passwort erneut eingeben**, genehmigen das neue Passwort, indem Sie es erneut eingeben.
- Klicken Sie auf **Passwor setzen**, um die Anfrage an den Server zu senden.

2.6.3 EPR - Zurücksetzen über die Konsole



- Anmelden als: "epruser" (ohne Anführungszeichen) mit dem öffentlichen Passwort "epr2000$" (ohne Anführungszeichen) an.

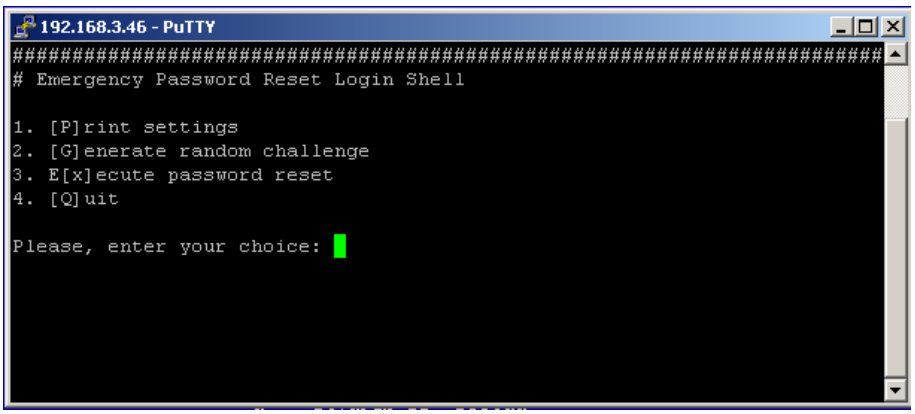


Abbildung 8: EPR-Anmelde-Shell, Anfangsmenü

In der **Emergency Password-Anmelde-Shell** werden die folgenden Optionen angezeigt.

1) Drucken der Einstellungen (Print settings) [P]
2) Generieren einer zufälligen Challenge (Generate random challenge) [G]
3) Ausführen eines Passwort-Resets (Execute password reset) für den Assistant (Benutzer engr) [x]
4) Ausführen eines Passwort-Resets für die Host-Plattform (Benutzer root)
5) Ausführen eines Passwort-Resets für CSTA (Benutzer root)
6) Verlassen (Quit) [Q]

- Geben Sie den in Klammern angezeigten Buchstaben für die gewünschte Option ein, und drücken Sie die [EINGABETASTE].

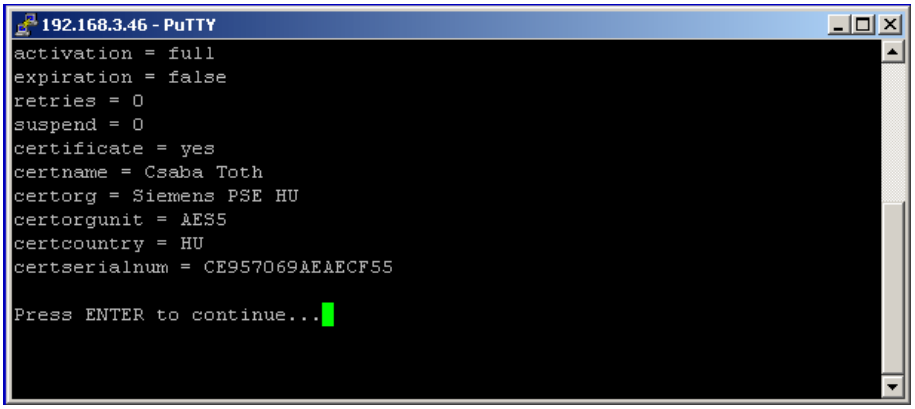


Abbildung 9: Drucken der Einstellungen (Print settings)

- Drücken Sie die [EINGABETASTE], um weitere aktuelle Einstellungen anzuzeigen.

- Drücken Sie am Ende der Liste die [EINGABETASTE], um zum Anfangsmenü zurückzukehren.

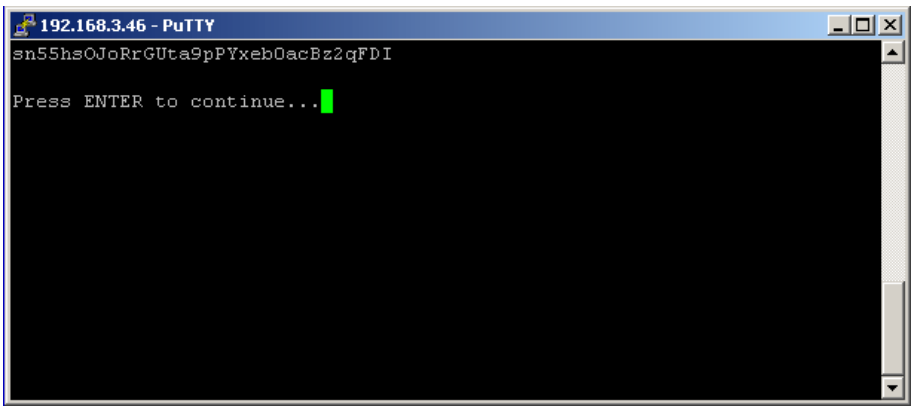


Abbildung 10: Generieren einer zufälligen Challenge (Generate random challenge)

Eine neue zufällige Challenge wird generiert und angezeigt.

- Drücken Sie die [EINGABETASTE], um zum Anfangsmenü zurückzukehren.

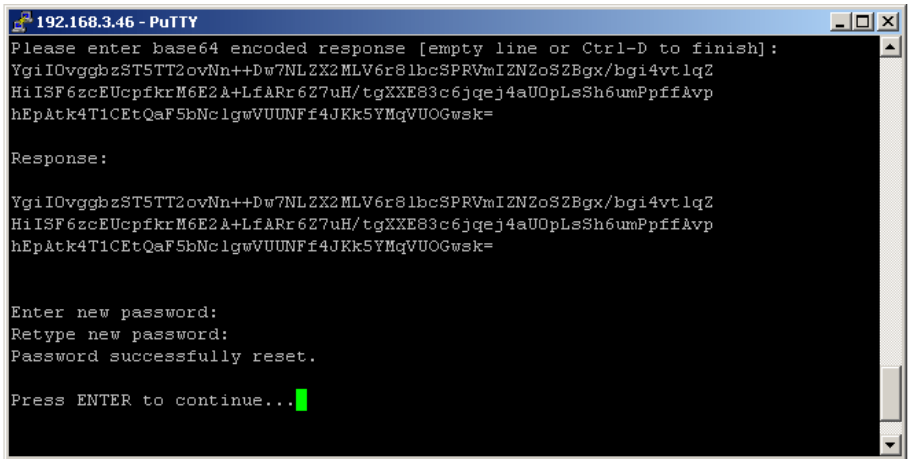


Abbildung 11: Ausführen eines Passwort-Resets (Execute password reset)

- Geben Sie hinter Response eine Antwort ein, indem Sie eine BASE64-codierte Antwort einfügen.
- Geben Sie eine Zeilenschaltung ein, oder drücken Sie [Strg]-[D], um die Eingabe abzuschließen.
- Geben Sie in Neues Passwort das neue Passwort ein.
- Wiederholen Sie in wiederholenEingabe des neuen Passworts das neue Passwort.
- Drücken Sie die [EINGABETASTE], um zum Anfangsmenü zurückzukehren.

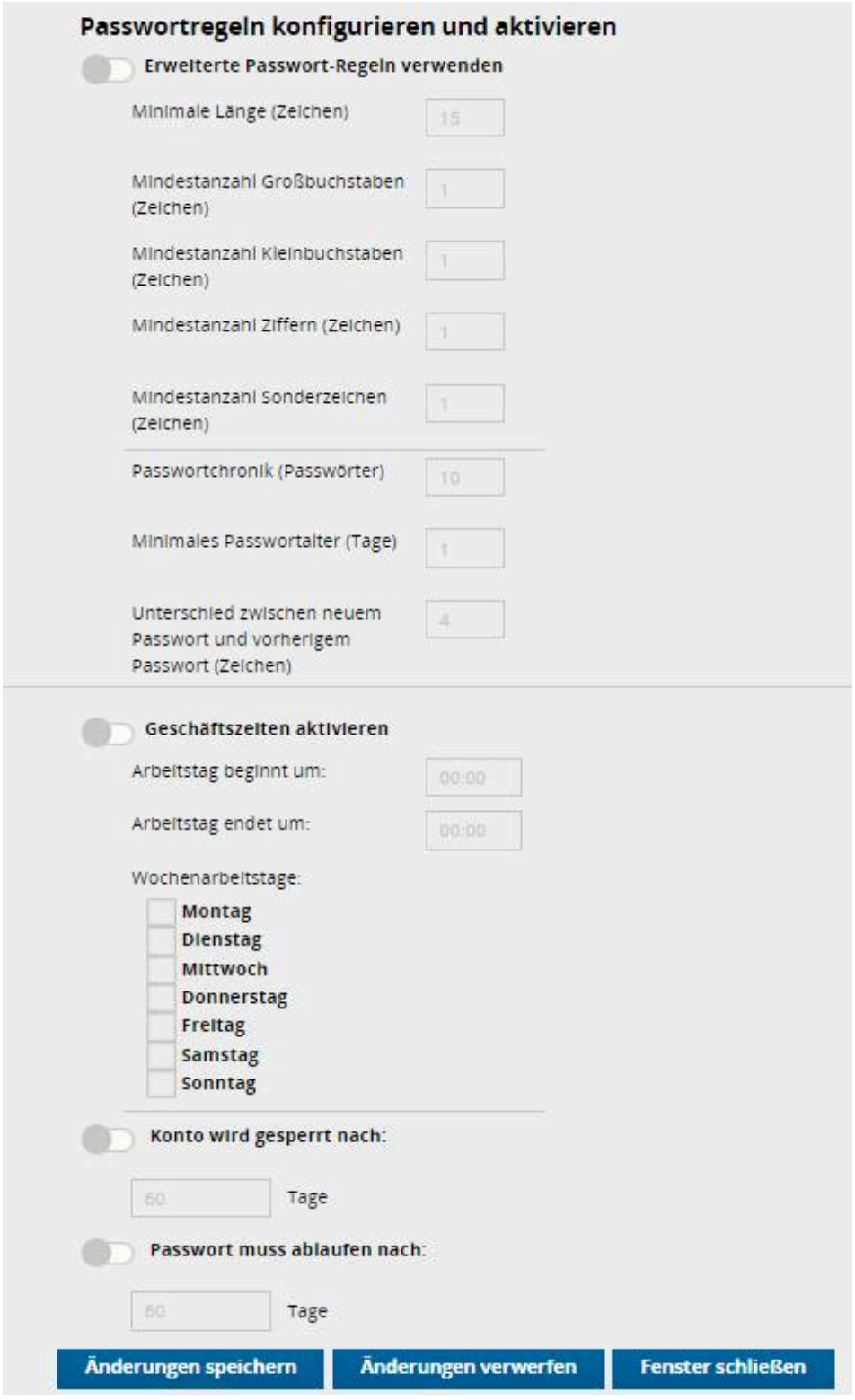
2.7 Konto- und Passwort-Einstellungen

Im Dialogfenster **Passwort-Einstellungen** können erweiterte Passwort-Richtlinien und -Regeln für eine zeitgesteuerte Verwendung des Kontos aktiviert und konfiguriert werden.

Starten Sie die Applikation.

Die Seite **Konfiguration** zum Konfigurieren der Konto- und Passwortrichtlinien kann von der Startseite aus aufgerufen werden:

Kennungsverwaltung -> Passwort-Einstellungen



Allgemeine Hinweise für Passwortrichtlinien

Sämtliche Benutzerkennungspasswörter (administrative und nichtadministrative) müssen den folgenden Regeln entsprechen, (welche Werte für **xx** möglich sind und sonstige weiterführende Informationen entnehmen Sie bitte den **Feldbeschreibungen**):

- Passwörter müssen mindestens **xx** Zeichen lang sein.
- Passwörter müssen eine Mischung aus Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen sein.
- Eine Wiederverwendung der vorherigen **xx** Passwörter ist nicht zulässig.
- Passwörter dürfen innerhalb von **xx** Tagen nur einmal geändert werden. Ausnahme: Administratoren oder Benutzer mit Administratorrechten können das Passwort auch häufiger ändern. Es kann erforderlich sein, dass Benutzer mit Administratorrechten vergessene Passwörter von Benutzern zurücksetzen müssen und daher die Möglichkeit haben sollten, Passwörter mehr als einmal am Tag zu ändern.
- Bei Änderung eines Passworts muss sich das neue Passwort in mindestens **xx** Zeichen vom bisherigen Passwort unterscheiden.
- Wörter aus dem Wörterbuch sind als Passwörter unzulässig.

  Die Wörterbuchprüfung erfolgt mittels "cracklib" unter Verwendung der Standard-Datenbank `/usr/share/cracklib/pw_dict.pwd`, die unter dem Betriebssystem (zurzeit SLES10 SP3) installiert wird.

NOTICE: Die Passwort- und Kontoregeln treten in Kraft, wenn die entsprechenden Kontrollkästchen aktiviert werden. Das Befehlszeilenprogramm "`passwd`" ist deaktiviert!

Feldbeschreibungen

Erweiterte Passwort-Regeln verwenden (Passwortchronik; erweiterte Passwortkomplexität)

Geschäftszeiten aktivieren

Konto wird gesperrt nach: xx Tagen Inaktivität

Passwort muss ablaufen nach: xx Tagen

Verwandte Themen

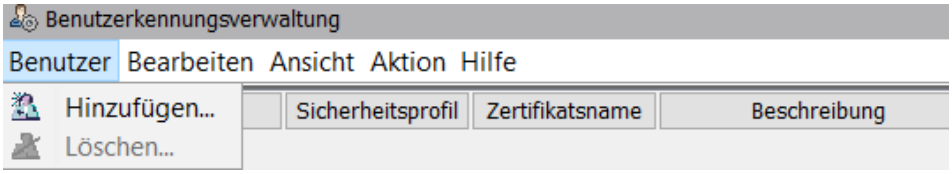
Passwort ändern

Emergency Password Reset (EPR)

2.8 Benutzerkennungsverwaltung

Das Dialogfeld **Benutzerkennungsverwaltung** wird verwendet, um Benutzer hinzuzufügen oder zu löschen bzw. um die Passwort-Eigenschaften eines bestimmten Benutzers oder einer Benutzergruppe zu ändern.

Um die Zugriffsrechte dieser Benutzer zu ändern, verwenden Sie das Dialogfeld **Zugriffsrechtekonfiguration**.



Linker Bereich (Benutzerliste)

Im linken Teil des Dialogfelds wird die Liste der Benutzerkennungen, Dialogfeld "Benutzerkennungsverwaltung" mit allen derzeit registrierten Benutzern und ihren Kennungseinstellungen angezeigt.

Mehrere Benutzer markieren

In diesem Dialogfeld können Sie mehrere Benutzernamen gleichzeitig markieren und die Eigenschaftswerte aller gewählten Benutzer mit einem einzigen Mausklick einheitlich definieren bzw. ändern. Sobald Sie auf **Anwenden** klicken, weist eine Meldung in einem Bearbeitungs-Dialogfeld darauf hin, dass die Passwort-Eigenschaften mehrerer Benutzerkennungen geändert werden.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Rechter Bereich

Der rechte Teil des Dialogfelds **Benutzerkennungsverwaltung** enthält folgende Bereiche:

- **Bereich "Identifizierung"**,
- Bereich "Aktionen",
- Bereich "Eigenschaften",
- Bereich "Automatisches Sperren".

Diese dienen zum Festlegen oder Ändern der Eigenschaften von vorhandenen oder neuen Benutzerkennungen. Eine detaillierte Beschreibung dieses Bereichs finden Sie in Bereiche im Dialogfeld "Benutzerkennungsverwaltung" auf page 322, und Steuerungselemente und Schaltflächen im Dialogfeld "Benutzerkennungsverwaltung" auf page 324.

Das Dialogfeld **Benutzerkennungsverwaltung** enthält folgende Komponenten:

- Liste der Benutzerkennungen, Dialogfeld "Benutzerkennungsverwaltung"
- Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"
- Menüleiste
- Symbolleiste

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine detaillierte Beschreibung aller Symbolschaltflächen finden Sie

unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung".

- Kontextmenü
- Menü Benutzer
- Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung
- Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung"
- Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung"
- Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"
- Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche
- Spalten im Dialogfeld "Benutzerkennungsverwaltung"
- Bereiche im Dialogfeld "Benutzerkennungsverwaltung"
  - **Bereich "Identifizierung"**,
  - Bereich "Aktionen",
  - Bereich "Eigenschaften",
  - Bereich "Automatisches Sperren".
- Steuerungselemente und Schaltflächen im Dialogfeld "Benutzerkennungsverwaltung"

Feldbeschreibungen

Kennung

Sicherheitsprofil

Beschreibung

Neues Passwort

Passwort-Eingabe wiederholen

Passwort löschen

Änderung des Passworts erzwingen

Max. Passwort-Gültigkeit

Passwort ist unbegrenzt gültig

Kennung sperren

Passwort-Änderung erlaubt

Zugang nur über Network Single Logon

Kennung automatisch sperren

während

Automatisch wieder entsperren

Anwenden

Verwerfen

Aktualisieren

Verwandte Themen

Spalten im Dialogfeld "Systemkennungsverwaltung"

Bereiche im Dialogfeld "Systemkennungsverwaltung"

Steuerungselemente und Schaltflächen im Dialogfeld "Systemkennungsverwaltung"

Export von Benutzerdaten

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.8.1 Liste der Benutzerkennungen, Dialogfeld "Benutzerkennungsverwaltung"

Liste der Benutzerkennungen - Anzeige der eingerichteten Benutzerdaten, Berechtigungen und Eigenschaften

Die **Benutzerliste** in der **linken Hälfte** des Dialogfelds **Benutzerkennungsverwaltung** zeigt alle in der **Zugangsverwaltung** eingetragenen Benutzer. Eine Beschreibung der eingerichteten Benutzerdaten finden Sie in: Spalten im Dialogfeld "Benutzerkennungsverwaltung"

Liste der Benutzerkennungen - Ändern der Benutzerdaten und Passwort-Einstellungen

Die in der **rechten Hälfte** des Dialogfelds **Benutzerkennungsverwaltung** angezeigten Bereiche im Dialogfeld "Benutzerkennungsverwaltung" enthalten die Felder und Steuerelemente für das Ändern der Benutzerdaten und der Passwort-Einstellungen.

- **Bereich "Identifizierung"**,
- Bereich "Aktionen",
- Bereich "Eigenschaften",
- Bereich "Automatisches Sperren".

NOTICE: Nur Benutzer mit entsprechender Administrator-Berechtigung sind berechtigt, Passwort-Einstellungen zu ändern.

Verwandte Themen

Benutzerkennungsverwaltung

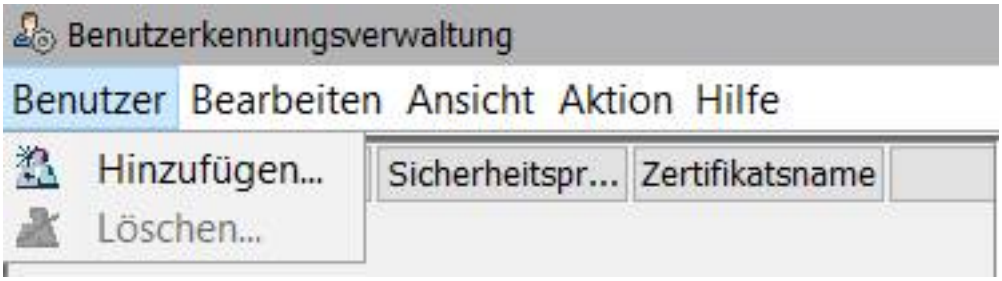
Passwort ändern

Menü Benutzer

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

2.8.2 Menü Benutzer

Das Menü **Benutzer** erscheint nur im Dialogfeld Benutzerkennungsverwaltung. In diesem Menü können Sie neue Benutzer hinzufügen oder bereits vorhandene Benutzer löschen. Sie finden hier folgende Einträge:



- **Hinzufügen**

  Wenn Sie im Menü **Benutzer** auf **Hinzufügen** klicken, wird das Dialogfeld Neue Benutzerkennung hinzufügen geöffnet. Die gleiche Funktion können Sie auch über das Kontextmenü und über die entsprechende Symbolschaltfläche in der Symbolleiste aufrufen.
- **Löschen**

  Wenn Sie im Menü **Benutzer** auf **Löschen** klicken, wird das Dialogfeld Benutzerkennungen löschen geöffnet. Die gleiche Funktion können Sie auch über das Kontextmenü und über die entsprechende Symbolschaltfläche in der Symbolleiste aufrufen.

Verwandte Themen

Symbolleiste

Menüleiste

Kontextmenü

Neue Benutzerkennung hinzufügen

Benutzerkennungen löschen

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

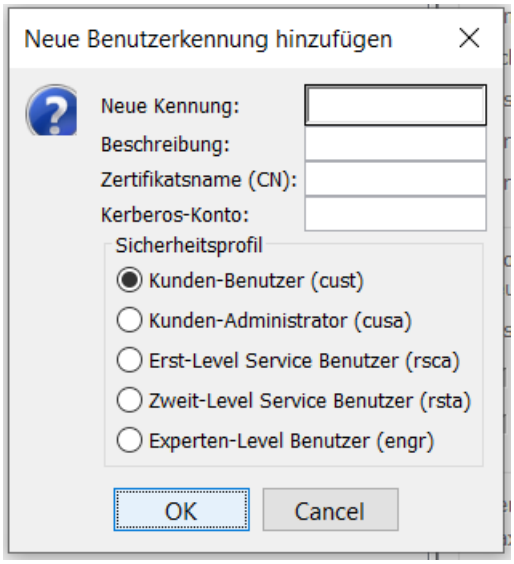
Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

Export von Benutzerdaten

2.8.3 Neue Benutzerkennung hinzufügen

Das Dialogfeld **Neue Benutzerkennung hinzufügen** wird angezeigt, wenn Sie im Menü Benutzer oder im Kontextmenü auf **Hinzufügen** oder in der Symbolleiste auf das entsprechende Symbol klicken.



Um einen neuen Benutzer hinzuzufügen, müssen Sie:

- den Namen des neuen Benutzers im Feld Neue Kennung eingeben,

  NOTICE: WICHTIG für V8R0: Der Kontoname muss mindestens drei Zeichen enthalten, darf nicht länger als 32 Zeichen sein, muss mit einem Kleinbuchstaben beginnen ('a'..'z'), und darf nur 'a'..'z', '0'..'9' und '-' enthalten.

- Geben Sie im Feld Beschreibung eine Kurzbeschreibung für den neuen Benutzernamen (Kennung) ein und
- weisen Sie diesem Benutzer im Feld **Zertifikatsname (CN)** ein Zertifikat (Eigenschaft Allgemeiner Name) zu; wenn auf dem System keine PKI-Authentifizierung verwendet wird, kann dieses Feld leer bleiben.
- Aktivieren Sie eines der Optionsfelder für das **Sicherheitsprofil** des neuen Benutzers:
  - Kunden-Benutzer (cust),
  - Kunden-Administrator (cusa),
  - Erst-Level Service Benutzer (rsca),
  - Zweit-Level Service Benutzer (rsta) oder
  - Experten-Level Benutzer (engr).

  Die Zugriffsrechte des neuen Accounts werden vom Sicherheitsprofil vererbt und stellen die selben Funktionalitäten bereit, wie sie in den vordefinierten Accounts vorliegen. Für genauere Informationen über Benutzerkennungen, siehe Sicherheitsebenen und vordefinierte Benutzerkennungen auf page 10.
- Bestätigen Sie die neue Kennung, indem Sie auf die Schaltfläche OK klicken oder
- brechen Sie die Eingabe ab. Klicken Sie hierfür auf **Abbrechen**.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü Benutzer

oder

über die Kontextmenü

oder

über die Symbolleiste

Verwandte Themen

Symbolleiste

Menüleiste

Kontextmenü

Menü Benutzer

Benutzerkennungen löschen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

Export von Benutzerdaten

Siehe auch

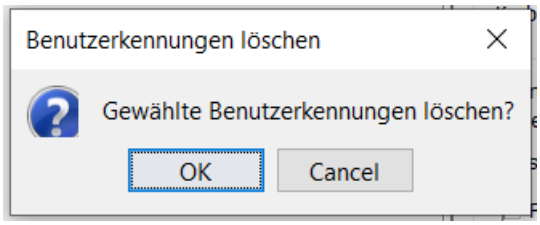
Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Benutzerkennungsverwaltung und Systemkennungsverwaltung - Beschreibung der Felder

Neue Benutzerkennung hinzufügen - Beschreibung der Felder.

2.8.4 Benutzerkennungen löschen

Wenn Sie im Menü **Benutzer** auf **Löschen** oder die entsprechende **Schaltfläche in der Symbolleiste** klicken, wird das Dialogfeld **Benutzerkennungen löschen** geöffnet, in dem Sie aufgefordert werden, den Löschvorgang zu bestätigen.



- Klicken Sie auf **OK**, um das Löschen aller gewählten Benutzer zu bestätigen.
- Klicken Sie auf **Abbrechen**, um den Löschvorgang abzubrechen.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü Benutzer

oder

über die Kontextmenü

oder

über die Symbolleiste

Siehe auch

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Benutzerkennungsverwaltung und Systemkennungsverwaltung - Beschreibung der Felder

Verwandte Themen

Symbolleiste

Menüleiste

Kontextmenü

Menü Benutzer

Neue Benutzerkennung hinzufügen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

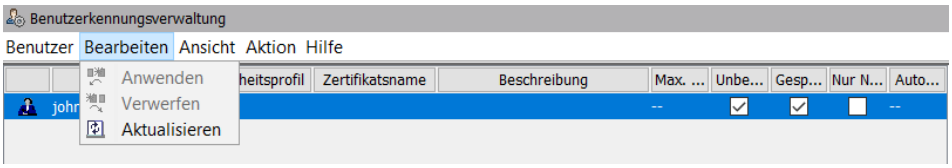
Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

Export von Benutzerdaten

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.8.5 Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Das Menü **Bearbeiten** wird in allen Dialogfeldern des Bereichs **Kennungsverwaltung** angezeigt. Sie finden hier folgende Einträge:



Menüoptionen

Anwenden	Wenn Sie im Menü **Bearbeiten** auf **Anwenden** klicken, werden die vereinbarten Eigenschaften für alle gewählten Kennungen übernommen. Dieser Befehl hat die gleiche Funktion wie die Schaltfläche **Anwenden** im unteren rechten Teil des Bildschirmanzeige und wie die Symbolschaltfläche **Änderungen übernehmen** in der Symbolleiste. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.
Verwerfen	Wenn Sie im Menü **Bearbeiten** auf **Verwerfen** klicken, werden alle vereinbarten Änderungen für den bzw. die gewählten Benutzer verworfen. Dieser Befehl hat die gleiche Funktion wie die Schaltfläche **Verwerfen** im unteren rechten Teil des Bildschirmanzeige und wie die Symbolschaltfläche **Änderungen verwerfen** in der Symbolleiste. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

Reload	Wenn Sie im Menü **Bearbeiten** auf **Aktualisieren** klicken, wird der Inhalt des Dialogfelds **Benutzerkennungsverwaltung** aktualisiert. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Dieser Befehl hat die gleiche Funktion wie die Symbolschaltfläche **Daten vom Server aktualisieren** in der Symbolleiste.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Bevor Sie Befehle ausführen, müssen Sie die gewünschten Elemente (Benutzerkennungen) markieren.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Symbolleiste

Menüleiste

Kontextmenü

Menü Benutzer

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung"

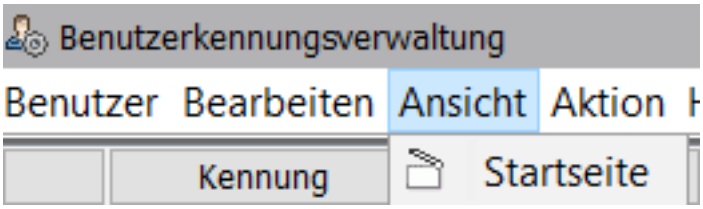
Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung"

Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

Export von Benutzerdaten

2.8.6 Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung"

Das Menü **Ansicht** enthält - je nach Software-Komponente - unterschiedliche Optionen. Bei den Komponenten Benutzerkennungsverwaltung und Systemkennungsverwaltung enthält das Menü **Ansicht** die Option **Startseite**.



Die Option **Startseite** im Menü **Ansicht** hat dieselbe Funktion wie die Symbolschaltfläche **Startseite anzeigen** in der Symbolleiste.

Wenn Sie auf die Menüoption **Startseite** oder auf das Symbol klicken, öffnet sich ein neues Browserfenster, in dem die **Startseite** von OpenScape 4000 Assistant/Manager angezeigt wird. Dort werden alle Anwendungen angezeigt, auf die der momentan angemeldete Benutzer Zugriff hat.

Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung".

Verwandte Themen

Symbolleiste

Menüleiste

Menü Benutzer

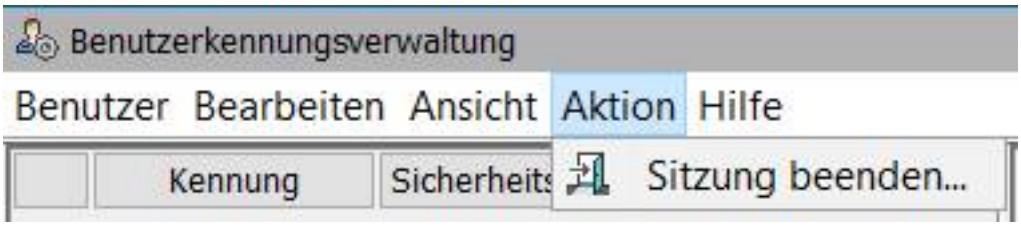
Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung"

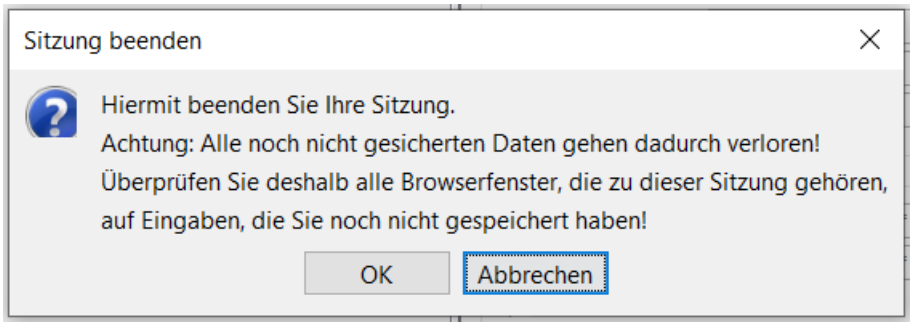
Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

2.8.7 Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung"

Das Menü **Aktion** enthält die Option **Sitzung beenden**. Diese hat die gleiche Funktion wie die Symbolschaltfläche **Sitzung beenden** in der Symbolleiste, Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung".



Sobald Sie auf **Sitzung beenden** klicken, erscheint eine Warnmeldung, die darauf hinweist, dass sämtliche nicht gespeicherten Sitzungsdaten verloren gehen. Sie werden aufgefordert, alle Sitzungsdaten zu speichern und das Verlassen der Sitzung zu bestätigen.



Verwandte Themen

Symbolleiste

Menüleiste

Menü Benutzer

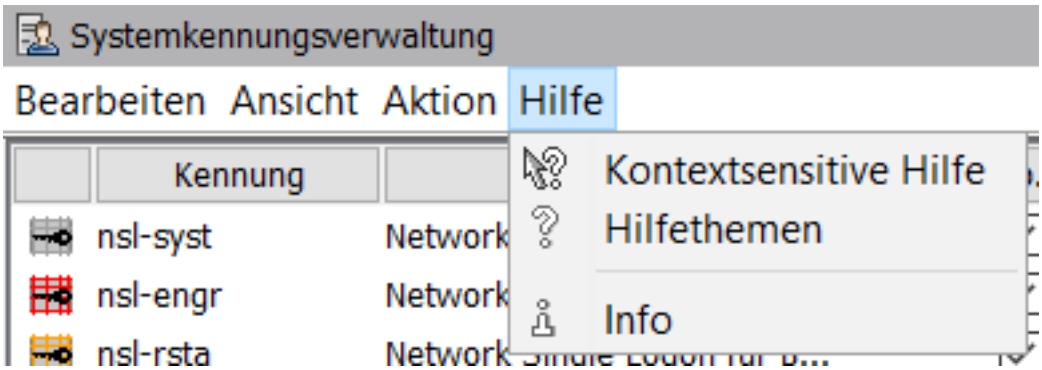
Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung"

Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

2.8.8 Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung"

Das Menü **Hilfe** wird bei allen Komponenten des Bereichs **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**. Das Menü **Hilfe** enthält bei allen Komponenten dieselben Optionen, und zwar:



Kontextsensitive Hilfe	Wenn Sie auf **Kontextsensitive Hilfe** klicken, wird die kontextbezogene Online-Hilfe zu der per Mausklick markierten Position aufgerufen. Die Kontextsensitive Hilfe können Sie auch aufrufen, indem Sie mit der Maus auf eine bestimmte Position der Bedienoberfläche klicken und die Tastenkombination **STRG+F1** betätigen.
Hilfe-Themen	Wenn Sie auf die **Hilfethemen** klicken, wird das Inhaltsverzeichnis der Online-Hilfe geöffnet. Die Online-Hilfe kann auch über die Taste **F1** aufgerufen werden.
Info	Im Dialogfenster **Info** werden die Informationen über die Programmversion der Software, das Erscheinungsjahr und die urheberrechtlichen Bestimmungen angezeigt.

Verwandte Themen

Symbolleiste

Menüleiste

Menü Benutzer

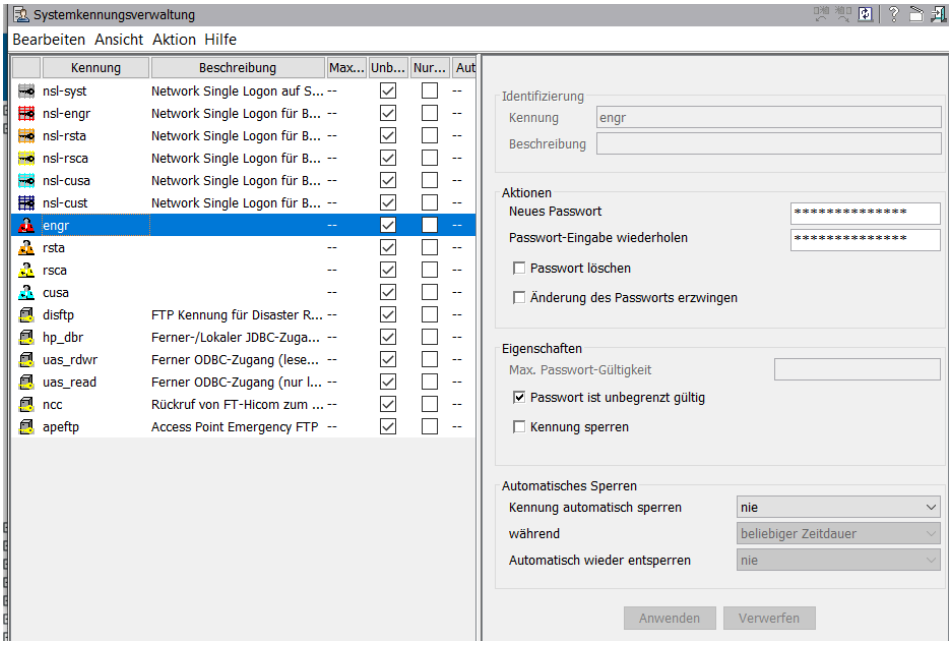
Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung"

Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung"

2.9 Systemkennungsverwaltung

Das Dialogfeld **Systemkennungsverwaltung** wird benutzt, um eine bestimmte Benutzergruppe (NSL und Systemkennungen) zu verwalten, d. h., um Systemkennungen hinzuzufügen oder zu löschen bzw. um die Passwort-Eigenschaften einer bestimmten Kennung oder einer Gruppe von Kennungen zu ändern. Zugriffsrecht-Modifikationen für bestimmte Benutzerkennungen oder Gruppen von Kennungen sollten Sie über das Programm Zugangsverwaltung -> **Zugriffsrechtekonfiguration** vornehmen.



Linker Bereich

Die Spalten im **linken** Teil des Dialogfelds bieten einen Überblick über alle derzeit verfügbaren Benutzerkennungen. In diesem Dialogfeld können Sie mehrere Benutzerkennungen gleichzeitig markieren und die Eigenschaftswerte aller gewählten Benutzer mit einem einzigen Mausklick einheitlich definieren bzw. ändern. Die Benutzeroberfläche entspricht in etwa dem Dialogfeld **Benutzerkennungsverwaltung**.

Sobald Sie auf **Anwenden** klicken, weist eine Meldung in einem Bearbeitungs-Dialogfeld darauf hin, dass die Passwort-Eigenschaften mehrerer Benutzerkennungen geändert werden.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Rechter Bereich

Der **rechte** Teil des Dialogfelds **Benutzerkennungsverwaltung** enthält folgende Bereiche:

- Bereich "Identifizierung",
- Bereich "Aktionen",
- Bereich "Eigenschaften",
- Bereich "Automatisches Sperren".

Diese dienen zum Festlegen oder Ändern der Eigenschaften von vorhandenen oder neuen Systemkennungen verwendet werden. Eine detaillierte Beschreibung dieses Bereichs finden Sie in Bereiche im Dialogfeld "Systemkennungsverwaltung" auf page 327, und Steuerungselemente und Schaltflächen im Dialogfeld "Systemkennungsverwaltung" auf page 329.

Der Inhalt der Benutzerliste hängt von den serverseitig eingerichteten Systemkennungen sowie von der Zugriffsrechten des momentan angemeldeten Benutzers ab - d. h.

Es gibt drei verschiedene Arten von Kennungen. Jede Art ist durch ein eigenes Symbol gekennzeichnet:

- **Systemkennungen**: Linux-Kennungen für verschiedene Einsatzbereiche. Über diese Kennungen wird die korrekte Funktion der OpenScape 4000-Leistungsmerkmale und die Kommunikation zu den Partnersystemen sichergestellt. Diese Kennungen werden nicht für interaktive Anmeldung verwendet.
- **Vordefinierte Administrator-Kennungen**: Kennungen für die Anmeldung von Administratoren mit eingeschränkten Zugriffsrechten.
- **Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL accounts)** Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird. Beachten sie, dass in der Voreinstellung alle NSL Kennungen offen sind! Das bedeutet, dass der uneingeschränkte Zugang zum Server über Network Single Logon ohne jeden Passwortschutz möglich ist, solange die Passwörter im Dialogfeld **Systemkennungsverwaltung** nicht gesetzt sind!

Eine Liste aller Kategorien von Kennungen sowie der einzelnen Kennungen finden Sie in Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen.

Komponenten der Benutzeroberfläche

Das Dialogfeld **Systemkennungsverwaltung** enthält folgende Elemente:

- Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

- Symbolleiste

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine Beschreibung aller Symbolschaltflächen finden Sie unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung".
- Menüleiste
- Kontextmenü
- Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"
- Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"
- Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung"
- Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung"
- Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche
- Spalten im Dialogfeld "Systemkennungsverwaltung"
- Bereiche im Dialogfeld "Systemkennungsverwaltung"
  - Bereich "Identifizierung"
  - Bereich "Aktionen"
  - Bereich "Eigenschaften"
  - Bereich "Automatisches Sperren"
- Steuerungselemente und Schaltflächen im Dialogfeld "Systemkennungsverwaltung"
- Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Feldbeschreibungen

Kennung

Beschreibung

Neues Passwort

Passwort-Eingabe wiederholen

Passwort löschen

Änderung des Passworts erzwingen

Max. Passwort-Gültigkeit

Passwort ist unbegrenzt gültig

Kennung sperren

Kennung automatisch sperren

während

Automatisch wieder entsperren

Anwenden

Verwerfen

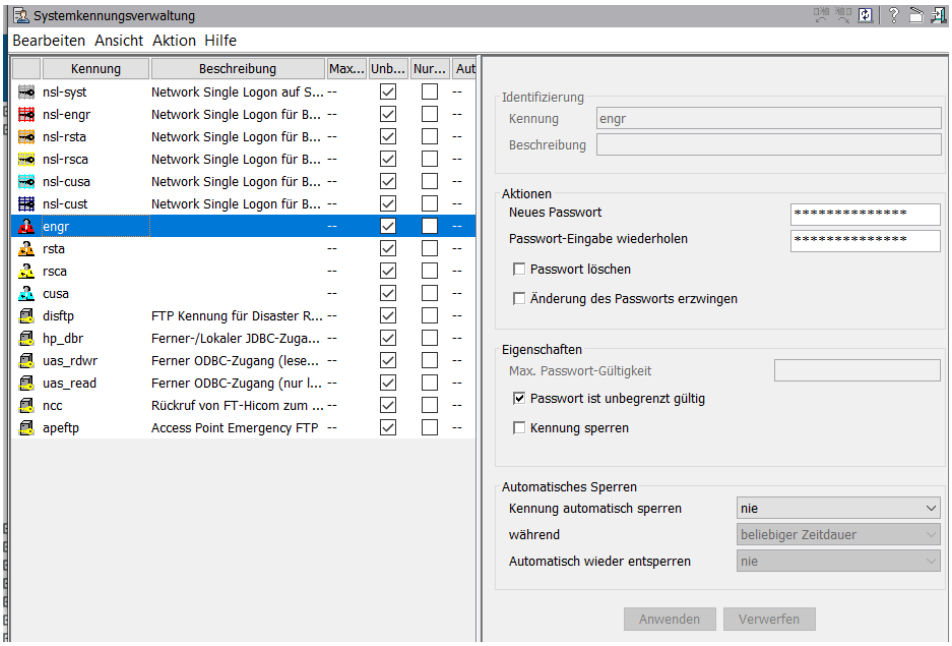
Aktualisieren

Verwandte Themen

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.9.1 Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"



Linker Bereich

Die Spalten im **linken** Teil des Dialogfelds bieten einen Überblick über alle derzeit verfügbaren Systemkennungen. In diesem Dialogfeld können Sie mehrere Systemkennungen gleichzeitig markieren und die Eigenschaftswerte aller gewählten Benutzer mit einem einzigen Mausklick einheitlich definieren bzw. ändern. Die Benutzeroberfläche entspricht in etwa dem Dialogfeld **Benutzerkennungsverwaltung**.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Rechter Bereich

Der **rechte** Teil des Dialogfelds **Benutzerkennungsverwaltung** enthält folgende Bereiche:

- Bereich "Identifizierung"
- Bereich "Aktionen"
- Bereich "Eigenschaften"
- Bereich "Automatisches Sperren"

Diese dienen zum Festlegen oder Ändern der Eigenschaften von vorhandenen oder neuen Systemkennungen verwendet werden. Eine detaillierte Beschreibung dieses Bereichs finden Sie in Bereiche im Dialogfeld "Systemkennungsverwaltung" auf page 327, und Steuerungselemente und Schaltflächen im Dialogfeld "Systemkennungsverwaltung" auf page 329.

Der Inhalt der Benutzerliste hängt von den serverseitig eingerichteten Systemkennungen sowie von der Zugriffsrechten des momentan angemeldeten Benutzers ab - d. h.

Es gibt drei verschiedene Arten von Kennungen. Jede Art ist durch ein eigenes Symbol gekennzeichnet:

- **Systemkennungen**: Linux-Kennungen für verschiedene Einsatzbereiche. Über diese Kennungen wird die korrekte Funktion der OpenScape 4000-Leistungsmerkmale und die Kommunikation zu den Partnersystemen sichergestellt. Diese Kennungen werden nicht für interaktive Anmeldung verwendet.
- **Vordefinierte Administrator-Kennungen**: Kennungen für die Anmeldung von Administratoren mit eingeschränkten Zugriffsrechten.
- **Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL accounts)** Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird. Beachten sie, dass in der Voreinstellung alle NSL Kennungen offen sind! Das bedeutet, dass der uneingeschränkte Zugang zum Server über Network Single Logon ohne jeden Passwortschutz möglich ist, solange die Passwörter im Dialogfeld **Systemkennungsverwaltung** nicht gesetzt sind!

Eine Liste aller Kategorien von Kennungen sowie der einzelnen Kennungen finden Sie in Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen.

Verwandte Themen

Benutzerkennungsverwaltung

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"

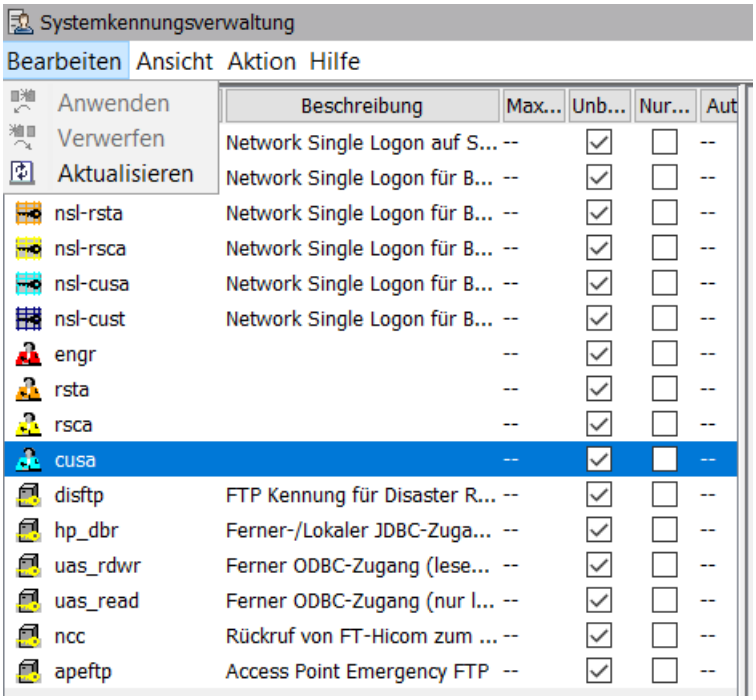
Symbolleiste

Kontextmenü

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.9.2 Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Das Menü **Bearbeiten** wird in allen Dialogfeldern des Bereichs **Kennungsverwaltung** angezeigt. Im Dialogfeld **Systemkennungsverwaltung** enthält dieses Menü folgende Einträge:



Menüoptionen

Anwenden	Wenn Sie im Menü **Bearbeiten** auf **Anwenden** klicken, werden die vereinbarten Eigenschaften für alle gewählten Kennungen übernommen. Dieser Befehl hat die gleiche Funktion wie die Schaltfläche **Anwenden** im unteren rechten Teil des Bildschirmanzeige und wie die Symbolschaltfläche **Änderungen übernehmen** in der Symbolleiste. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.
Verwerfen	Wenn Sie im Menü **Bearbeiten** auf **Verwerfen** klicken, werden alle vereinbarten Änderungen für den bzw. die gewählten Benutzer verworfen. Dieser Befehl hat die gleiche Funktion wie die Schaltfläche **Verwerfen** im unteren rechten Teil des Bildschirmanzeige und wie die Symbolschaltfläche **Änderungen verwerfen** in der Symbolleiste. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.
Reload	Wenn Sie im Menü **Bearbeiten** auf **Aktualisieren** klicken, wird der Inhalt des Dialogfelds **Benutzerkennungsverwaltung** aktualisiert. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Dieser Befehl hat die gleiche Funktion wie die Symbolschaltfläche **Daten vom Server aktualisieren** in der Symbolleiste.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung" oder über die Kontextmenü oder über die Symbolleiste

Markieren von Elementen

Bevor Sie Befehle ausführen, müssen Sie die gewünschten Elemente (Benutzerkennungen) markieren.

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Symbolleiste

Menüleiste

Kontextmenü

Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung"

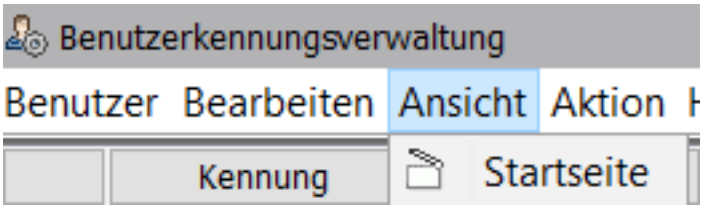
Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.9.3 Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"

Das Menü **Ansicht** enthält - je nach Software-Komponente - unterschiedliche Optionen. Bei den Komponenten Benutzerkennungsverwaltung und Systemkennungsverwaltung enthält das Menü **Ansicht** die Option **Startseite**.



Die Option **Startseite** im Menü **Ansicht** hat dieselbe Funktion wie die Symbolschaltfläche **Startseite anzeigen** in der Symbolleiste.

Wenn Sie auf die Menüoption **Startseite** oder auf das Symbol klicken, öffnet sich ein neues Browserfenster, in dem die **Startseite** von OpenScape 4000 Assistant/Manager angezeigt wird. Dort werden alle Anwendungen angezeigt, auf die der momentan angemeldete Benutzer Zugriff hat.

Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung".

Verwandte Themen

Symbolleiste

Menüleiste

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung"

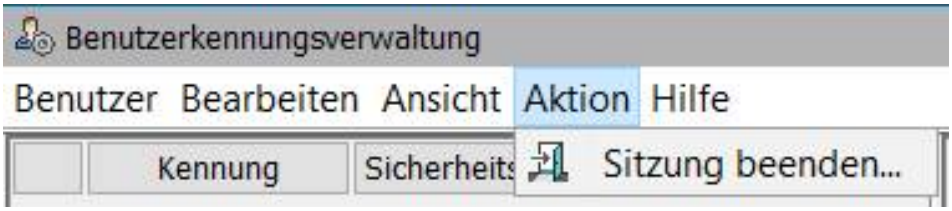
Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

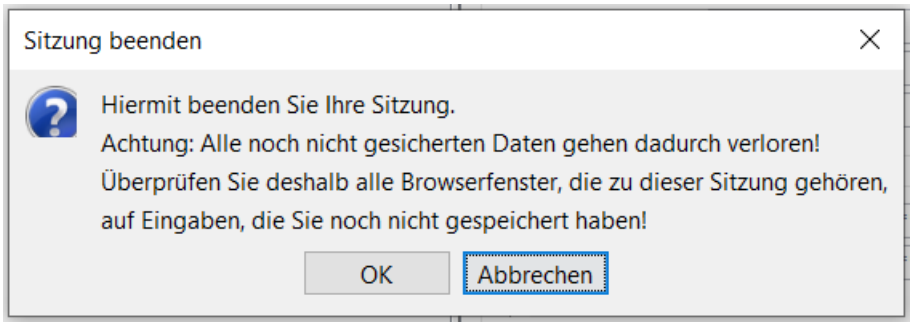
Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.9.4 Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung"

Das Menü **Aktion** enthält die Option **Sitzung beenden**. Diese hat die gleiche Funktion wie die Symbolschaltfläche **Sitzung beenden** in der Symbolleiste, Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung".



Sobald Sie auf **Sitzung beenden** klicken, erscheint eine Warnmeldung, die darauf hinweist, dass sämtliche nicht gespeicherten Sitzungsdaten verloren gehen. Sie werden aufgefordert, alle Sitzungsdaten zu speichern und das Verlassen der Sitzung zu bestätigen.



Verwandte Themen

Symbolleiste

Menüleiste

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"

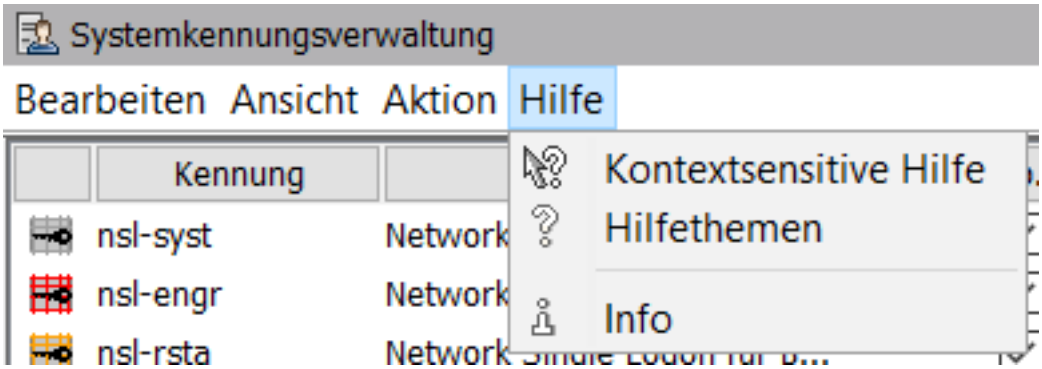
Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.9.5 Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung"

Das Menü **Hilfe** wird bei allen Komponenten der Komponente **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**. Das Menü **Hilfe** enthält bei allen Komponenten dieselben Optionen, und zwar:



Kontextsensitive Hilfe	Wenn Sie auf **Kontextsensitive Hilfe** klicken, wird die kontextbezogene Online-Hilfe zu der per Mausklick markierten Position aufgerufen. Die Kontextsensitive Hilfe können Sie auch aufrufen, indem Sie mit der Maus auf eine bestimmte Position der Bedienoberfläche klicken und die Tastenkombination **STRG+F1** betätigen.
Hilfe-Themen	Wenn Sie auf die **Hilfethemen** klicken, wird das Inhaltsverzeichnis der Online-Hilfe geöffnet. Die Online-Hilfe kann auch über die Taste **F1** aufgerufen werden.
Info	Im Dialogfenster **Info** werden die Informationen über die Programmversion der Software, das Erscheinungsjahr und die urheberrechtlichen Bestimmungen angezeigt.

Verwandte Themen

Symbolleiste

Menüleiste

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung"

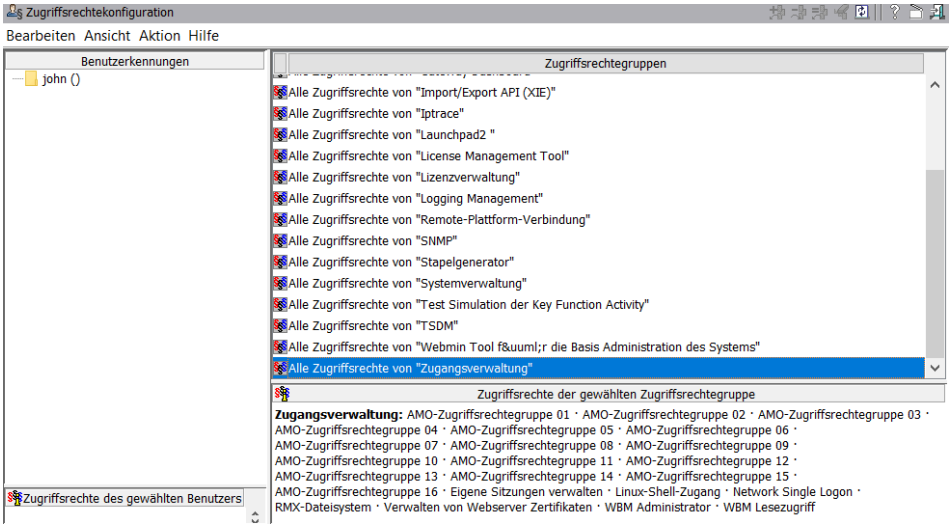
Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung"

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.10 Zugriffsrechtekonfiguration

Im Dialogfeld **Zugriffsrechtekonfiguration** können Sie den Benutzern verfügbare Zugriffsrechtegruppen (für die Anwendungsausführung) zuweisen.



Vereinfacht wird der Prozess für die selektive Zuweisung von Zugriffsrechten dadurch, dass man "Zugriffsrechtegruppen" festlegen kann.

Nach der Installation stehen vordefinierte Zugriffsrechtegruppen zur Verfügung. Im Dialogfeld **Zugriffsrechtegruppen-Konfiguration** können zusätzliche Zugriffsrechtegruppen erzeugt und modifiziert werden. Änderungen, die in einer Zugriffsrechtegruppe vorgenommen werden, gelten automatisch für alle Benutzer, denen diese Gruppe zugewiesen ist.

Das Dialogfeld **Zugriffsrechtekonfiguration** ist vertikal unterteilt und umfasst zwei nebeneinander angeordnete Bereiche:

Benutzerkennungen (linker Bereich)

Im linken Bereich, unter dem Titel Benutzerkennungen, werden in einer zweistufigen Baumstruktur alle verfügbaren **Benutzer** (obere Ebene) sowie die ihnen zugeordneten Zugriffsrechtegruppen (untergeordnete Ebene) angezeigt.

Zugriffsrechtegruppen (rechter Bereich)

Im rechten Teil, unter **Zugriffsrechtegruppen**, werden alle zuweisbaren Zugriffsrechtegruppen angezeigt.

Vorschaufenster

Am unteren Rand beider Bereiche befindet sich je ein **Vorschaufenster**, das ein- und ausgeblendet werden kann. Im Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration" werden die Eigenschaften des ausgewählten Benutzers bzw. der Zugriffsrechtegruppe angezeigt. Die Höhe der Vorschaufenster ist veränderbar.

Beide Bereiche - sowohl die Baumstruktur der Benutzerkennungen als auch die Liste der Zugriffsrechtegruppen - verfügen über erweiterte Auswahlmöglichkeiten; die Menüfunktionen werden je nach Auswahl in diesen Baumstrukturen aktiviert, und zwar sowohl in den Standard-Menüs als auch im Kontextmenü.

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Benutzerkennungen bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die Umschalttaste und

markieren Sie bei gedrückter **Umschalttaste** die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Komponenten der Benutzeroberfläche im Dialogfeld "Zugriffsrechtekonfiguration"

Das Dialogfeld **Zugriffsrechtekonfiguration** enthält folgende Elemente:

- Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine detaillierte Beschreibung aller Symbolschaltflächen finden Sie unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration".
- Menüleiste
- Symbolleiste

  Für eine detaillierte Beschreibung aller Symbolschaltflächen, siehe Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration".
- Kontextmenü
- Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"
- Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration"

  Die Option **Vorschaufenster für Zugriffsrechte** im Menü **Ansicht** dient zum Einblenden/Ausblenden der **Vorschaufenster**.

  Weitere Informationen zu den Vorschaufenstern finden Sie unter . Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".
- Menü "Aktion", Leistungsmerkmal "Zugriffsrechtekonfiguration"
- Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtekonfiguration"
- Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"
- Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

Verwandte Themen

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

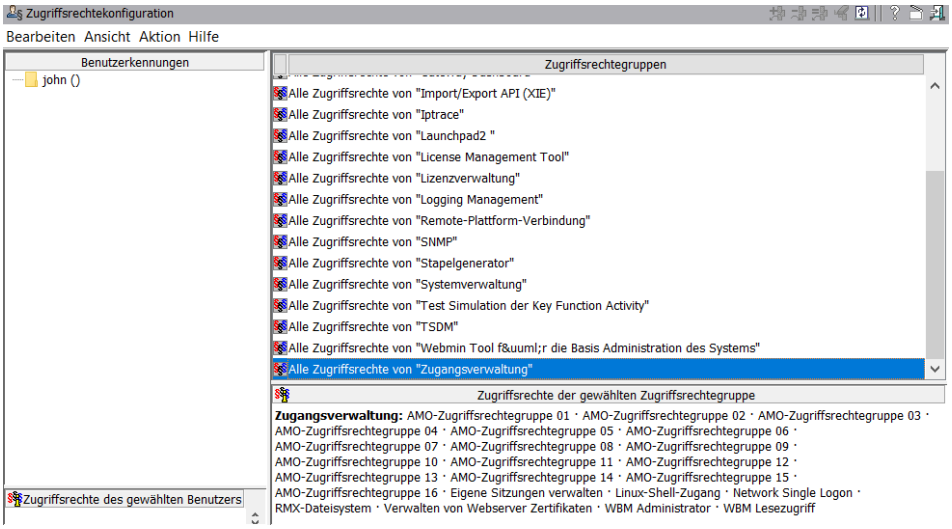
Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

2.10.1 Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"



Das Dialogfeld **Zugriffsrechtekonfiguration** ist vertikal unterteilt und umfasst zwei nebeneinander angeordnete Bereiche:

- "Benutzerkennungen" (linker Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

  Im linken Bereich, unter dem Titel **Benutzerkennungen**, werden in einer zweistufigen Baumstruktur alle verfügbaren Benutzer (obere Ebene) sowie die ihnen zugeordneten Zugriffsrechtegruppen (untergeordnete Ebene) angezeigt.
- "Zugriffsrechtegruppen" (rechter Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

  Im rechten Teil, unter **Zugriffsrechtegruppen**, werden alle zuweisbaren Zugriffsrechtegruppen angezeigt.

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Benutzerkennungen bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die Umschalttaste und markieren Sie bei gedrückter **Umschalttaste** die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

- Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

  Am unteren Rand beider Bereiche befindet sich je ein **Vorschaufenster**, das ein- und ausgeblendet werden kann. Im Vorschaufenster werden die Eigenschaften des ausgewählten Benutzers bzw. der Zugriffsrechtegruppe angezeigt. Die Höhe der Vorschaufenster ist veränderbar.

  Beide Bereiche - sowohl die Baumstruktur der Benutzerkennungen als auch die Liste der Zugriffsrechtegruppen - verfügen über erweiterte Auswahlmöglichkeiten; die Menüfunktionen werden je nach Auswahl in diesen Baumstrukturen aktiviert.

- Symbolleiste

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine Beschreibung aller Symbolschaltflächen finden Sie unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration".
- Menüleiste

Weitere Details zu den Bereichen finden Sie unter:

"Benutzerkennungen" (linker Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

"Zugriffsrechtegruppen" (rechter Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration"

Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Verwandte Themen

Kontextmenü

Vorschaufenster einblenden/ausblenden

Mehrere Vorschaufenster gleichzeitig anzeigen

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.10.1.1 "Benutzerkennungen" (linker Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

Zeigt eine zweistufige Baumstruktur mit allen verfügbaren **Benutzern** (oberste Ebene) sowie den zugehörigen **Zugriffsrechtegruppen** (untergeordnete Ebene) an. Jeder Benutzer ist durch einen Ordner dargestellt. Jeder Ordner enthält die diesem Benutzer zugewiesenen Zugriffsrechtegruppen. Jeder Ordner kann geöffnet werden, um die dem Benutzer zugewiesenen Zugriffsrechtegruppen anzuzeigen.

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Benutzerkennungen bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die Umschalttaste und markieren Sie bei gedrückter **Umschalttaste** die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Informationen über das Zuweisen und Entziehen von Zugriffsrechtegruppen für bestimmte Benutzer finden Sie im Abschnitt Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Siehe auch Zugriffsrechtekonfiguration, Bereiche im Dialogfeld "Zugriffsrechtekonfiguration" und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Verwandte Themen

Kontextmenü

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

2.10.1.2 "Zugriffsrechtegruppen" (rechter Bereich), Dialogfeld "Zugriffsrechtekonfiguration"

Zeigt alle Zugriffsrechtegruppen an, die Benutzern zugewiesen werden können.

Informationen über das Zuweisen und Entziehen von Zugriffsrechtegruppen für bestimmte Benutzer finden Sie im Abschnitt Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Benutzerkennungen bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die Umschalttaste und markieren Sie bei gedrückter **Umschalttaste** die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Siehe auch Zugriffsrechtekonfiguration, Bereiche im Dialogfeld "Zugriffsrechtekonfiguration" und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Verwandte Themen

Kontextmenü

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

2.10.2 Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

Zuweisen von Zugriffsrechtegruppen

Zugriffsrechtegruppen können den Benutzern wie folgt zugewiesen werden:

- Wählen Sie im rechten Fenster eine oder mehrere Gruppen. Ziehen Sie die gewählte(n) Gruppe(n) mit der Maus in das linke Fenster, und dort über alle Benutzer, denen diese Gruppen zugewiesen werden sollen.

  oder
- Wählen Sie im rechten Fenster eine oder mehrere Gruppen. Wählen Sie im linken Fenster alle Benutzer, denen diese Gruppen zugewiesen werden sollen. Es können nur Benutzernamen aus dieser Liste gewählt werden. Wählen Sie in der Menüleiste **Bearbeiten** - **Zuweisen** oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste bzw. im Kontextmenü . Mit dieser Funktion können die verfügbaren Gruppen in einem Arbeitsschritt mehreren Benutzern zugewiesen werden.

Entziehen von Zugriffsrechtegruppen

Die Gruppenzuweisung kann wie folgt wieder aufgehoben werden:

- Wählen Sie im linken Fenster alle Gruppen, die dem Benutzer entzogen werden sollen. Es können nur Gruppen aus dieser Liste gewählt werden. Wählen Sie in der Menüleiste **Bearbeiten** - **Entziehen** oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste bzw. im Kontextmenü.

  oder
- Markieren Sie im linken Bereich einen oder mehrere Benutzer, denen Sie Zugriffsrechtegruppen entziehen möchten. Im rechten Bereich werden die Zugriffsrechtegruppen angezeigt, die den markierten Benutzern entzogen werden können. Markieren Sie im rechten Bereich die Zugriffsrechtegruppen, die Sie den Benutzern entziehen möchten. Wählen Sie in der Menüleiste **Bearbeiten** - **Entziehen** oder klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste bzw. im Kontextmenü. Eine Sicherheitsabfrage wird angezeigt und die markierten Rechte werden entzogen, allerdings nur, wenn Sie im linken Bereich Benutzerkennungen markiert haben.

Sämtliche Änderungen werden umgehend an den Server übermittelt und gelten folglich für alle neuen Anmeldungen betroffener Benutzer. Die Änderungen können sich auch auf laufende Sitzungen auswirken, da die Server-Komponente der Zugangsverwaltung regelmäßig eine Benachrichtigung an andere Applikationen ausgibt.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

oder

über die Kontextmenü

oder

über das Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

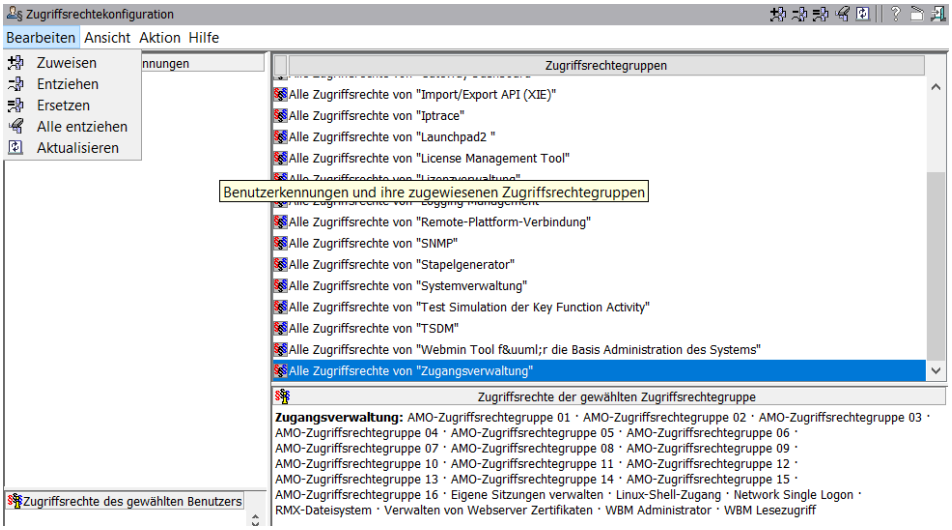
Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

2.10.3 Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Das Menü **Bearbeiten** wird in allen Dialogfeldern des Bereichs **Kennungsverwaltung** angezeigt. Im Dialogfeld **Zugriffsrechtekonfiguration** enthält dieses Menü folgende Einträge:



Menüoptionen

Zuweisen	Wenn Sie im Menü **Bearbeiten** auf **Zuweisen** klicken, werden die im rechten Bereich gewählten Zugriffsrechtegruppen allen im linken Bereich gewählten Benutzern zugewiesen. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.
Entziehen	Wenn Sie im Menü **Bearbeiten** auf **Entziehen** klicken, werden alle im linken Bereich gewählten Zugriffsrechtegruppen den zugehörigen Benutzern entzogen. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen. **Hinweis: Entziehen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Ersetzen	Wählen Sie im linken Bereich den/die gewünschten Benutzer und im rechten Bereich die Zugriffsrechtegruppen, die an Stelle der vorhandenen Zugriffsrechtegruppen eingesetzt werden sollen. Wenn Sie im Menü **Bearbeiten** auf **Ersetzen** klicken, werden die zuvor zugewiesenen Zugriffsrechtegruppen durch die aktuell markierten Zugriffsrechtegruppen ersetzt. Die vorher zugewiesenen Zuordnungen werden überschrieben. Unterschied zu **Zuweisen**: Bei **Zuweisen** werden die neuen Zugriffsrechtegruppen zu den bereits zugewiesenen Zugriffsrechtegruppen hinzugefügt, und diese werden nicht überschrieben. Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen: Über das Kontextmenü oder über die Symbolleiste. **Hinweis: Ersetzen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Alle entziehen	Markieren Sie im linken Bereich den/die Benutzer, denen alle Zugriffsrechte entzogen werden sollen. Wenn Sie im Menü **Bearbeiten** auf **Alle entziehen** klicken, werden den markierten Benutzern alle zugewiesenen Zugriffsrechte entzogen. Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen: Über das Kontextmenü oder über die Symbolleiste. **Hinweis: Alle Entziehen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Reload	Wenn Sie im Menü **Bearbeiten** auf **Aktualisieren** klicken, wird der Inhalt des Dialogfelds **Benutzerkennungsverwaltung** aktualisiert. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Dieser Befehl hat die gleiche Funktion wie die Symbolschaltfläche **Daten vom Server aktualisieren** in der Symbolleiste.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Systemkennungen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

2.10.4 Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Im Menü **Ansicht** des Dialogfelds **Zugriffsrechtekonfiguration** werden folgende Optionen angezeigt:

- **Vorschaufenster für Zugriffsrechte**

  Die Option **Vorschaufenster für Zugriffsrechte** im Menü **Ansicht** des Dialogfelds **Zugriffsrechtekonfiguration** dient zum Einblenden/Ausblenden der **Vorschaufenster**, die am unteren Rand des Dialogfeldes **Zugriffsrechtekonfiguration** angezeigt werden. In den Vorschaufenstern wird eine Kurzbeschreibung des markierten Zugriffsrechts angezeigt.

  Weitere Informationen finden Sie in Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".
- **Alle Vorschaufenster schließen**

  Mit dieser Option schließen Sie alle geöffneten Textfenster, in denen Vorschautext angezeigt wird. Um die geschlossenen Vorschaufenster wieder zu öffnen/anzuzeigen, aktivieren Sie im Menü **Ansicht** die Option **Vorschaufenster für Zugriffsrechte**.
- **Start**

  Klicken Sie auf die Option **Startseite** im Menü **Ansicht** (oder auf das Symbol **Startseite anzeigen** in der Symbolleiste), um ein neues Browser-

Fenster zu öffnen, in dem die Startseite von **OpenScape 4000 Assistant/ Manager** angezeigt wird.

Verwandte Themen

Kontextmenü

Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

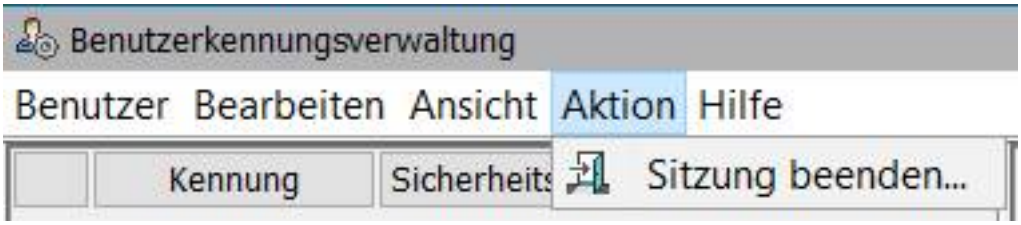
Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

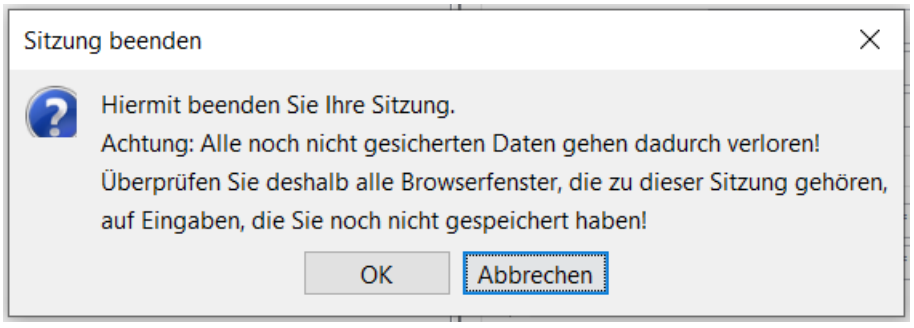
Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

2.10.5 Menü "Aktion", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Das Menü **Aktion** enthält die Option **Sitzung beenden**. Diese hat die gleiche Funktion wie die Symbolschaltfläche **Sitzung beenden** in der Symbolleiste, Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration".



Sobald Sie auf **Sitzung beenden** klicken, erscheint eine Warnmeldung, die darauf hinweist, dass sämtliche nicht gespeicherten Sitzungsdaten verloren gehen. Sie werden aufgefordert, alle Sitzungsdaten zu speichern und das Verlassen der Sitzung zu bestätigen.



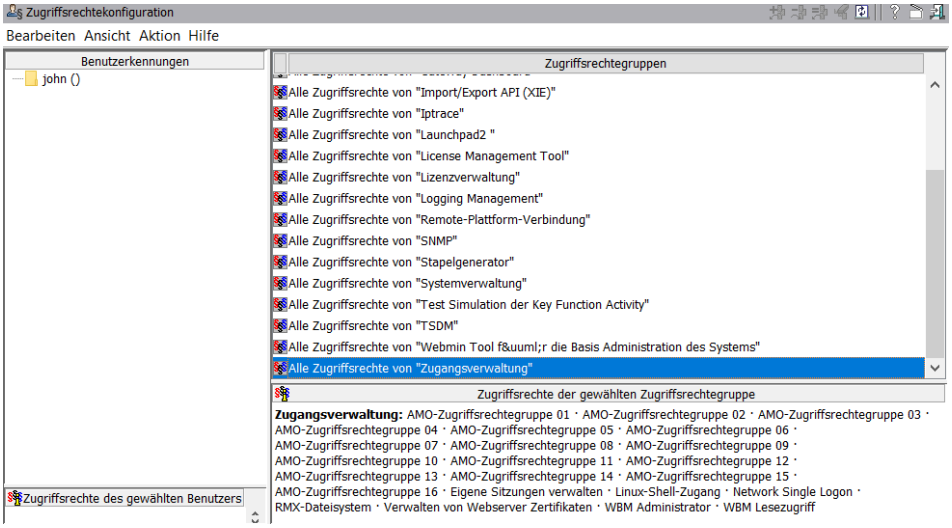
Verwandte Themen

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

2.10.6 Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"



Die Option **Vorschaufenster für Zugriffsrechte** im Menü **Ansicht** und im **Kontext** Menü des Dialogfelds **Zugriffsrechtekonfiguration** dient zum Einblenden/Ausblenden der **Vorschaufenster**, die am unteren Rand des Dialogfeldes **Zugriffsrechtekonfiguration** angezeigt werden. In den Vorschaufenstern werden Kurzbeschreibungen der markierten Zugriffsrechte bzw. aller Zugriffsrechte des markierten Benutzers angezeigt. Die Höhe der Vorschaufenster ist veränderbar.

Verwandte Themen

Vorschaufenster einblenden/ausblenden,

Mehrere Vorschaufenster gleichzeitig anzeigen,

Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Kontextmenü

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration"

2.10.6.1 Vorschaufenster einblenden/ausblenden

Die **Vorschaufenster** am unteren Rand des Dialogfelds **Zugriffsrechtekonfiguration** können durch Aktivieren/Deaktivieren der Option

Vorschaufenster für Zugriffsrechte im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration"oder im Kontextmenü eingeblendet oder ausgeblendet werden. Die Höhe der Vorschaufenster ist veränderbar.

Die Vorschaufenster zeigen alle Zugriffsrechte, die derzeit der gewählten Zugriffsrechtegruppe zugewiesen sind; Falls Sie - im linken Bereich - einen Benutzer statt einer Zugriffsrechtegruppe markiert haben, werden im linken Vorschaufenster alle Zugriffsrechte angezeigt, die derzeit diesem Benutzer zugewiesen sind, und der Titel des Vorschaufensters ändert sich in **Zugriffsrechte des gewählten Benutzers**.

Wenn Sie jedoch im linken Bereich ein bestimmtes Zugriffsrecht markiert haben, ändert sich der Titel des Vorschaufensters entsprechend und lautet jetzt **Zugriffsrechte der gewählten Zugriffsrechtegruppe**.

Verwandte Themen

Kontextmenü

Mehrere Vorschaufenster gleichzeitig anzeigen,

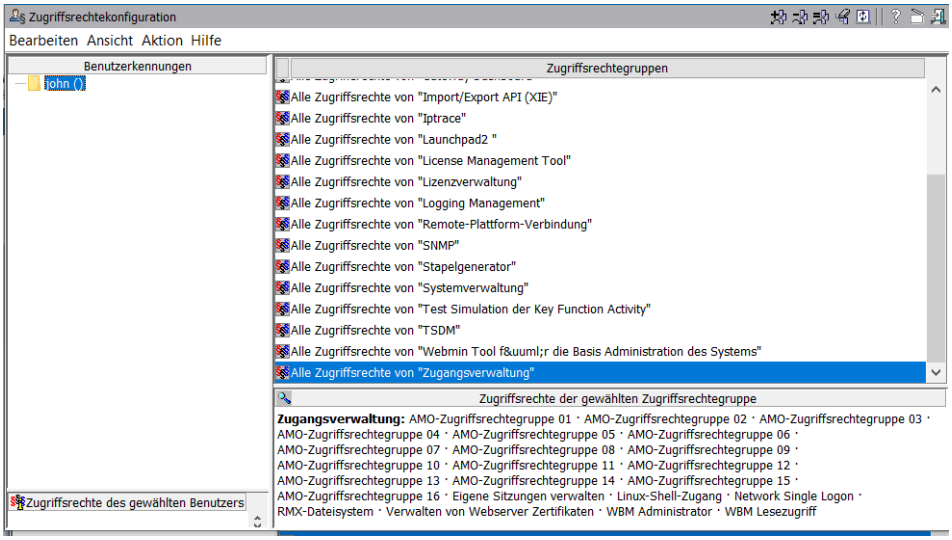
Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

2.10.6.2 Mehrere Vorschaufenster gleichzeitig anzeigen

Das Symbol in der Titelleiste der Vorschaufenster verändert sein Aussehen und wird als Lupe angezeigt, wenn Sie die Maus darüber bewegen. Die Höhe der Vorschaufenster ist veränderbar.



So öffnen Sie ein zusätzliches Vorschaufenster

- Bewegen Sie die Maus auf das Symbol in der Titelleiste eines Vorschaufensters. Das Symbol verändert sein Aussehen und wird jetzt als Lupe angezeigt.
- Klicken Sie auf das Lupensymbol. Ein zusätzliches Vorschaufenster wird eingeblendet. Es enthält denselben Text, der auch im entsprechenden ursprünglichen Vorschaufenster angezeigt wird, d.h. eine Kurzbeschreibung

des markierten Zugriffsrechts oder aller Zugriffsrechte des markierten Benutzers (linkes Fenster) bzw. der markierten Zugriffsrechtegruppe (rechtes Fenster).

- Alternative: Sie können das Textfenster auch mit einem Doppelklick auf das markierte Objekt (Benutzerkennung, Zugriffsrechte oder Zugriffsrechtegruppe) öffnen.
- Sie können nacheinander mehrere Textfenster öffnen und gleichzeitig am Bildschirm anzeigen.
- Um ein oder mehrere Textfenster wieder zu schließen, klicken Sie entweder auf die Schaltfläche **Schließen** im jeweiligen Textfenster, oder wählen Sie im Menü **Ansicht** oder im **Kontextmenü** die Option **Alle Vorschaufenster schließen**, um alle geöffneten Textfenster, die Vorschautexte enthalten, auf einmal zu schließen.

Es ist möglich, mehrere Textfenster gleichzeitig anzeigen.

Über das Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration" können Sie

- die Vorschaufenster ein- und ausblenden,
- alle zusätzlich geöffneten Vorschautextfenster schließen,
- zur Startseite von **OpenScape 4000 Assistant/Manager** zurückkehren.

Weitere Informationen finden Sie in Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Verwandte Themen

Kontextmenü

Vorschaufenster einblenden/ausblenden

Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

2.10.6.3 Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration"

Das Vorschaufenster unterhalb des linken Bereichs im Fenster **Zugriffsrechtekonfiguration** kann zwei unterschiedliche Titel haben, und zwar:

Zugriffsrechte des gewählten Benutzers

Dieser Titel wird im linken Vorschaufenster angezeigt, wenn Sie im linken Bereich einen **Benutzer** markiert haben.

Zugriffsrechte der gewählten Zugriffsrechtegruppe

Dieser Titel wird im linken Vorschaufenster angezeigt, wenn Sie im linken Bereich eine **Zugriffsrechtegruppe** markiert haben.

Vorschaufenster einblenden/ausblenden

Die **Vorschaufenster** können Sie nach Bedarf einblenden oder ausblenden. Die Höhe der Vorschaufenster ist veränderbar.

Weitere Informationen finden Sie in Vorschaufenster einblenden/ausblenden.

Mehrere Vorschaufenster gleichzeitig anzeigen

Sie können mehrere Vorschaufenster gleichzeitig öffnen und am Bildschirm anzeigen lassen.

Weitere Informationen finden Sie in Mehrere Vorschaufenster gleichzeitig anzeigen.

Verwandte Themen

Kontextmenü

Vorschaufenster einblenden/ausblenden

Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

2.10.6.4 Vorschaufenster, rechter Bereich, Dialogfeld "Zugriffsrechtekonfiguration"

Das Vorschaufenster **Zugriffsrechte der gewählten Zugriffsrechtegruppe** befindet sich unterhalb des rechten Bereichs im Fenster **Zugriffsrechtekonfiguration**. In diesem Fenster wird die Liste der zu einer Zugriffsrechtegruppe gehörenden Zugriffsrechte angezeigt.

Vorschaufenster einblenden/ausblenden

Die **Vorschaufenster** können Sie nach Bedarf einblenden oder ausblenden - siehe Beschreibung im Abschnitt Vorschaufenster einblenden/ausblenden. Die Höhe der Vorschaufenster ist veränderbar.

Mehrere Vorschaufenster gleichzeitig anzeigen

Sie können mehrere Vorschaufenster gleichzeitig öffnen und am Bildschirm anzeigen lassen.

Weitere Informationen finden Sie in Mehrere Vorschaufenster gleichzeitig anzeigen.

Verwandte Themen

Kontextmenü

Vorschaufenster einblenden/ausblenden

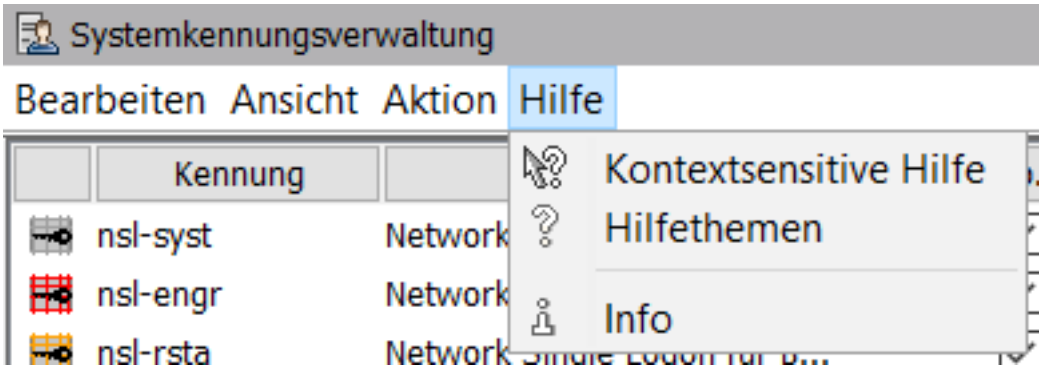
Vorschaufenster, linker Bereich, Dialogfeld "Zugriffsrechtekonfiguration",

Bereiche im Dialogfeld "Zugriffsrechtekonfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

2.10.7 Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtekonfiguration"

Das Menü **Hilfe** wird bei allen Komponenten der Komponente **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**. Das Menü **Hilfe** enthält bei allen Komponenten dieselben Optionen, und zwar:



Kontextsensitive Hilfe	Wenn Sie auf **Kontextsensitive Hilfe** klicken, wird die kontextbezogene Online-Hilfe zu der per Mausklick markierten Position aufgerufen. Die Kontextsensitive Hilfe können Sie auch aufrufen, indem Sie mit der Maus auf eine bestimmte Position der Bedienoberfläche klicken und die Tastenkombination **STRG+F1** betätigen.
Hilfe-Themen	Wenn Sie auf die **Hilfethemen** klicken, wird das Inhaltsverzeichnis der Online-Hilfe geöffnet. Die Online-Hilfe kann auch über die Taste **F1** aufgerufen werden.
Info	Im Dialogfenster **Info** werden die Informationen über die Programmversion der Software, das Erscheinungsjahr und die urheberrechtlichen Bestimmungen angezeigt.

Verwandte Themen

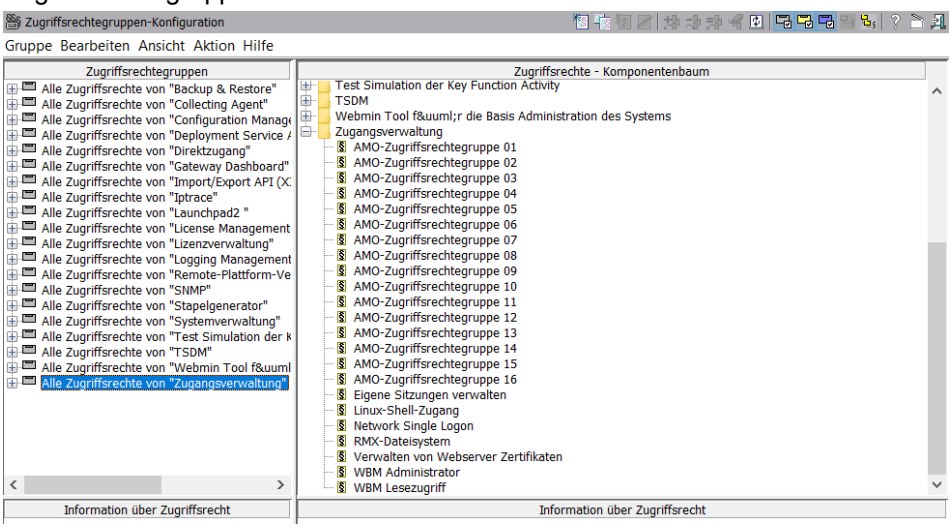
Menüleiste

Symbolleiste

Benutzeroberfläche der Zugangsverwaltung

2.11 Zugriffsrechtegruppen-Konfiguration

Über das Dialogfeld **Zugriffsrechtegruppen-Konfiguration** können Sie Zugriffsrechtegruppen einrichten und ändern.



Mit Hilfe von Zugriffsrechtegruppen können die Benutzerrechte für die Ausführung und Nutzung der verfügbaren Anwendungen verwaltet werden.

Vereinfacht wird der Prozess für die selektive Zuweisung von Zugriffsrechten dadurch, dass man "vordefinierte Zugriffsrechtegruppen" festlegen kann. Siehe Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Nach der Installation stehen vordefinierte Zugriffsrechtegruppen zur Verfügung. Im Dialogfeld **Zugriffsrechtegruppen-Konfiguration** können zusätzliche Zugriffsrechtegruppen erzeugt und modifiziert werden. Änderungen, die in einer Zugriffsrechtegruppe vorgenommen werden, gelten automatisch für alle Benutzer, denen diese Gruppe zugewiesen ist.

Das Zuweisen der Zugriffsrechtegruppen zu individuellen Benutzern erfolgt im Dialogfeld Zugriffsrechtekonfiguration.

Komponenten der Benutzeroberfläche

Das Dialogfeld **Zugriffsrechtegruppen-Konfiguration** ist vertikal in zwei Bereiche unterteilt, in denen Zugriffsrechte und Zugriffsrechtegruppen in mehrstufigen Baumstrukturen angezeigt werden, und enthält folgende Elemente:

- Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"
  - "Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

    Drei Kategorien von Zugriffsrechtegruppen können angezeigt werden: **Vordefinierte Zugriffsrechtegruppen**, **Selbst erstellte Zugriffsrechtegruppen** und **Zugriffsrechtegruppen für dynamische Applikationen**. Das Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" und das Kontextmenü bieten Ihnen die Möglichkeit, diese verschiedenen Kategorien von Zugriffsrechtegruppen ein- oder auszublenden.
  - "Zugriffsrechte - Komponentenbaum/Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"
- Vorschaufenster, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

  Die Vorschaufenster, Dialogfeld "Zugriffsrechtegruppen-Konfiguration" am unteren Rand der beiden Fensterbereiche zeigen unter dem Titel Information über Zugriffsrecht eine Kurzbeschreibung des gerade gewählten Zugriffsrechts an. Durch Aktivieren/Deaktivieren der Menüoption **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" oder im Kontextmenü können Sie die **Vorschaufenster** ein- und ausblenden. Die Höhe der Vorschaufenster ist veränderbar.
- Symbolleiste

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine Beschreibung aller Symbolschaltflächen finden Sie unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration".
- Menüleiste
- Kontextmenü
- Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"
- Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"
- Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

- Menü "Aktion", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"
- Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Verwandte Themen

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.1 Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Das Dialogfeld **Zugriffsrechtegruppen-Konfiguration** ist vertikal in zwei Bereiche unterteilt und wie folgt gegliedert:

- "Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

  Drei Kategorien von Zugriffsrechtegruppen können angezeigt werden: **Vordefinierte Zugriffsrechtegruppen**, **Selbst erstellte Zugriffsrechtegruppen** und **Zugriffsrechtegruppen für dynamische Applikationen**. Das Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" und das Kontextmenü bieten Ihnen die Möglichkeit, diese verschiedenen Kategorien von Zugriffsrechtegruppen ein- oder auszublenden.
- "Zugriffsrechte - Komponentenbaum/Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"
- Vorschaufenster, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

  Die Vorschaufenster, Dialogfeld "Zugriffsrechtegruppen-Konfiguration" am unteren Rand der beiden Fensterbereiche zeigen unter dem Titel Information über Zugriffsrecht eine Kurzbeschreibung des gerade gewählten Zugriffsrechts an. Durch Aktivieren/Deaktivieren der Menüoption **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" oder in der Symbolleiste können Sie die **Vorschaufenster** ein- und ausblenden. Die Höhe der Vorschaufenster ist veränderbar.

  – Vorschaufenster "Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"
  – Vorschaufenster "Zugriffsrechte - Komponentenbaum/Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

  Weitere Informationen finden Sie in Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".
- Symbolleiste

  Die **Symbolschaltflächen** in der Symbolleiste haben die gleichen Funktionen wie die Einträge in den Hauptmenüs. Eine Beschreibung aller Symbolschaltflächen finden Sie unter Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

- Menüleiste

Verwandte Themen

Kontextmenü

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.1.1 "Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Das Dialogfeld **Zugriffsrechtegruppen-Konfiguration** besteht aus einem vertikal in zwei Bereiche unterteilten Fenster. Darin werden die Zugriffsrechtegruppe und Zugriffsrechte in einer mehrstufige Baumstruktur mit folgender Gliederung angezeigt:

Linker Bereich: Zugriffsrechtegruppen

- Obere Ebene: Alle verfügbaren Zugriffsrechtegruppen (Access Right Groups = ARGs).

  Enthält die Ordner aller verfügbaren Zugriffsrechtegruppen, nach Registrierungseinheiten (registration units) geordnet.

  Eine Zugriffsrechtegruppe kann mehrere Komponenten enthalten.

  Drei Kategorien von Zugriffsrechtegruppen können angezeigt werden: **Vordefinierte Zugriffsrechtegruppen**, **Selbst erstellte Zugriffsrechtegruppen** und **Zugriffsrechtegruppen für dynamische Applikationen**. Das Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" und das Kontextmenü bieten Ihnen die Möglichkeit, diese verschiedenen Kategorien von Zugriffsrechtegruppen ein- oder auszublenden. Mehr Informationen finden Sie im Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".
- Zweite Ebene: Ordner zweiten Grades. Jeder Ordner entspricht in der Regel einer Komponente und enthält alle dem Benutzer innerhalb dieser Komponente zugewiesenen Zugriffsrechte.
- Dritte Ebene: Alle Zugriffsrechte, die dem Benutzer innerhalb einer Zugriffsrechtegruppe zugewiesen wurden.

Siehe auch Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

2.11.1.2 "Zugriffsrechte - Komponentenbaum/Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Das Dialogfeld **Zugriffsrechtegruppen-Konfiguration** besteht aus einem vertikal in zwei Bereiche unterteilten Fenster. Darin werden die Zugriffsrechtegruppen und Zugriffsrechte in einer mehrstufige Baumstruktur mit folgender Gliederung angezeigt:

Rechter Bereich: Zugriffsrechte - Komponenten-Applikationsbaum

In diesem Bereich haben Sie die Wahl zwischen den Ansichten **Komponentenbaum** und **Applikationsbaum**. Um die Ansicht zu wechseln, wählen Sie im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration", im Kontextmenü oder in der Symbolleiste die Option **Zugriffsrechte - Komponentenbaum anzeigen** bzw. die Option **Zugriffsrechte - Applikationsbaum anzeigen**. Im **Kontextmenü** werden diese Optionen nur im rechten Fensterbereich angezeigt.

- **Ansicht Komponentenbaum**
  - Obere Ebene: Jeder Ordner stellt eine Komponente dar. Die Applikationen innerhalb der Komponenten sind bei dieser Ansicht ausgeblendet. Innerhalb jeder Komponente werden direkt die zuweisbaren Zugriffsrechte als auswählbare Elemente angezeigt.
  - Zweite Ebene: Die zuweisbaren Zugriffsrechte werden direkt als auswählbare Elemente innerhalb der einzelnen Komponenten angezeigt.

  Sie können Drag&Drop verwenden, um Zugriffsrechte (aus dem rechten Bereich) bestimmten Zugriffsrechtegruppen (im linken Bereich) zuzuweisen- siehe Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".
- **Ansicht Applikationsbaum**
  - Obere Ebene: Jeder Ordner ersten Grades stellt eine Komponente dar. Applikationen werden als Ordner zweiten Grades innerhalb der Komponenten angezeigt. Jede Komponente kann eine oder mehrere Applikationen enthalten.
  - Zweite Ebene: Diese Ebene wird nur in der Ansicht **Applikationsbaum** angezeigt. Applikationen werden als Ordner zweiten Grades innerhalb der Komponenten angezeigt. Jede Komponente kann eine oder mehrere Applikationen enthalten. Innerhalb jeder Applikation werden die zuweisbaren Zugriffsrechte als auswählbare Elemente angezeigt.
  - Dritte Ebene: Die zuweisbaren Zugriffsrechte werden als auswählbare Elemente innerhalb jeder Applikation angezeigt. (Verfügbare Komponenten können aus mehr als einer Applikation bestehen, die auf der Startseite angezeigt werden.)

  Sie können Drag&Drop verwenden, um Zugriffsrechte (aus dem rechten Bereich) bestimmten Zugriffsrechtegruppen (im linken Bereich) zuzuweisen- siehe Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

  NOTICE: Das Zuweisen von mindestens einem Zugriffsrecht aus einer Applikation an eine Zugriffsrechtegruppe bewirkt, dass die entsprechende Applikation auf der Startseite für alle Benutzer angezeigt wird, die die entsprechenden Zugriffsrechte für diese Applikation besitzen.

  Siehe hierzu auch Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration", Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration" und Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.2 Vorschaufenster, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Die **Vorschaufenster** am unteren Rand der beiden Fensterbereiche zeigen unter dem Titel **Information über Zugriffsrecht** eine Kurzbeschreibung des gerade gewählten Zugriffsrechts an.

Durch Aktivieren/Deaktivieren der Menüoption **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" können Sie die **Vorschaufenster** ein- und ausblenden. Die Höhe der Vorschaufenster ist veränderbar.

Weitere Informationen hierzu finden Sie unter

"Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration" und

"Zugriffsrechte - Komponentenbaum/Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Verwandte Themen

Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.2.1 Vorschaufenster "Zugriffsrechtegruppen" (linker Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Am unteren Rand beider Bereiche des Dialogfelds **Zugriffsrechtegruppen-Konfiguration** befindet sich je ein **Vorschaufenster**. Die Vorschaufenster können durch Aktivieren bzw. Deaktivieren der Option **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" eingeblendet bzw. ausgeblendet werden.Die Höhe der Vorschaufenster ist veränderbar.

In den **Vorschaufenstern** werden kurze Beschreibungen der ausgewählten Zugriffsrechte angezeigt.

Verwandte Themen

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.2.2 Vorschaufenster "Zugriffsrechte - Komponentenbaum/ Applikationsbaum" (rechter Bereich), Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Am unteren Rand beider Bereiche des Dialogfelds **Zugriffsrechtegruppen-Konfiguration** befindet sich je ein **Vorschaufenster**. Die Vorschaufenster können durch Aktivieren bzw. Deaktivieren der Option **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" eingeblendet bzw. ausgeblendet werden.Die Höhe der Vorschaufenster ist veränderbar.

In den **Vorschaufenstern** werden kurze Beschreibungen der ausgewählten Zugriffsrechte angezeigt.

Verwandte Themen

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.3 Zugriffsrechte zuweisen/entziehen, Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Beachten Sie, dass die im folgenden beschriebenen Operationen bei **vordefinierten** Zugriffsrechtegruppen **nicht möglich** sind.

Zuweisen von Zugriffsrechten an Zugriffsrechtegruppen

1) Wählen Sie im rechten Fenster ein Zugriffsrecht oder mehrere Zugriffsrechte.

   Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

   Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.
2) Ziehen Sie das gewählte Zugriffsrecht bzw. die gewählten Zugriffsrechte mit der Maus in die linke Fensterhälfte auf die Zugriffsrechtegruppe, der dieses Zugriffsrecht zugewiesen werden soll.

   Haben Sie mehrere **nicht aufeinander folgende** Elemente markiert, müssen Sie die Drag&Drop-Operation bei gedrückter Taste **Strg** ausführen, damit die Markierung der Elemente nicht rückgängig gemacht wird.

oder

1) Wählen Sie im rechten Fenster ein oder mehrere Zugriffsrecht(e).
2) Wählen Sie in der linken Fensterhälfte alle Zugriffsrechtegruppen, denen diese Zugriffsrechte zugewiesen werden sollen. Es können nur Zugriffsrechtegruppen aus dieser Liste gewählt werden.
3) Wählen Sie in der Menüleiste **Bearbeiten** -> **Zuweisen** oder Klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste. oder Klicken Sie auf die entsprechende Schaltfläche im Kontextmenü.

   Mit dieser Funktion können die verfügbaren Zugriffsrechte in einem Arbeitsschritt mehreren Zugriffsrechtegruppen zugewiesen werden.

Entziehen der Zugriffsrechte für Zugriffsrechtegruppen

1) Wählen Sie in der linken Fensterhälfte alle Zugriffsrechte, die einer Zugriffsrechtegruppe entzogen werden sollen.
2) Wählen Sie in der Menüleiste **Bearbeiten -> Entziehen**

   oder

   Klicken Sie auf die entsprechende Schaltfläche in der Symbolleiste.

   oder

   Klicken Sie auf die entsprechende Schaltfläche im Kontextmenü.

   Sämtliche Änderungen werden umgehend an den Server übermittelt und gelten folglich für alle neuen Anmeldungen betroffener Benutzer.

Die Änderungen können sich auch auf laufende Sitzungen auswirken, da die Server-Komponente der Zugangsverwaltung regelmäßig eine Benachrichtigung an andere Applikationen ausgibt.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

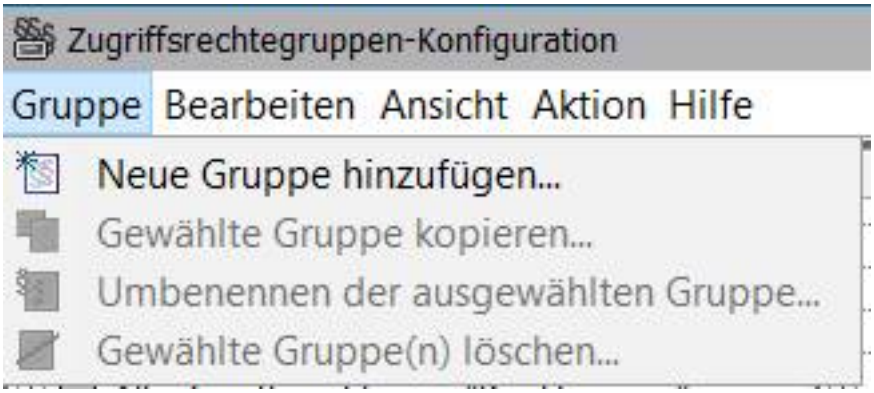
Bereiche im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

2.11.4 Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Das Menü **Gruppe** erscheint nur im Dialogfeld Zugriffsrechtegruppen-Konfiguration. In diesem Menü können Sie Zugriffsrechtegruppen hinzufügen, kopieren, umbenennen und löschen. Sie finden hier folgende Einträge:



Menüoptionen

Neuen Gruppe hinzufügen	Öffnet das Dialogfeld **Neue Zugriffsrechtegruppe hinzufügen**.
Gewählte Gruppe kopieren	Öffnet das Dialogfeld **Kopieren der ausgewählten Gruppenzugriffsrechte**.
Umbenennen der ausgewählten Gruppe	Öffnet das Dialogfeld **Umbenennen der ausgewählten Gruppenzugriffsrechte**.
Gewählte Gruppe(n) löschen	Öffnet das Dialogfeld Gruppen löschen und löscht die gewählte(n) Zugriffsrechtegruppe(n) nach Bestätigung mit **OK**.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

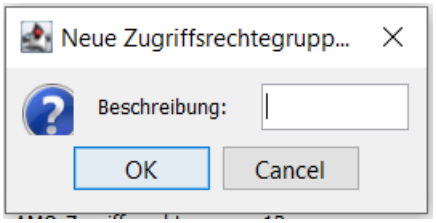
Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.5 Neue Zugriffsrechtegruppe hinzufügen

Das Dialogfeld **Neue Zugriffsrechtegruppe hinzufügen** wird angezeigt, wenn Sie auf **Neue Gruppe hinzufügen** im Menü **Gruppe** bzw. auf das entsprechende Symbol in der Symbolleiste klicken.



Bedienoberfläche

Beschreibung	Eingabefeld für die Kennung einer Zugriffsrechtegruppe. Die Funktion des Felds **Beschreibung** ist bei folgenden Aktionen im Menü **Gruppe** identisch: **Neue Gruppe hinzufügen**, **Gewählte Gruppe kopieren**, **Gewählte Gruppe umbenennen**.
OK	Aktion bestätigen und ausführen.
Abbrechen	Aktion abbrechen.

Verwandte Themen

Symbolleiste

Kontextmenü

Menüleiste

Menü Benutzer

Benutzerkennungen löschen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

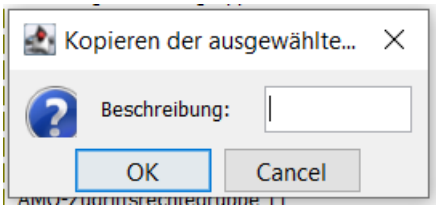
Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.6 Gewählte Zugriffsrechtegruppe kopieren

Das Dialogfeld **Kopieren der ausgewählten Gruppenzugriffsrechte** wird angezeigt, wenn Sie auf **Gewählte Gruppe kopieren** im Menü **Gruppe** bzw. auf das entsprechende Symbol in der Symbolleiste oder im Kontextmenü klicken.



Bedienoberfläche

Beschreibung	Eingabefeld für die Kennung einer Zugriffsrechtegruppe. Die Funktion des Felds **Beschreibung** ist bei folgenden Aktionen im Menü **Gruppe** identisch: **Neue Gruppe hinzufügen**, **Gewählte Gruppe kopieren**, **Gewählte Gruppe umbenennen**.
OK	Aktion bestätigen und ausführen.
Abbrechen	Aktion abbrechen.

Verwandte Themen

Symbolleiste

Kontextmenü

Menüleiste

Menü Benutzer

Benutzerkennungen löschen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.7 Umbenennen der ausgewählten Zugriffsrechtegruppe

Das Dialogfeld **Umbenennen der ausgewählten Zugriffsrechtegruppe** wird angezeigt, wenn Sie auf **Gewählte Gruppe umbenennen** im Menü **Gruppe** bzw. auf das entsprechende Symbol in der Symbolleiste klicken.

Bedienoberfläche

Beschreibung	Eingabefeld für die Kennung einer Zugriffsrechtegruppe. Die Funktion des Felds **Beschreibung** ist bei folgenden Aktionen im Menü **Gruppe** identisch: **Neue Gruppe hinzufügen**, **Gewählte Gruppe kopieren**, **Gewählte Gruppe umbenennen**.
OK	Aktion bestätigen und ausführen.
Abbrechen	Aktion abbrechen.

Verwandte Themen

Symbolleiste

Kontextmenü

Menüleiste

Menü Benutzer

Benutzerkennungen löschen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.8 Gruppen löschen

Das Dialogfeld **Gruppen löschen** wird angezeigt, wenn Sie im Menü **Gruppe** auf **Gewählte Gruppe(n)** löschen bzw. auf das entsprechende Symbol in der Symbolleiste klicken.

Um Zugriffsrechtegruppen zu löschen, markieren Sie die gewünschte(n) Gruppe(n), wählen dann die Menüoption **Gewählte Gruppe(n) löschen** bzw. das entsprechende Symbol in der Symbolleiste und bestätigen den Löschvorgang mit **OK**.

NOTICE: Das Zuweisen von mindestens einem Zugriffsrecht aus einer Applikation an eine Zugriffsrechtegruppe bewirkt, dass die entsprechende Applikation auf der Startseite für alle Benutzer angezeigt wird, die die entsprechenden Zugriffsrechte für diese Applikation besitzen.

Bedienoberfläche

OK	Aktion bestätigen und ausführen.
Abbrechen	Aktion abbrechen.

Verwandte Themen

Symbolleiste

Kontextmenü

Menüleiste

Menü Benutzer

Benutzerkennungen löschen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

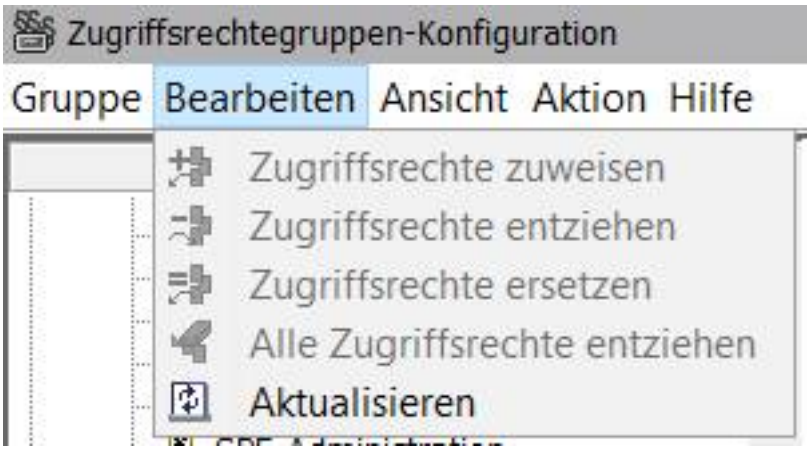
Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.9 Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Das Menü **Bearbeiten** wird in allen Dialogfeldern des Bereichs **Kennungsverwaltung** angezeigt. Im Dialogfeld **Zugriffsrechtegruppen-Konfiguration** enthält dieses Menü folgende Einträge:



Menüoptionen

Zugriffsrechte zuweisen	Wenn Sie im Menü **Bearbeiten** auf **Zugriffsrechte zuweisen** klicken, werden die im rechten Bereich gewählten Zugriffsrechte allen im linken Bereich gewählten Zugriffsrechtegruppen zugewiesen. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

Zugriffsrechte entziehen	• Wenn Sie im Menü **Bearbeiten** auf **Zugriffsrechte entziehen** klicken, werden alle im linken Bereich gewählten Zugriffsrechte den zugehörigen Zugriffsrechtegruppen entzogen. • Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen. • **Hinweis:** Der Befehl **Zugriffsrechte entziehen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Zugriffsrechte ersetzen	• Wählen Sie im linken Bereich die Menge der manuell erstellten Zugriffsrechtegruppen (funktioniert nur für MANUELL ERSTELLTE Zugriffsrechtegruppen) und im rechten Bereich die Menge der einzelnen Zugriffsrechte oder übergeordnete Ordner. Wenn Sie im Menü **Bearbeiten** auf **Zugriffsrechte ersetzen** klicken, werden die zuvor zugewiesenen Zugriffsrechte durch die aktuell markierten Zugriffsrechte ersetzt. Die vorher zugewiesenen Zuordnungen werden überschrieben. Unterschied zu **Zuweisen**: Bei **Zuweisen** werden die neuen Zugriffsrechte zu den bereits zugewiesenen Zugriffsrechten hinzugefügt, und diese werden nicht überschrieben. Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen: Über das Kontextmenü oder über die Symbolleiste. • **Hinweis:** Der Befehl **Zugriffsrechte ersetzen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Alle Zugriffsrechte entziehen	• Markieren Sie im linken Bereich die Menge der manuell erstellten Zugriffsrechtegruppen (funktioniert nur für MANUELL ERSTELLTE Zugriffsrechtegruppen). Sie haben auch die Möglichkeit, die übrigen Zugriffsrechtegruppen auszublenden, um nur die manuell erstellten Zugriffsrechtegruppen anzuzeigen. Wenn Sie im Menü **Bearbeiten** auf **Alle Zugriffsrechte entziehen** klicken, werden den markierten Zugriffsrechtegruppen alle zugewiesenen Rechte entzogen. Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen: Über das Kontextmenü oder über die Symbolleiste. **Hinweis:** Der Befehl **Alle Zugriffsrechte entziehen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.
Reload	Wenn Sie im Menü **Bearbeiten** auf **Aktualisieren** klicken, wird der Inhalt des Dialogfelds **Zugriffsrechtegruppen-Konfiguration** aktualisiert. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Dieser Befehl hat die gleiche Funktion wie die Symbolschaltfläche **Daten vom Server aktualisieren** in der Symbolleiste.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Symbolleiste

Kontextmenü

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

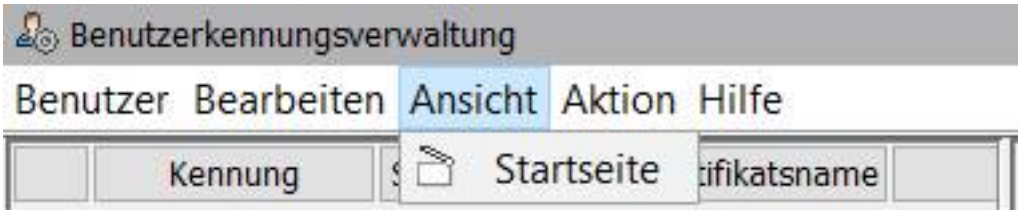
Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.10 Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Das Menü **Ansicht** im Dialogfeld Zugriffsrechtegruppen-Konfiguration enthält folgende Einträge:



Menüoptionen

Vordefinierte Zugriffsrechtegruppen	Einblenden/Ausblenden der vordefinierten Zugriffsrechtegruppen.
Selbst erstellte Zugriffsrechtegruppen	Einblenden/Ausblenden der selbst erstellten Zugriffsrechtegruppen.
Zugriffsrechtegruppen für dynamische Applikationen	Einblenden/Ausblenden der Zugriffsrechtegruppen für dynamische Applikationen.

Zugriffsrechte - Komponentenbaum anzeigen	Jeder Ordner stellt eine Komponente dar. Die Applikationen innerhalb der Komponenten sind bei dieser Ansicht ausgeblendet. Innerhalb jeder Komponente werden direkt die zuweisbaren Zugriffsrechte als auswählbare Elemente angezeigt.
Zugriffsrechte - Applikationsbaum anzeigen	Jeder Ordner ersten Grades stellt eine Komponente dar. Applikationen werden als Ordner zweiten Grades innerhalb der Komponenten angezeigt. Die Applikationen sind bei dieser Ansicht als Ordner zweiten Grades eingeblendet. Jede Komponente kann eine oder mehrere Applikationen enthalten. Innerhalb jeder Applikation werden die zuweisbaren Zugriffsrechte als auswählbare Elemente angezeigt. (Verfügbare Komponenten können aus mehr als einer Applikation bestehen, die auf der Startseite angezeigt werden.)
Information über Zugriffsrecht	Einblenden/Ausblenden der Vorschaufenster durch Aktivieren/Deaktivieren dieser Menüoption. In den Vorschaufenstern wird eine Kurzbeschreibung des gerade gewählten Zugriffsrechts angezeigt.
Start	Gleiche Funktion wie Symbol **Startseite anzeigen** in der Symbolleiste. Öffnet ein neues Browser-Fenster, in dem die **Startseite von OpenScape 4000 Assistant/ Manager** angezeigt wird.

Alternative Möglichkeiten, Anzeige- und Bearbeitungsfunktionen auszuführen

über das Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

oder

über die Kontextmenü

oder

über die Symbolleiste

Markieren von Elementen

Um mehrere aufeinander folgende Elemente (Zugriffsrechte bzw. Zugriffsrechtegruppen) zu markieren, drücken Sie die **Umschalttaste** und markieren Sie bei gedrückter Umschalttaste die Elemente mit der linken Maustaste.

Um mehrere **nicht aufeinander folgende** Elemente zu markieren oder die Markierung einzelner Elemente wieder aufzuheben, drücken Sie die Taste **Strg** und markieren Sie bei gedrückter Taste Strg die Elemente mit der linken Maustaste.

Verwandte Themen

Kontextmenü

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

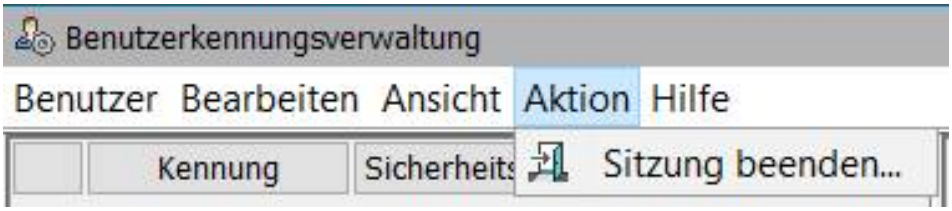
Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration".

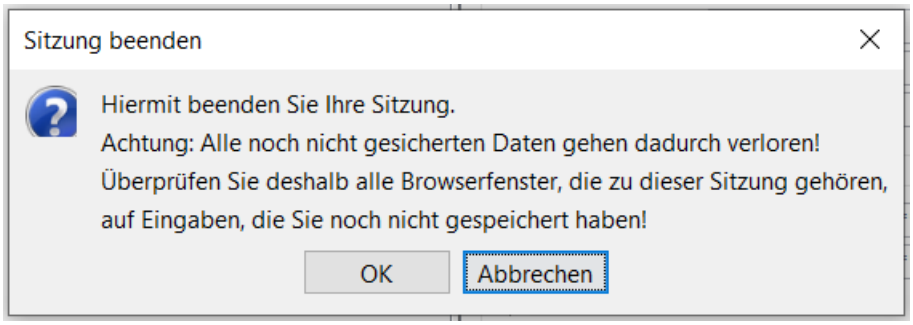
Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

2.11.11 Menü "Aktion", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Das Menü **Aktion** enthält die Option **Sitzung beenden**. Diese hat die gleiche Funktion wie die Symbolschaltfläche **Sitzung beenden** in der Symbolleiste, Mehr Informationen finden Sie im Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration".



Sobald Sie auf **Sitzung beenden** klicken, erscheint eine Warnmeldung, die darauf hinweist, dass sämtliche nicht gespeicherten Sitzungsdaten verloren gehen. Sie werden aufgefordert, alle Sitzungsdaten zu speichern und das Verlassen der Sitzung zu bestätigen.



Verwandte Themen

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

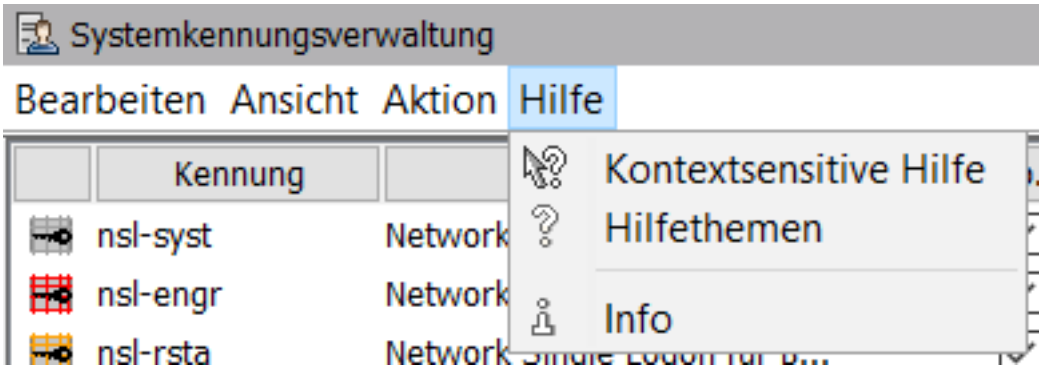
Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

2.11.12 Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Das Menü **Hilfe** wird bei allen Komponenten der Komponente **Kennungsverwaltung** angezeigt, außer bei **Export von Benutzerdaten**. Das Menü **Hilfe** enthält bei allen Komponenten dieselben Optionen, und zwar:



Kontextsensitive Hilfe	Wenn Sie auf **Kontextsensitive Hilfe** klicken, wird die kontextbezogene Online-Hilfe zu der per Mausklick markierten Position aufgerufen. Die Kontextsensitive Hilfe können Sie auch aufrufen, indem Sie mit der Maus auf eine bestimmte Position der Bedienoberfläche klicken und die Tastenkombination **STRG+F1** betätigen.
Hilfe-Themen	Wenn Sie auf die **Hilfethemen** klicken, wird das Inhaltsverzeichnis der Online-Hilfe geöffnet. Die Online-Hilfe kann auch über die Taste **F1** aufgerufen werden.
Info	Im Dialogfenster **Info** werden die Informationen über die Programmversion der Software, das Erscheinungsjahr und die urheberrechtlichen Bestimmungen angezeigt.

Verwandte Themen

Menüleiste

Menü Benutzer

Menü "Gruppe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

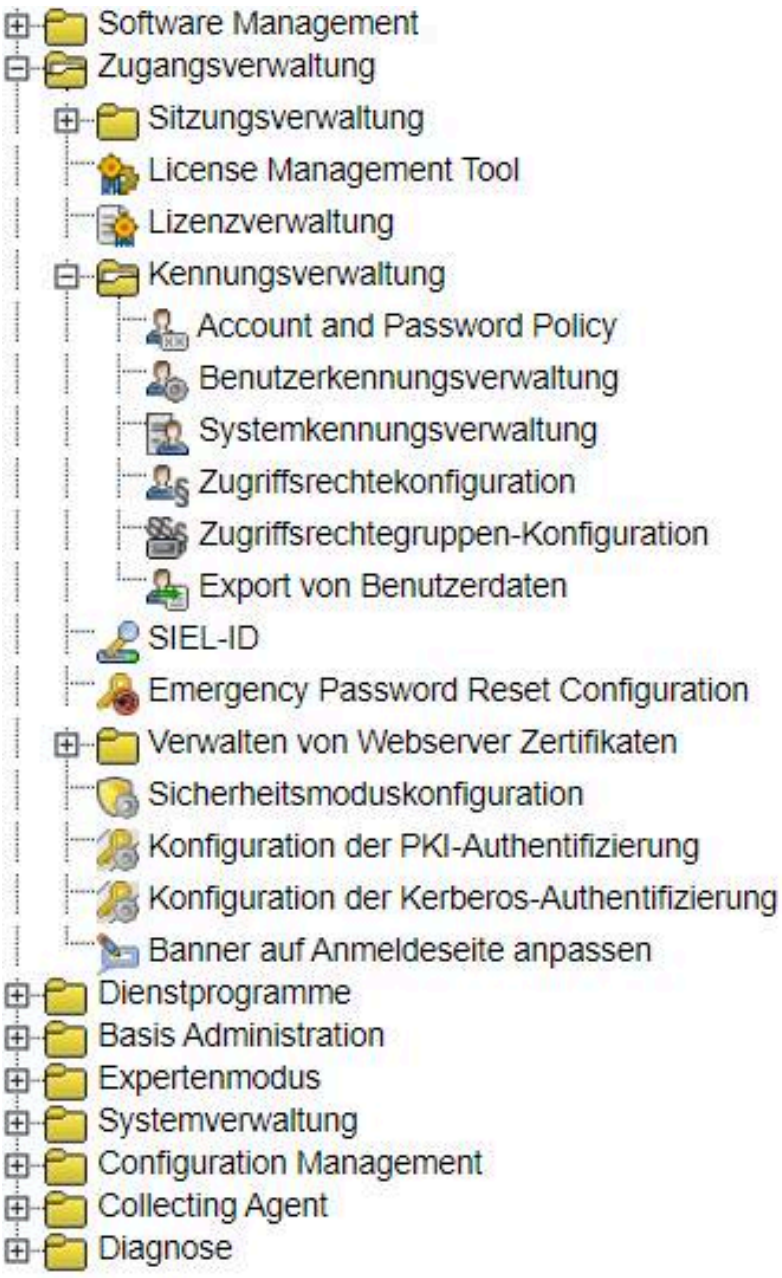
Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

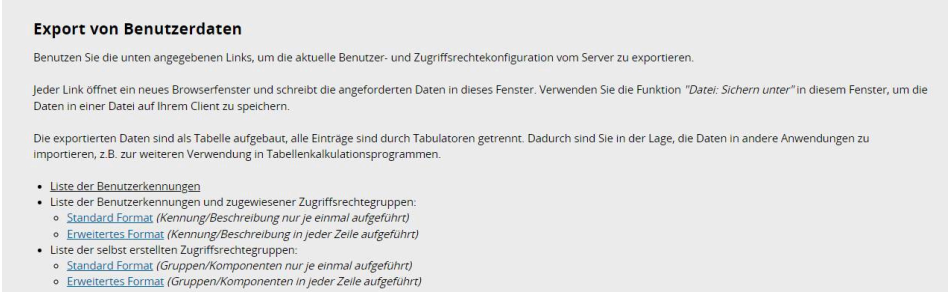
2.12 Export von Benutzerdaten

Der Link **Export von Benutzerdaten** auf der **Startseite** der **Zugangsverwaltung** im Ordner **Kennungsverwaltung** öffnet das Fenster **Export von Benutzerdaten**.



Für das Exportieren der Benutzer- und Zugriffsrechtekonfigurationsdaten vom Server einer Anlage stehen Ihnen die Links im Fenster **Export von Benutzerdaten** zur Verfügung.

Export von Benutzerdaten ermöglicht das Anzeigen und Exportieren folgender Benutzerdaten:



Export von Benutzerdaten

Benutzen Sie die unten angegebenen Links, um die aktuelle Benutzer- und Zugriffsrechtekonfiguration vom Server zu exportieren.

Jeder Link öffnet ein neues Browserfenster und schreibt die angeforderten Daten in dieses Fenster. Verwenden Sie die Funktion *"Datei: Sichern unter"* in diesem Fenster, um die Daten in einer Datei auf Ihrem Client zu speichern.

Die exportierten Daten sind als Tabelle aufgebaut, alle Einträge sind durch Tabulatoren getrennt. Dadurch sind Sie in der Lage, die Daten in andere Anwendungen zu importieren, z.B. zur weiteren Verwendung in Tabellenkalkulationsprogrammen.

- Liste der Benutzerkennungen
- Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen:
  - Standard Format *(Kennung/Beschreibung nur je einmal aufgeführt)*
  - Erweitertes Format *(Kennung/Beschreibung in jeder Zeile aufgeführt)*
- Liste der selbst erstellten Zugriffsrechtegruppen:
  - Standard Format *(Gruppen/Komponenten nur je einmal aufgeführt)*
  - Erweitertes Format *(Gruppen/Komponenten in jeder Zeile aufgeführt)*

2.12.1 "Liste der Benutzerkennungen", Fenster "Export von Benutzerdaten"

Klicken Sie auf den Link **Liste der Benutzerkennungen**, um die Liste aller eingerichteten Benutzerkennungen und deren Passwort-Attribute für eine Anlage anzeigen zu lassen. Beim Klicken auf den Link werden die angeforderten Daten in einem neu geöffneten Browser-Fenster angezeigt.

Um die Daten in einer Datei auf Ihrem System zu speichern, wählen Sie im neu geöffneten Browser-Fenster die Funktion **Datei** -> **Speichern unter** und speichern Sie die Datei als **Textdatei** (***.txt**).

Wenn Sie die Daten direkt in eine Textdatei exportieren möchten, ohne sie vorher anzuzeigen, klicken Sie mit der rechten Maustaste auf den Link **Liste der Benutzerkennungen**, wählen Sie im Kontextmenü die Option **Ziel speichern unter**, und speichern Sie die Datei als **Textdatei** (***.txt**).

Die Daten der Textdatei können Sie in ein Tabellenkalkulationsprogramm importieren, um sie zu formatieren oder auszuwerten, z. B. in MS Excel mit **Daten** -> **Externe Daten** -> **Textdatei importieren**.

	A	B	C	D	E
1	**# eur.cgi v1.0**				
2	**Export von Benutzerdaten: Liste der Benutzerkennungen**	**24.06.2010 14:33**	**Manager**	**0.520**	
3	**Kennung**	**Beschreibung**	**Gesperrt**	**Max. Passwort-Gültigkeit**	**Passwort-Änderung erlaubt**
4	stevie	stevieb@mycomp.com, x12345	Nein	40	Nein
5	gert	gertf@mycomp.com, x98765	Nein	80	Ja
6	peter	peters@mycomp.com, x24680	Nein	40	Ja
7	mark	markw@mycomp.com, x86420	Nein	40	Ja
8	chris	chriss@mycomp.com, x13579	Nein	-1	Nein
9	# 0				

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der Benutzerkennungen

Kennung

Beschreibung

Gesperrt

Max. Passwort-Gültigkeit

Passwort-Änderung erlaubt

2.12.2 "Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen", Fenster "Export von Benutzerdaten"

Klicken Sie auf den Link **Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen**, um die Liste aller eingerichteten Benutzerkennungen und aller Zugriffsrechtegruppen, die den Benutzerkennungen zugewiesen sind, für eine Anlage anzeigen zu lassen. Beim Klicken auf den Link werden die angeforderten Daten in einem neu geöffneten Browser-Fenster angezeigt.

Um die Daten in einer Datei auf Ihrem System zu speichern, wählen Sie im neu geöffneten Browser-Fenster die Funktion **Datei** -> **Speichern unter** und speichern Sie die Datei als **Textdatei** (***.txt**).

Wenn Sie die Daten direkt in eine Textdatei exportieren möchten, ohne sie vorher anzuzeigen, klicken Sie mit der rechten Maustaste auf den Link **Liste der Benutzerkennungen**, wählen Sie im Kontextmenü die Option **Ziel speichern unter**, und speichern Sie die Datei als **Textdatei** (***.txt**).

Die Daten der Textdatei können Sie in ein Tabellenkalkulationsprogramm importieren, um sie zu formatieren oder auszuwerten, z. B. in MS Excel mit **Daten** -> **Externe Daten** -> **Textdatei importieren**. Benutzerkennung und dazugehörige Beschreibung werden in jeder Zeile angezeigt.

	A	B	C	D
1	**# eur.cgi v1.0**			
2	**Export von Benutzerdaten: Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen**	**24.06.2010 14:33**	**Manager**	**0.520**
3	**Kennung**	**Beschreibung**	**ID der Zugriffsrechtegruppe**	**Beschreibung der Zugriffsrechtegruppe**
4	stevie	stevieb@mycomp.com, x12345	arg3	Local Administrator
5	gert	gertf@mycomp.com, x98765	arg2	Config. Management read-only
6			all-PM	Alle Zugriffsrechte von "Performance Management"
7	peter	peters@mycomp.com, x24680	arg3	Local Administrator
8			all-RepGen	Alle Zugriffsrechte von "Report Generator"
9	mark	markw@mycomp.com, x86420	all-SysM	Alle Zugriffsrechte von "Systemverwaltung"
10			arg2	Config. Management read-only
11	chris	chriss@mycomp.com, x13579	all-cm_subadm	Alle Zugriffsrechte von "Configuration Management"
12			all-SysM	Alle Zugriffsrechte von "Systemverwaltung"
13			all-FaultM	Alle Zugriffsrechte von "Fault Management"
14	# 0			

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen

Kennung

Beschreibung

ID der Zugriffsrechtegruppe

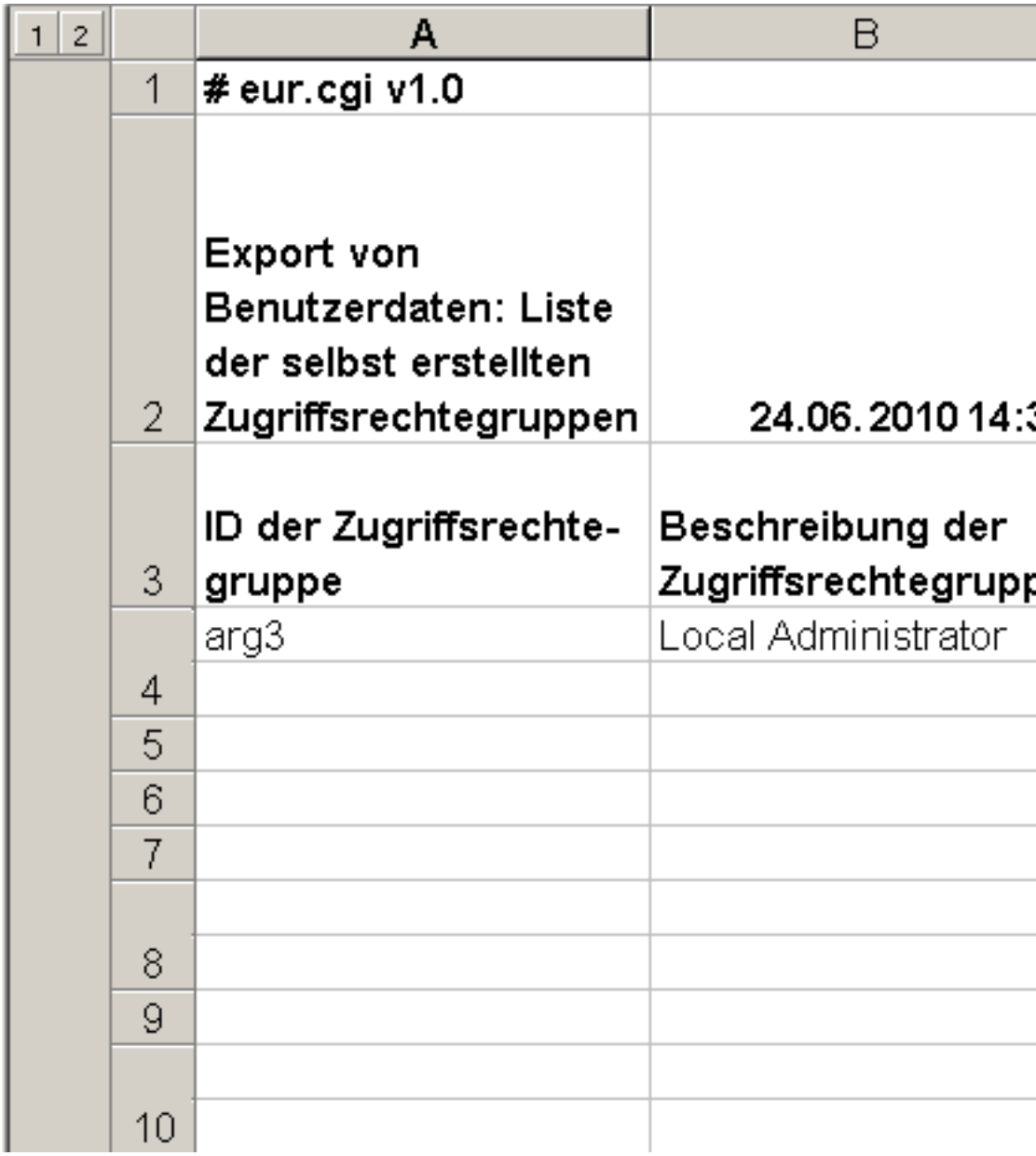
Beschreibung der Zugriffsrechtegruppe

2.12.3 "Liste der selbst erstellten Zugriffsrechtegruppen", Fenster "Export von Benutzerdaten"

Klicken Sie auf den Link **Liste der selbst erstellten Zugriffsrechtegruppen**, um die Liste aller selbst erstellten Zugriffsrechtegruppen und deren zugewiesene Zugriffsrechte anzeigen zu lassen. Beim Klicken auf den Link werden die angeforderten Daten in einem neu geöffneten Browser-Fenster angezeigt.

Um die Daten in einer Datei auf Ihrem System zu speichern, wählen Sie im neu geöffneten Browser-Fenster die Funktion **Datei** -> **Speichern unter** und speichern Sie die Datei als **Textdatei** (***.txt**).

Wenn Sie die Daten direkt in eine Textdatei exportieren möchten, ohne sie vorher anzuzeigen, klicken Sie mit der rechten Maustaste auf den Link **Liste der Benutzerkennungen**, wählen Sie im Kontextmenü die Option **Ziel speichern unter**, und speichern Sie die Datei als **Textdatei** (***.txt**). Die Daten der Textdatei können Sie in ein Tabellenkalkulationsprogramm importieren, um sie zu formatieren oder auszuwerten, z. B. in MS Excel mit **Daten** -> **Externe Daten** -> **Textdatei importieren**. Benutzerkennung und dazugehörige Beschreibung werden in jeder Zeile angezeigt.



1 2		A	B
	1	# eur.cgi v1.0	
	2	Export von Benutzerdaten: Liste der selbst erstellten Zugriffsrechtegruppen	24.06.2010 14:3
	3	ID der Zugriffsrechte-gruppe	Beschreibung der Zugriffsrechtegrupp
		arg3	Local Administrator
	4		
	5		
	6		
	7		
	8		
	9		
	10		

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der selbst erstellten Zugriffsrechtegruppen

ID der Zugriffsrechtegruppe

Beschreibung der Zugriffsrechtegruppe

ID der Komponente

Beschreibung der Komponente

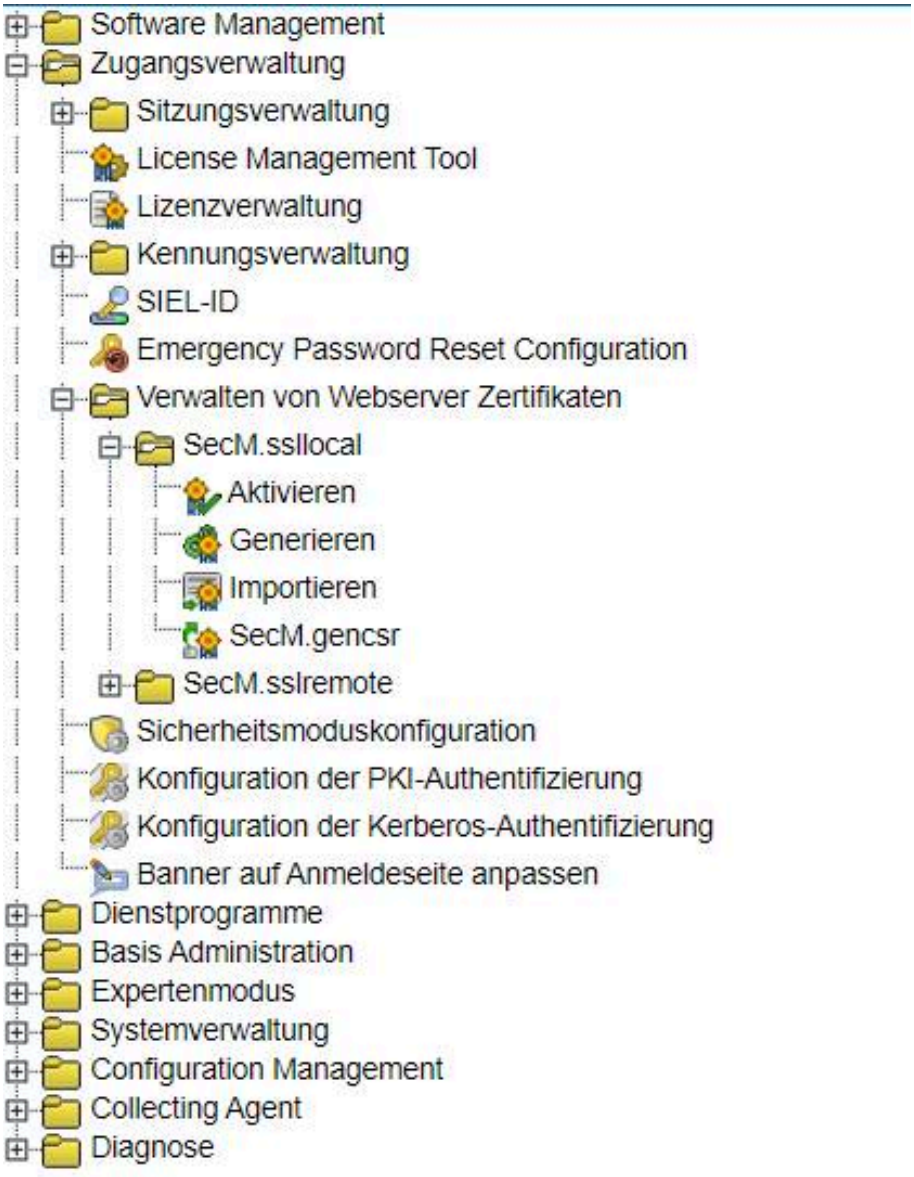
ID des Zugriffsrechts

Beschreibung des Zugriffsrechts

2.13 Verwalten von Web-Server-Zertifikaten

Der Bereich **Verwalten von Web-Server-Zertifikaten** umfasst folgende Funktionsbereiche:

- Zertifikate für diesen Web-Server
  - Aktivieren - Bei NICHT INSTALLIERTER HG35xx-Baugruppe
  - Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant
  - Generieren
  - Import
  - Über CSR generieren
- Zertifikate für Netzverwaltung
  - Stammzertifikat
  - CSR signieren
  - Import der Zertifizierungsstelle (CA) zur Verteilung an die Clients



2.13.1 Zertifikate für diesen Web-Server

Zwei asymmetrische öffentliche Schlüsselalgorithmen werden für Webserver-Zertifikate unterstützt:

- RSA

  RSA wurde 1994 standardisiert und ist der am häufigsten verwendete Algorithmus, der den Test der Zeit bestanden hat. Der Schlüssel hat eine Länge von 2048 Bits und gilt als Sicherheitsstandard.
- ECDSA

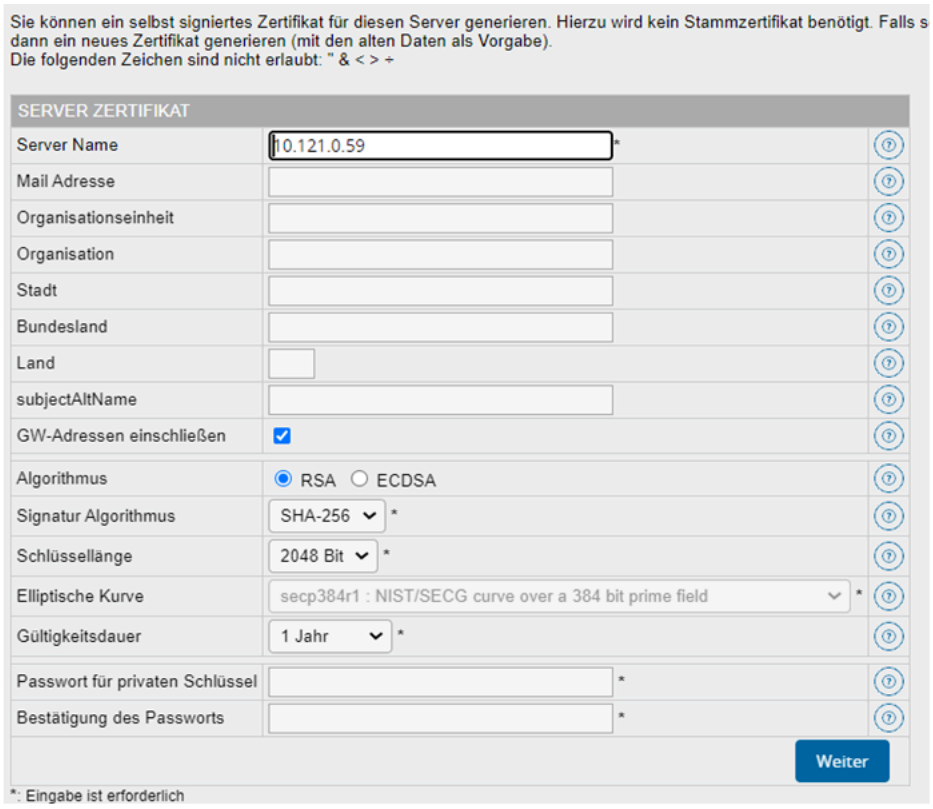
  ECDSA wurde 2005 standardisiert und bietet im Vergleich zu RSA das gleiche Maß an Sicherheit, jedoch mit kleineren Schlüsselgrößen. Kleinere Schlüssel führen zu schnelleren Berechnungen und weniger Speicherplatzbedarf.

SHA-2-Unterstützung für Digitalsignaturen

OpenScape 4000 unterstützt SHA-2-Hash-Verschlüsselungsfunktionen für das digitale Signieren auf dem System generierter Zertifikate. SHA-2 bietet eine höhere Sicherheit für die generierten Zertifikate. Die in OpenScape 4000 implementierte SHA-2-Familie besteht aus mehreren Hash-Funktionen: SHA256, SHA384 und SHA512 (SHA224 wird nicht vom Internet Explorer unterstützt und daher nicht als Option bereitgestellt). Die Zahl im Funktionsnamen gibt die Länge des Hash-Werts in Bits an. OpenScape 4000 verwendet zum Generieren und Signieren von Zertifikaten das Tool OpenSSL.

Sie können die folgenden Parameter während der Generierung eines Zertifikats wählen. Die SPE SSL-Stammzertifikat- und SPE SSL-Zertifikat-Dialoge bieten:

- Optionsfeld "Algorithmentyp", wobei die Auswahl folgende Parameter beeinflusst
- Ein Signaturalgorithmus-Dropdown-Feld, in dem Sie die kryptografische Funktion auswählen können: SHA-256, SHA-384 oder SHA-512.
- Für RSA muss die Schlüssellänge angegeben werden. Die Mindestlänge von 2048 Bits gilt als Sicherheitsstandard.
- Für ECDSA muss die elliptische Kurve angegeben werden. Alle openssl-unterstützten elliptischen Kurven für ECDSA-Algorithmus sind hier aufgeführt. Die populärsten Kurven sind: NIST-genehmigte Suite B, z. B. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1).



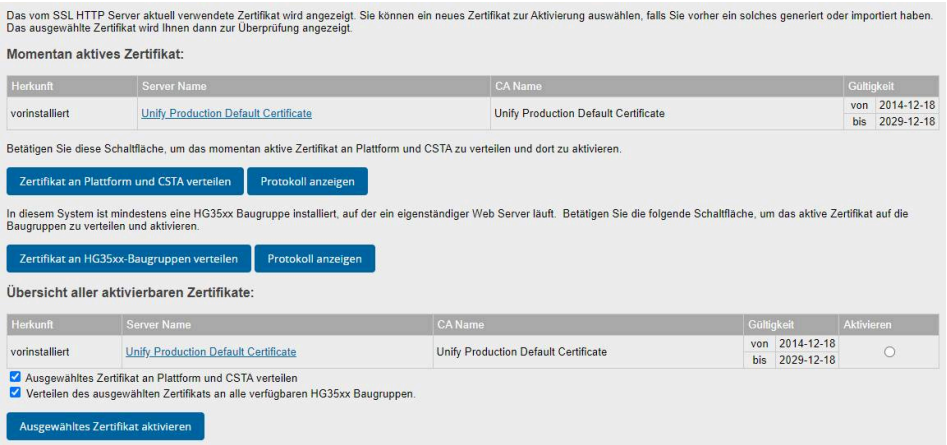
- Aktivieren - HG35xx-Platine NICHT installiert
- Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant
- Generieren
- Importieren
- Über CSR generieren

2.13.1.1 Aktivieren - HG35xx-Platine NICHT installiert

Navigieren Sie auf der **Startseite** von **Access Management** zu **Webserverzertifikate verwalten -> Zertifikate für diesen Webserver**.

Klicken oder doppelklicken Sie auf **Aktivieren**, um den Dialog **Serverzertifikat aktivieren** zu öffnen. Folgende Zertifikate werden angezeigt:

- Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)
- Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)



Benutzeroberfläche

Die folgenden Zertifikate werden im **Dialogfeld Serverzertifikat** aktivieren angezeigt:

- Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)

  Das vom SSL HTTP-Server aktuell verwendete, d.h. momentan aktive Sicherheitszertifikat, und
- Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

  In dieser Liste werden alle aktivierbaren Zertifikate angezeigt. Sie können aus dieser Liste ein neues Zertifikat zur Aktivierung auswählen, falls Sie vorher ein solches generiert oder importiert haben. Das ausgewählte Zertifikat wird Ihnen dann zur Überprüfung angezeigt.

  Nur signierte Zertifikate können aktiviert werden.

NOTICE: Die Software wird standardmäßig mit vorinstalliertem Sicherheitszertifikat ausgeliefert. Bei vorinstalliertem Zertifikat muss kein Passwort eingegeben werden. Das Feld Passworteintrag wird nicht mit vorinstallierten Zertifikaten angezeigt.

Verteilen des AKTUELL AKTIVEN Zertifikats an die Plattform - nur Assistant

1) Klicken Sie auf die **Schaltfläche Zertifikat an Plattform verteilen** unterhalb der Tabelle **Derzeit aktive Zertifikate**.

   Der folgende Dialog **Serverzertifikat aktivieren** wird angezeigt und Sie werden aufgefordert, das Passwort für den privaten Schlüssel des Zertifikats einzugeben.
2) Geben Sie das Passwort ein und klicken Sie auf **Zertifikat verteilen**.
3) Der **Status**dialog zeigt dann den Fortschritt der Verteilung und Aktivierung an.

4) Nach Abschluss der Verteilung erscheint eine der folgenden Meldungen:

- eine Bestätigungsmeldung über das erfolgreiche Verteilen des Zertifikats oder
- eine Fehlermeldung, die angibt, dass beim Übertragen des aktiven Server-Zertifikats auf die Plattform ein Fehler aufgetreten ist.

Die Fehlermeldung wird auf dem Bildschirm angezeigt und Sie werden aufgefordert, den Vorgang zu wiederholen.

5) Falls der Fehler weiterhin auftritt, sollten Sie die angezeigte Fehlermeldung an Ihren Systemadministrator oder an den Service weiterleiten.

NOTICE:

Bei Standalone und Survivable SoftGates und Standalone und Survivable EntGW leitet die SoftGate SW das Webzertifikat vom Assistant an das Platform Portal weiter, bevor der Apache-Webserver zur Aktivierung des Zertifikats neu gestartet wird.

Aktivieren eines Zertifikats

Möchten Sie ein anderes als das momentan aktive Zertifikat aktivieren, gehen Sie wie folgt vor:

1) Im Dialog **Serverzertifikat aktivieren**, Tabelle **Übersicht aller aktivierbaren Zertifikate**, Spalte **Aktivieren**, wählen Sie das Optionsfeld des Zertifikats, das Sie aktivieren möchten. Wenn Sie möchten, dass das ausgewählte Zertifikat aktiviert und gleichzeitig an die Plattform verteilt wird, aktivieren Sie das Kontrollkästchen **Ausgewähltes Zertifikat an Plattform verteilen**, das sich unterhalb der Tabelle **Übersicht aller aktivierbaren Zertifikate** befindet. (Die Verteilung von Zertifikaten an die Plattform ist nur für den %%assistant%% verfügbar.)

Nur signierte Zertifikate können aktiviert werden.

2) Klicken Sie auf **Weiter**.

Die Zertifikatsdetails werden dann im Dialog **Serverzertifikat aktivieren** angezeigt und das Programm fordert Sie auf, das Passwort für den privaten Schlüssel einzugeben.

Bei vorinstallierten Zertifikaten ist die Eingabe des Passworts nicht erforderlich, und daher wird keine Eingabeaufforderung und kein Passwort-Eingabefeld angezeigt.

3) Geben Sie das **Passwort** für den privaten Schlüssel ein, falls erforderlich, und klicken Sie auf **Zertifikat aktivieren**.

NOTICE: Der Web-Server und die OpenScape 4000-Prozesse müssen nach dem Aktivieren eines neuen Zertifikats immer neu gestartet werden. Dabei werden alle laufenden Sitzungen auf dem Server beendet, auch die eigene Sitzung.

Eine Warnmeldung des Servers wird angezeigt und weist darauf hin, dass der Web-Server und die OpenScape 4000-Prozesse nach dem Aktivieren eines neuen Zertifikats neu gestartet werden müssen, und dass dabei alle

laufenden Sitzungen - auch die eigene Sitzung - auf dem Server beendet werden.

Das ausgewählte Zertifikat wird aktiviert und im Dialogfeld **Serverzertifikat aktivieren** als neues, **derzeit aktives Zertifikat** angezeigt.

oder

4) Klicken Sie im Dialog Serverzertifikat **aktivieren** auf **Zurück,** wenn Sie das neue Zertifikat nicht aktivieren möchten.

Feldbeschreibungen

Aktivieren (Link auf Startseite der Zugangsverwaltung)

Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)

Herkunft (Spalte in den Tabellen "Derzeit aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Serverzertifikat aktivieren")

Servername (Spalte in den Tabellen "Derzeit aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Serverzertifikat aktivieren")

Zertifikatsinformationen (Dialogfeld “Zertifikat anzeigen”, erreichbar durch Klicken auf Link in Spalte “Server Name”)

Zertifikat löschen (Schaltfläche in Ansicht “Zertifikatsinformationen”, Dialogfeld “Zertifikat anzeigen”)

CA-Name (Spalte in den Tabellen Aktuell aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Serverzertifikat aktivieren)

Gültigkeit (von / bis) (Spalte in den Tabellen Aktuell aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialog Serverzertifikat aktivieren)

Aktives Zertifikat verteilen (Schaltfläche unter der Tabelle Aktuell aktives Zertifikat, Dialog Serverzertifikat aktivieren **)**

Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

Aktivieren (Optionsfeld in der Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Serverzertifikat aktivieren **)**

Verteilen des ausgewählten Zertifikats an alle verfügbaren HG35xx-Baugruppen (Kontrollkästchen unter Tabelle “Übersicht aller aktivierbaren Zertifikate”, Dialogfeld “Server-Zertifikat aktivieren”)

Ausgewähltes Zertifikat aktivieren (Schaltfläche unter Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zertifikat aktivieren (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

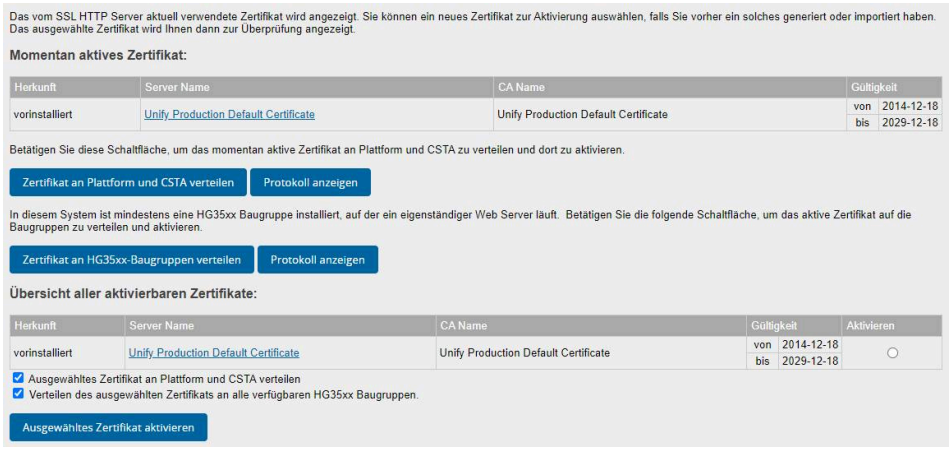
Zurück (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

2.13.1.2 Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant

Falls in diesem System mindestens eine HG35xx-Platine installiert ist, auf der ein eigenständiger Web-Server läuft, werden im Dialogfeld **Server-Zertifikat aktivieren** die folgenden zusätzlichen Steuerelemente angezeigt:

- Aktives Zertifikat verteilen (Schaltfläche unter Tabelle Derzeit aktive Zertifikat-Tabelle, Dialogfeld Server-Zertifikat aktivieren)

- Verteilen des ausgewählten Zertifikats an alle verfügbaren HG35xx-Baugruppen (Kontrollkästchen unter Tabelle “Übersicht aller aktivierbaren Zertifikate”, Dialogfeld “Server-Zertifikat aktivieren”)



Anmerkung: Die HG35xx-Platinen, die nicht auf Linux (STMI und NCUI) basieren, unterstützen nur RSA-Zertifikate für die webbasierte Verwaltung. Wenn der ausgewählte Zertifikattyp ECDSA ist, wird er nicht an diese Platinentypen verteilt. Alle SoftGate-basierten Platinen unterstützen ECDSA.

Benutzeroberfläche

Die folgenden Zertifikate werden im Dialogfeld **Server-Zertifikat aktivieren** angezeigt:

- Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)

  Das vom SSL HTTP-Server aktuell verwendete, d.h. momentan aktive Sicherheitszertifikat, und
- Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

  In dieser Liste werden alle aktivierbaren Zertifikate angezeigt. Sie können aus dieser Liste ein neues Zertifikat zur Aktivierung auswählen, falls Sie vorher ein solches generiert oder importiert haben. Das ausgewählte Zertifikat wird Ihnen dann zur Überprüfung angezeigt.

  Nur signierte Zertifikate können aktiviert werden.

Anmerkung: Die Software wird standardmäßig mit vorinstalliertem Sicherheitszertifikat ausgeliefert. Bei vorinstalliertem Zertifikat muss kein Passwort eingegeben werden. Das Feld für die Eingabe des Passworts wird beim vorinstallierten Zertifikat nicht angezeigt.

Verteilen des AKTUELL AKTIVEN Zertifikats an die Plattform - nur Assistant

1) Klicken Sie auf die Schaltfläche **Zertifikat an Plattform verteilen** unter der Tabelle **Derzeit aktives Zertifikat**.

Das folgende Dialogfeld **Server-Zertifikat aktivieren** wird angezeigt und Sie werden aufgefordert, das Passwort für den privaten Schlüssel des Zertifikats einzugeben.

2) Geben Sie das Passwort ein und klicken Sie auf **Zertifikat verteilen**.

3) Im Dialogfeld **Status** wird dann der Fortschritt der Verteilung und Aktivierung angezeigt.

4) Nach Abschluss der Verteilung erscheint eine der folgenden Meldungen:

- eine Bestätigungsmeldung über das erfolgreiche Verteilen des Zertifikats oder
- eine Fehlermeldung, die angibt, dass beim Übertragen des aktiven Server-Zertifikats auf die Plattform ein Fehler aufgetreten ist.

Die Fehlermeldung wird auf dem Bildschirm angezeigt und Sie werden aufgefordert, den Vorgang zu wiederholen.

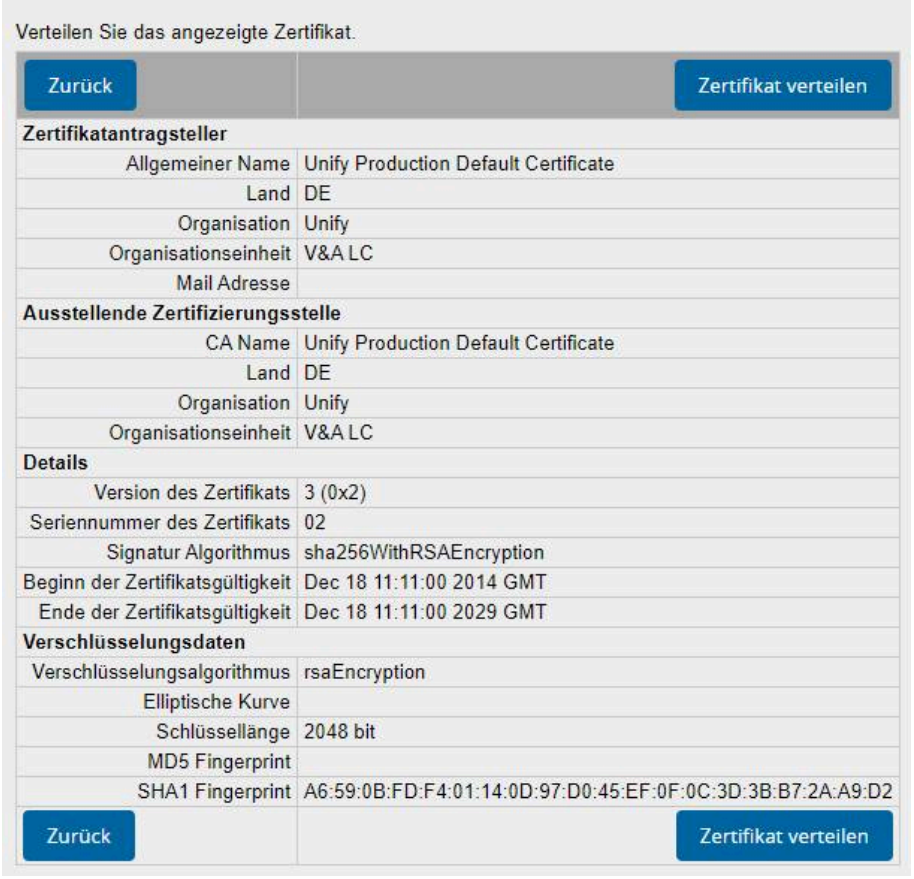
5) Falls der Fehler weiterhin auftritt, sollten Sie die angezeigte Fehlermeldung an Ihren Systemadministrator oder an den Service weiterleiten.

Anmerkung: Die HG35xx-Platinen, die nicht auf Linux (STMI und NCUI) basieren, unterstützen nur RSA-Zertifikate für die webbasierte Verwaltung. Wenn der ausgewählte Zertifikattyp ECDSA ist, wird er nicht an diese Platinentypen verteilt. Alle SoftGate-basierten Platinen unterstützen ECDSA.

Verteilen des MOMENTAN AKTIVEN Zertifikats an alle verfügbaren HG35xx-Baugruppen

1) Klicken Sie auf die Schaltfläche **Zertifikat an HG35xx-Platinen verteilen** unter der Tabelle **Derzeit aktives Zertifikat** .

   Das folgende Dialogfeld **Server-Zertifikat aktivieren** wird angezeigt und Sie werden aufgefordert, das Passwort für den privaten Schlüssel des Zertifikats einzugeben.



2) Geben Sie das Passwort ein und klicken Sie auf **Zertifikat verteilen**.
3) Im Dialogfeld **Status** wird dann der Fortschritt der Verteilung und Aktivierung angezeigt.
4) Nach Abschluss der Verteilung erscheint eine der folgenden Meldungen:

   - eine Bestätigungsmeldung über das erfolgreiche Verteilen des Zertifikats oder
   - eine Fehlermeldung, die angibt, dass beim Übertragen des aktiven Server-Zertifikats auf die HG35xx-Baugruppen ein Fehler aufgetreten ist.

   Die vom System ausgegebene Fehlermeldung wird am Bildschirm angezeigt und Sie werden aufgefordert, den Vorgang zu wiederholen. Falls der Fehler erneut auftritt, sollten Sie die Konfiguration über das Gateway Dashboard überprüfen, die Baugruppenliste aktualisieren und eine Verbindung zu allen aufgelisteten Baugruppen herstellen.
5) Falls der Fehler weiterhin auftritt, sollten Sie die angezeigte Fehlermeldung an Ihren Systemadministrator oder an den Service weiterleiten.

Aktivieren und Verteilen eines AUSGEWÄHLTEN Zertifikats an alle verfügbaren HG35xx-Baugruppen bzw. an die Plattform (nur auf dem Assistant)

Wenn Sie ein anderes Zertifikat anstelle des derzeit aktiven aktivieren möchten, folgen Sie bitte den Schritten, die im Abschnitt **Aktivieren eines Zertifikats** beschrieben sind.

Möchten Sie das ausgewählte Zertifikat beim Aktivieren zugleich auch an alle verfügbaren HG35xx-Baugruppen bzw. an die Plattform verteilen, so gehen Sie bitte wie folgt vor:

1) Aktivieren Sie das Kontrollkästchen **Das ausgewählte Zertifikat an die Plattform verteilen**, das sich unter der Tabelle **Übersicht aller aktivierbaren Zertifikate** befindet.
2) Aktivieren Sie das Kontrollkästchen **Das ausgewählte Zertifikat an alle verfügbaren HG35xx-Platinen verteilen**, das sich unter der Tabelle **Übersicht aller aktivierbaren Zertifikate** befindet.
3) Klicken Sie auf die Schaltfläche **Ausgewähltes Zertifikat aktivieren**, die sich unterhalb der Tabelle **Übersicht aller aktivierbaren Zertifikate** befindet.

   Das ausgewählte Zertifikat wird wie gewohnt auf dem Server aktiviert und zugleich an alle verfügbaren HG35xx-Baugruppen verteilt.

Feldbeschreibungen

Aktivieren (Link auf Startseite der Zugangsverwaltung)

Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)

Herkunft (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Server-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zertifikatsinformationen (Dialogfeld “Zertifikat anzeigen”, erreichbar durch Klicken auf Link in Spalte “Server Name”)

Zertifikat löschen (Schaltfläche in Ansicht “Zertifikatsinformationen”, Dialogfeld “Zertifikat anzeigen”)

CA-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Gültigkeitsdauer (von/bis) (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Aktives Zertifikat verteilen (Schaltfläche unter Tabelle Derzeit aktives Zertifikat, Dialogfeld Server-Zertifikat aktivieren**)**

Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

Aktivieren (Optionsschaltfläche in Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren**)**

Verteilen des ausgewählten Zertifikats an alle verfügbaren HG35xx-Baugruppen (Kontrollkästchen unter Tabelle “Übersicht aller aktivierbaren Zertifikate”, Dialogfeld “Server-Zertifikat aktivieren”)

Ausgewähltes Zertifikat aktivieren (Schaltfläche unter Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

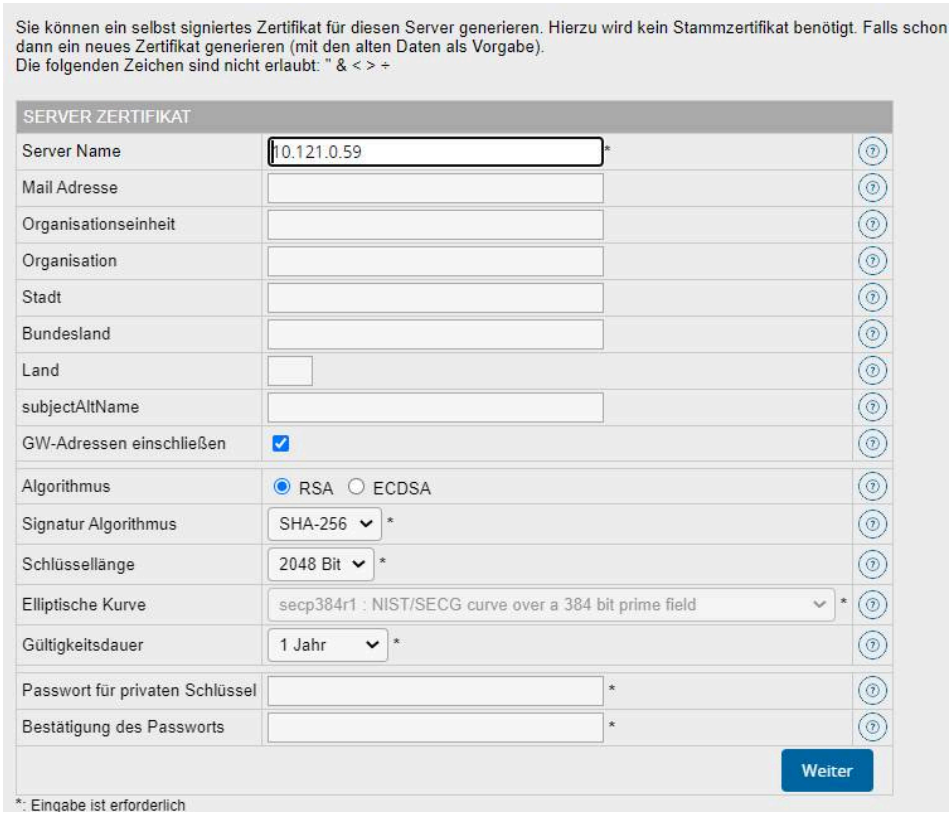
Zertifikat aktivieren (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

Zurück (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

2.13.1.3 Generieren

Das Leistungsmerkmal **Generieren** bietet die einfachste Methode, um ein neues SSL-Sicherheitszertifikat für den Server zu erzeugen und vom Server selbst signieren zu lassen.

Der Server erzeugt hierfür eine interne, eigene CA-Zertifizierungsstelle, die das neu erzeugte Zertifikat automatisch selbst signiert. Der Name dieser CA-Zertifizierungsstelle ist immer identisch mit dem Server-Namen. Das so erzeugte und selbstsignierte Zertifikat kann daraufhin aktiviert werden. Zum Erzeugen eines neuen Zertifikats ist kein Stammzertifikat erforderlich.



Falls bereits ein selbstsigniertes Zertifikat für den Server existiert, werden die Daten des vorhandenen Zertifikats mit einem entsprechenden Hinweis unter **Zertifikat anzeigen** angezeigt.

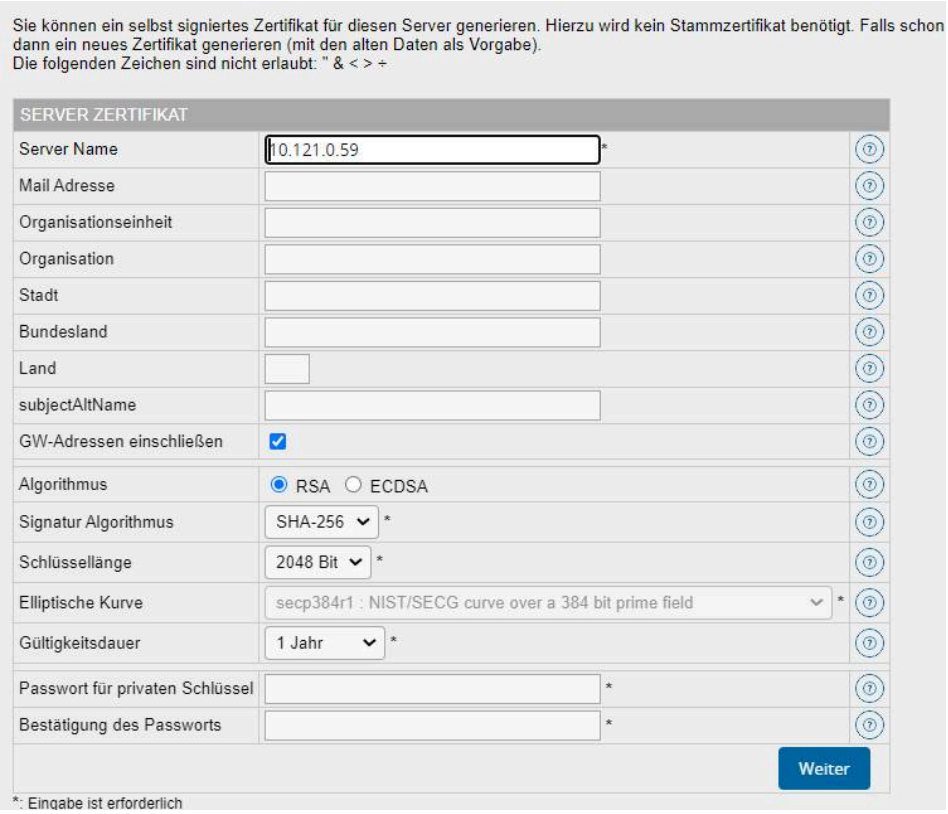
NOTICE: Warnung Falls bereits ein selbst signiertes Zertifikat für diesen Server existiert und Sie trotzdem ein neues erzeugen, wird das vorhandene Zertifikat überschrieben.

Neues Zertifikat generieren

Navigieren Sie auf der **Startseite** der **Zugangsverwaltung** zu dem Bereich **Verwalten von Web-Server-Zertifikaten -> Zertifikate für diesen Web-Server** und klicken bzw. doppelklicken Sie auf **Generieren**.

Es existiert bereits ein selbstsigniertes Zertifikat für diesen Server

Falls bereits ein selbstsigniertes Zertifikat für diesen Server existiert, werden die Daten des vorhandenen Zertifikats im Browser unter **Zertifikat anzeigen** angezeigt. Ein Hinweis gibt an, dass bereits ein selbstsigniertes Zertifikat auf diesem Server existiert.

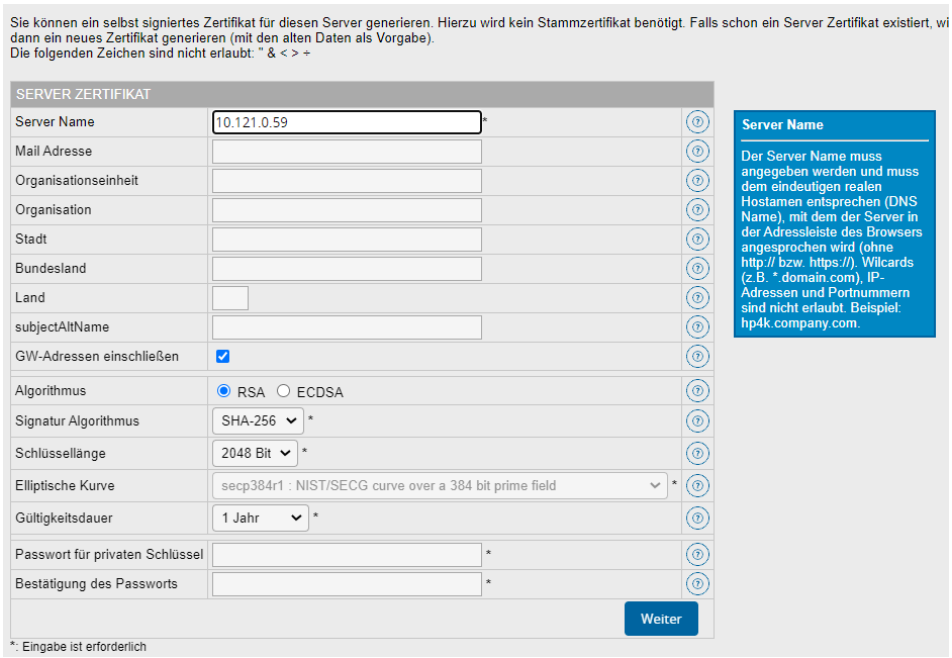


Falls noch kein selbstsigniertes Zertifikat für diesen Server existiert, springt das Programm direkt zum Dialogfeld **Server-Zertifikat (selbstsigniert)** generieren. In einigen Feldern werden Standardwerte angezeigt, die Sie übernehmen können.

NOTICE: Warnung Falls bereits ein selbst signiertes Zertifikat für diesen Server existiert und Sie trotzdem ein neues erzeugen, wird das vorhandene Zertifikat überschrieben.

Klicken Sie im Dialogfeld **Zertifikat anzeigen** auf **Neues Zertifikat**.

Das Dialogfeld **Server-Zertifikat (selbstsigniert) generieren** wird angezeigt. Es enthält zusätzliche Hinweise zur Dateneingabe. Bitte beachten Sie die Hinweise. Folgende Zeichen dürfen in den Eingabefelder nicht verwendet werden: **" & < > Ã·** sowie Akzente und Sonderzeichen.



Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

1) Zusätzliche Kontext-Informationen zu den einzelnen Eingabefeldern erhalten Sie, indem Sie auf das Symbol "**?**" rechts neben dem jeweiligen Feld klicken. Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.

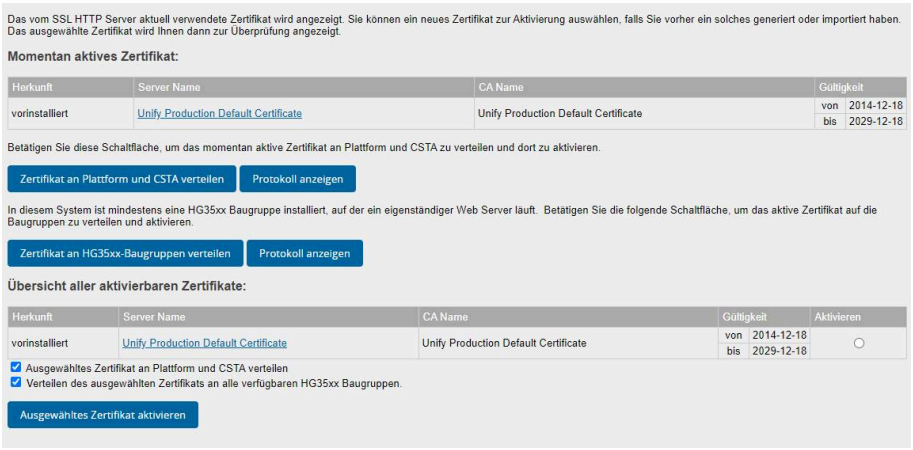
2) Geben Sie alle erforderlichen Daten ein, und klicken Sie auf **Weiter**.

Durch Eingabe eines **Passworts** sichern Sie den privaten Schlüssel des Zertifikats gegen Missbrauch.

NOTICE: Dieses Passwort wird nirgendwo gespeichert! Es muss daher beim Aktivieren dieses Zertifikats erneut eingegeben werden, auch wenn dies Tage oder Monate später erfolgt. Ein Zertifikat ist unbrauchbar, wenn das Passwort vergessen wurde.

Nach dem Erzeugen eines neuen Zertifikats springt das Programm zurück zum Dialogfeld **Server-Zertifikat aktivieren**. Das neu erzeugte Zertifikat

wird angezeigt und ist in der Regel bereits vorausgewählt (markiert). In der Spalte **Herkunft** steht in diesem Fall **Generiert**.



3) Um das neu generierte Zertifikat zu aktivieren, markieren Sie die Optionsschaltfläche des Zertifikats in der Spalte **Aktivieren** - sofern diese nicht bereits markiert ist - und klicken Sie auf **Weiter**.

Die Detaildaten des markierten Zertifikats werden im Dialogfeld **Server-Zertifikat aktivieren** angezeigt und Sie werden aufgefordert, das Passwort für den privaten Schlüssel zu diesem Zertifikat einzugeben.

Nur signierte Zertifikate können aktiviert werden.

4) Geben Sie das **Passwort** ein und klicken Sie dann auf **Zertifikat aktivieren**.

Das markierte Zertifikat wird aktiviert und als neues **Momentan aktives Zertifikat** im Dialogfeld **Server-Zertifikat aktivieren** angezeigt.

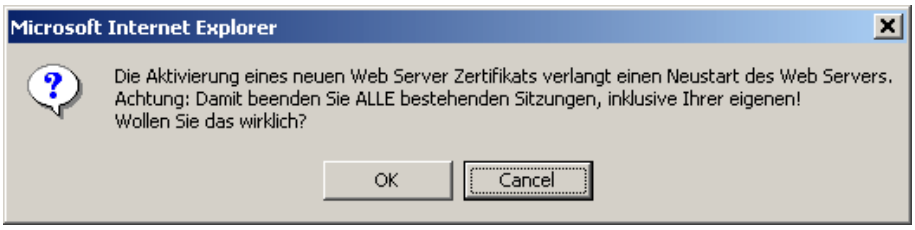
Der **Status** der aktivierbaren Zertifikate wird zusätzlich durch eine **Farbe** angezeigt. Die Farben haben folgende Bedeutung:

rot = signiertes Zertifikat, im Server aktiviert

grün = signiertes Zertifikat vorhanden, aktivierbar

NOTICE: Der Web-Server und die OpenScape 4000-Prozesse müssen nach dem Aktivieren eines neuen Zertifikats immer neu gestartet werden. Dabei werden alle laufenden Sitzungen auf dem Server beendet, auch die eigene Sitzung.

Eine Warnmeldung des Servers wird angezeigt und weist darauf hin, dass der Web-Server nach dem Aktivieren eines neuen Zertifikats neu gestartet werden muss, und dass dabei alle laufenden Sitzungen - auch die eigene Sitzung - auf dem Server beendet werden.



Wenn Sie auf **OK** klicken, wird das markierte Zertifikat aktiviert und als neues **Momentan aktives Zertifikat** im Browser angezeigt.

Verteilen eines Zertifikats an alle verfügbaren HG35xx-Baugruppen eines Systems

Falls auf dem aktuellen System mindestens eine HG35xx-Baugruppe installiert ist, auf der ein eigenständiger Web-Server läuft, haben Sie die Möglichkeit, das momentan aktive Zertifikat oder ein ausgewähltes Zertifikat an alle verfügbaren HG35xx-Baugruppen zu verteilen. Weitere Informationen hierzu finden Sie unter folgenden Links:

- **Verteilen des MOMENTAN AKTIVEN Zertifikats an alle verfügbaren HG35xx-Baugruppen**

  und
- Aktivieren und Verteilen eines AUSGEWÄHLTEN Zertifikats an alle verfügbaren HG35xx-Baugruppen bzw. an die Plattform (nur auf dem Assistant)

Dialogfeld "Server-Zertifikat (selbstsigniert) generieren", Feldbeschreibungen

Server-Name

Mail-Adresse

Organisationseinheit

Organisation

Stadt

Bundesland

Land

Zugangsverwaltung - Beschreibung der Felder on page 161

Signatur-Algorithmus

Schlüssellänge

Gültigkeitsdauer

Passwort für privaten Schlüssel

Bestätigung des Passworts

Weiter (Schaltfläche)

Dialogfeld "Server-Zertifikat aktivieren", Feldbeschreibungen

Aktivieren (Link auf Startseite der Zugangsverwaltung)

Momentan aktives Zertifikat (Tabelle in Dialogfeld "Server-Zertifikat aktivieren")

Herkunft (Spalte in Tabellen "Momentan aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Server Name (Spalte in Tabellen "Momentan aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Zertifikatsinformationen (Dialogfeld "Zertifikat anzeigen", erreichbar durch Klicken auf Link in Spalte "Server Name")

Zertifikat löschen (Schaltfläche in Ansicht "Zertifikatsinformationen", Dialogfeld "Zertifikat anzeigen")

CA Name (Spalte in Tabellen "Momentan aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Gültigkeit (von / bis) (Spalte in Tabellen "Momentan aktives Zertifikat" und "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Aktives Zertifikat verteilen (Schaltfläche unter Tabelle "Momentan aktives Zertifikat", Dialogfeld "Server-Zertifikat aktivieren"**)**

Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld "Server-Zertifikat aktivieren")

Aktivieren (Optionsschaltfläche in Tabelle "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren"**)**

Verteilen des ausgewählten Zertifikats an alle verfügbaren HG35xx-Baugruppen (Kontrollkästchen unter Tabelle "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Ausgewähltes Zertifikat aktivieren (Schaltfläche unter Tabelle "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Zertifikat aktivieren (Schaltfläche, Dialogfeld "Server-Zertifikat aktivieren")

Zurück (Schaltfläche, Dialogfeld "Server-Zertifikat aktivieren")

2.13.1.4 Import

Dieses Leistungsmerkmal ermöglicht das Importieren eines auf einem anderen Host erzeugten Zertifikats inklusive privatem Schlüssel. Es werden X.509 PEM und PKCS #12 Dateien unterstützt. Nach dem Importieren muss der Web-Server für die Benutzung dieses Zertifikats und des zugehörigen privaten Schlüssels konfiguriert werden. Um den verschlüsselten privaten Schlüssel zu entschlüsseln, muss das Passwort eingegeben werden.

Neues Zertifikat importieren

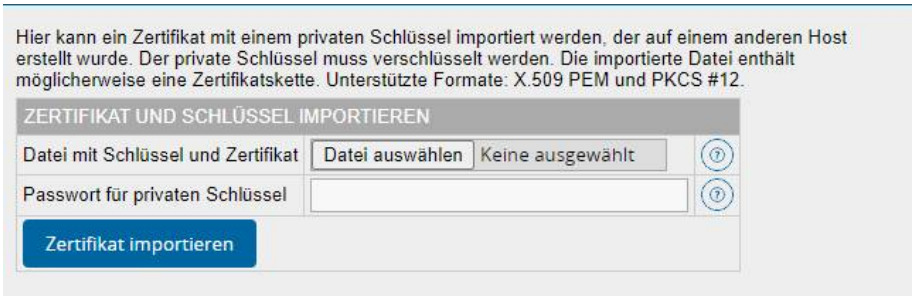
1) Navigieren Sie auf der **Startseite** der **Zugangsverwaltung** zu dem Bereich **Verwalten von Web-Server-Zertifikaten -> Zertifikate für diesen Web-Server**.
2) Klicken bzw. doppelklicken Sie auf **Importieren**.

   Das Dialogfeld **Server-Zertifikat und Schlüssel importieren** wird angezeigt. Unter folgenden Bedingungen ist das Importieren eines auf einem anderen Host erzeugten Zertifikats inklusive privatem Schlüssel möglich:

   - Unterstütztes Dateiformat: X. 509 PEM und PKCS #12. Falls die Dateinamenerweiterung *.p12 ist, wird die Datei als PKCS#12 behandelt,

für andere Dateinamenerweiterungen wird das X.509 PEM Format vorausgesetzt.

- Privater Schlüssel und Passwort zum Entschlüsseln sind erforderlich und vorhanden.



3) Klicken Sie auf **Durchsuchen** und wählen Sie die entsprechende Datei aus.

   Unterstütztes Dateiformat: X. 509 PEM und PKCS #12. Falls die Dateinamenerweiterung *.p12 ist, wird die Datei als PKCS#12 behandelt, für andere Dateinamenerweiterungen wird das X.509 PEM Format vorausgesetzt.

4) Geben Sie das **Passwort** für die Entschlüsselung des privaten Schlüssels ein.

5) Klicken Sie auf **Importieren**.

   Das Programm springt zurück zum Dialogfeld **Server-Zertifikat aktivieren**. Das importierte Zertifikat wird angezeigt und ist bereits ausgewählt (markiert). In der Spalte **Herkunft** steht in diesem Fall **Importiert**. Das importierte Zertifikat kann jetzt aktiviert werden.

   Der **Status** des markierten Zertifikats wird jetzt zusätzlich durch eine **Farbe** angezeigt. Die Farben haben folgende Bedeutung:

   rot = signiertes Zertifikat, im Server aktiviert

   grün = signiertes Zertifikat vorhanden, aktivierbar

Feldbeschreibungen

Datei mit Schlüssel und Zertifikat (Eingabefeld)

Passwort für privaten Schlüssel (Eingabefeld)

Zertifikat importieren (Schaltfläche)

2.13.1.5 Über CSR generieren

Das Leistungsmerkmal **Über CSR generieren** dient dazu, eine Zertifikatsanforderung (CSR = Certificate Sign Request) für ein neues Zertifikat zu erzeugen. Zu Testzwecken wird die Zertifikatsanforderung automatisch in ein selbst signiertes Zertifikat umgewandelt, das Sie testen können. Nach dem Testen des selbstsignierten Zertifikats können Sie die Zertifikatsanforderung exportieren und an eine Zertifizierungsintanz (CA) übertragen. Sobald die Zertifizierungsinstanz Ihnen das signierte Zertifikat zurückgeschickt hat, können Sie dieses importieren und aktivieren.

Vorhandene Zertifikatsanforderungen (CSRs) und Zertifikate anzeigen

1) Navigieren Sie auf der **Startseite** der **Zugangsverwaltung** zu dem Bereich **Verwalten von Web-Server-Zertifikaten -> Zertifikate für diesen Web-Server**.
2) Klicken bzw. doppelklicken Sie auf den Link **Über CSR generieren**.
3) Das Dialogfeld **Zertifikat über CSR generieren** wird geöffnet.

   - Falls noch kein selbstsigniertes Zertifikat bzw. keine Zertifikatsanforderung auf dem Server vorhanden ist, wird das leere Dialogfeld **Zertifikat über CSR generieren** angezeigt und es erscheint die Meldung: **Es wurden noch keine Zertifikatsanforderungen (CSR) erzeugt.**. In diesem Fall müssen Sie erst eine neue Zertifikatsanforderung erzeugen. Siehe Neue Zertifikatsanforderung (CSR) generieren.
   - Falls bereits Zertifikatsanforderungen auf diesem Server existieren, wird das Dialogfeld **Zertifikat über CSR generieren** geöffnet. Darin werden alle vorhandenen Zertifikate und Zertifikatsanforderungen (CSRs) angezeigt.
   - Es können maximal 5 Zertifikate verwaltet werden.
   - Zum **Anzeigen** oder **Löschen** des Zertifikats bitte den **Server-Namen** anklicken.
   - Zum **Verlängern** des Zertifikats bitte in der Spalte **Gültigkeitsdauer** auf das **Ablaufdatum** anklicken.
   - Die **Legende** im Dialogfeld **Zertifikat über CSR generieren** enthält die Informationen zum **Status** und erklärt die Funktion der Symbolschaltflächen **testen**, **exportieren**, **importieren**, **aktivieren**. Die Aktionen **testen**, **exportieren**, **importieren**, **aktivieren** sind jeweils abhängig vom aktuellen Zustand eines Zertifikats ausführbar bzw. nicht ausführbar.
   - Der **Status** der angezeigten CSRs bzw. Zertifikate wird durch spezifische Farben angezeigt. Die **Farben** haben folgende Bedeutung:

   rot = signiertes Zertifikat, im Server aktiviert grün = signiertes Zertifikat vorhanden, aktiv, bereit zur Aktivierung gelb = CSR exportiert, Zertifikat noch ohne Signatur blau = CSR generiert, noch nicht exportiert

Zertifikatsdaten über Link "Server Name" anzeigen

1) Klicken Sie auf den angezeigten Server-Namen in der Spalte **Server Name**.

   Das Programm springt zurück zum Dialogfeld **Zertifikat anzeigen** und zeigt die Detaildaten des Zertifikats unter **Zertifikatsinformationen** an.
2) Klicken Sie auf **Weiter**.

   Das Programm springt zurück zum Dialogfeld **Zertifikat über CSR generieren** und zeigt alle vorhandenen CSRs und Zertifikate an.

Neue Zertifikatsanforderung (CSR) generieren

1) Navigieren Sie auf der **Startseite** der **Zugangsverwaltung** zu dem Bereich **Verwalten von Web-Server-Zertifikaten -> Zertifikate für diesen Web-Server**.
2) Klicken Sie auf **Über CSR generieren**, um eine neue Zertifikatsanforderung zu erzeugen.

   - **Neue Zertifikatsanforderung (CSR) generieren - Es existiert noch keine CSR**

     Falls noch kein selbstsigniertes Zertifikat bzw. keine Zertifikatsanforderung auf dem Server vorhanden ist, wird das leere Dialogfeld **Zertifikat über CSR generieren** angezeigt und es erscheint die Meldung: **Es wurden noch keine Zertifikatsanforderungen (CSR) erzeugt.**. In diesem Fall müssen Sie erst eine neue Zertifikatsanforderung erzeugen. Siehe Neue Zertifikatsanforderung (CSR) generieren.
   - **Neue Zertifikatsanforderung (CSR) generieren - Es existieren bereits CSRs**

3) Falls bereits Zertifikatsanforderungen auf diesem Server existieren, wird das Dialogfeld **Zertifikat über CSR generieren** geöffnet. Darin werden alle vorhandenen Zertifikate und Zertifikatsanforderungen (CSRs) angezeigt. Klicken Sie auf **Neue Zertifikatsanforderung generieren**.

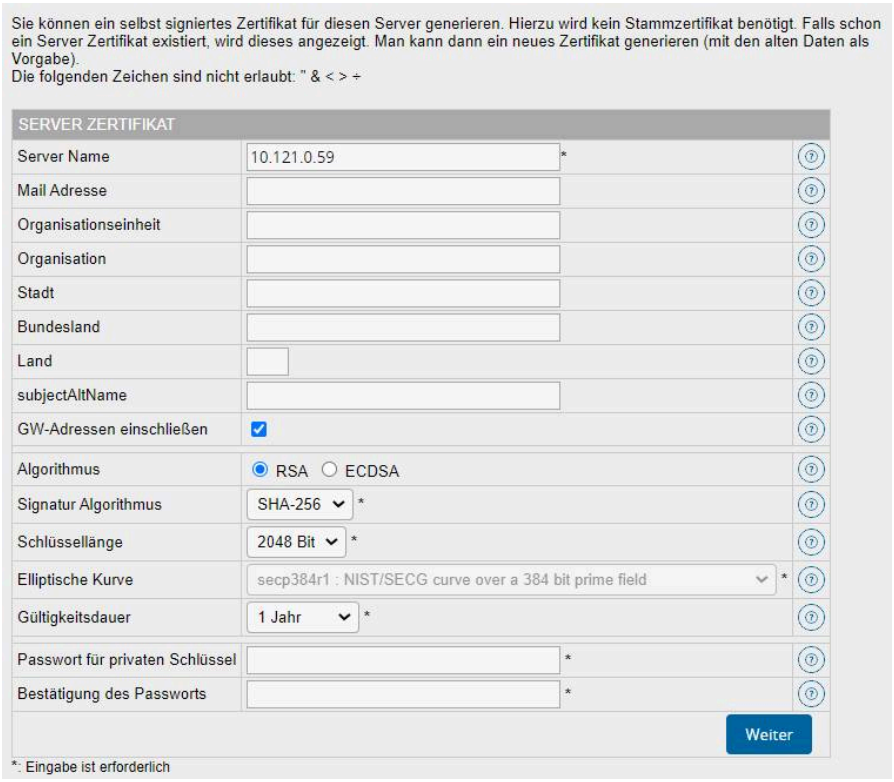
   a) Falls noch keine Zertifikatsanforderung (CSR) auf diesem Server existiert, wird das Dialogfeld **Server-Zertifikat (selbstsigniert) generieren** angezeigt.

   b) Falls bereits eine Zertifikatsanforderung bzw. ein selbstsigniertes Zertifikat auf diesem Server existiert, wird das Dialogfeld **Zertifikat über CSR generieren** angezeigt . Die Daten des vorhandenen, momentan aktivien Zertifikats werden in den Eingabefeldern angezeigt und können übernommen werden.

   Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

   Folgende Zeichen dürfen in den Eingabefelder nicht verwendet werden: **" & < > Ã·** sowie Akzente und Sonderzeichen.
4) Zusätzliche Kontext-Informationen zu den einzelnen Eingabefeldern erhalten Sie, indem Sie auf das Symbol "**?**" rechts neben dem jeweiligen

Feld klicken. Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.



5) Geben Sie alle erforderlichen Daten ein, und klicken Sie auf **Weiter**.

Durch Eingabe eines **Passworts** sichern Sie den privaten Schlüssel des Zertifikats gegen Missbrauch.

NOTICE: Dieses Passwort wird nirgendwo gespeichert! Es muss daher beim Aktivieren dieses Zertifikats erneut eingegeben werden, auch wenn dies Tage oder Monate später erfolgt. Ein Zertifikat ist unbrauchbar, wenn das Passwort vergessen wurde.

Zu jedem Eingabefeld werden beim Klicken auf "**?**" zusätzliche Infos angezeigt.

Zu Testzwecken wird die Zertifikatsanforderung beim Erzeugen automatisch in ein selbstsigniertes Zertifikat umgewandelt, das Sie anschließend testen können.

Neu erzeugte Zertifikatsanforderung anzeigen

6) Das Programm springt zum Dialogfeld **Zertifikat anzeigen**. Die Daten der neuen Zertifikatsanforderung werden angezeigt, sowie die Bestätigung "Ihre Zertifikatsanforderung wurde erzeugt und zu Testzwecken automatisch signiert."

7) Klicken Sie auf **Weiter**.

Das Dialogfeld **Zertifikat über CSR generieren** wird geöffnet. Das generierte Zertifikat wird angezeigt und ist BLAU markiert. Die Farbe BLAU zeigt den Status "CSR generiert, noch nicht exportiert" an.

Neues, selbstsigniertes Zertifikat testen

8) Testen Sie das neue, selbstsignierte Zertifikat, indem Sie im Dialogfeld **Zertifikat über CSR generieren** in der Spalte **Bearbeiten** auf das Symbol **Testen** klicken.

Nach erfolgreichem Test springt das Programm zurück zum Dialogfeld **Server-Zertifikat aktivieren**. In der Spalte **Herkunft** steht in diesem Fall **Über CSR generiert**. Das generierte Test-Zertifikat wird angezeigt und ist bereits ausgewählt und GRÜN markiert. Das Zertifikat ist jetzt selbstsigniert und aktivierbar.

Der **Status** des markierten Zertifikats wird zusätzlich durch eine Farbe angezeigt. Die **Farben** haben folgende Bedeutung:

rot = signiertes Zertifikat, im Server aktiviert

grün = signiertes Zertifikat vorhanden, aktiv, bereit zur Aktivierung

gelb = CSR exportiert, Zertifikat noch ohne Signatur

blau = CSR generiert, noch nicht exportiert

Die Aktionen **testen**, **exportieren**, **importieren**, **aktivieren** sind jeweils abhängig vom aktuellen Zustand eines Zertifikats ausführbar bzw. nicht ausführbar.

Neue Zertifikatsanforderung (CSR) exportieren

9) **Exportieren** Sie nach erfolgreichem Test das CSR, indem Sie in der Spalte **Bearbeiten** auf das Symbol **Exportieren** klicken.

Das Dialogfeld **Zertifikatsanforderung (CSR) exportieren** wird angezeigt. Der Inhalt (verschlüsselter Code) des Zertifikats wird im Bereich **CSR exportieren** angezeigt.

Abhängig vom Status des jeweiligen Zertifikats können diese Schaltflächen aktiviert bzw. nicht aktiviert werden (grau dargestellt).

CSR mit Copy&Paste kopieren oder als Datei exportieren

10) Kopieren Sie den Inhalt des CSRs entweder mit Copy&Paste in eine Textdatei, die sie anschließend speichern, oder exportieren Sie den Inhalt des CSR als Datei, indem Sie auf **CSR als Datei exportieren** klicken.

NOTICE: Beachten Sie bitte, dass Sie beim Kopieren mit Copy&Paste die erste Zeile (---BEGIN CERTIFICATE REQUEST ---) und die letzte Zeile (---END CERTIFICATE REQUEST ---) mit kopieren und sichern müssen.
Der verwendete Server-Typ ist "Apache + mod_ssl + OpenSSL".

---

11) Wenn Sie auf **CSR als Datei exportieren** klicken, öffnet sich das Dialogfeld **Dateidownload**. Klicken Sie in diesem Dialogfeld auf **Speichern**, und **nicht** auf **Öffnen**.

12) Der Dateiname **server.csr** im Feld **Dateiname** wird vom Programm vorgegeben. Sie können diesen Namen übernehmen oder in einen beliebigen anderen Dateinamen ändern. Speichern Sie die Datei in einem Ordner Ihrer Wahl.

13) Sobald das Dialogfeld **Download beendet** angezeigt wird, klicken Sie auf **Schließen**, um den Vorgang zu beenden.

14) Das exportierte CSR können Sie zum Signieren an die Zertifizierungsinstanz schicken.

    Das Exportieren kann für jedes CSR beliebig oft wiederholt werden.

    Nach erfolgreichem Exportieren wird der Status des exportierten CSRs im Dialogfeld **Zertifikat über CSR generieren** auf GELB gesetzt. Dies bedeutet, dass das Zertifikat bereits einmal exportiert wurde. Der **Status** der angezeigten CSRs bzw. Zertifikate wird durch spezifische Farben angezeigt. Die **Farben** haben folgende Bedeutung:

    rot = signiertes Zertifikat, im Server aktiviert

    grün = signiertes Zertifikat vorhanden, aktiv, bereit zur Aktivierung

    gelb = CSR exportiert, Zertifikat noch ohne Signatur

    blau = CSR generiert, noch nicht exportiert

    Signiertes Zertifikat importieren

    Ein von einer externen Zertifizierungsinstanz signiertes Zertifikat, das zu einer vorher generierten Zertifikatsanforderung (CSR) mit einem entsprechenden privaten Schlüssel gehört, kann unter Angabe des Passworts für den privaten Schlüssel importiert und angezeigt werden.

15) **Importieren** Sie das signierte Zertifikat, sobald Sie es von der Zertifizierungsinstanz erhalten haben, indem Sie im Dialogfeld **Zertifikat über CSR generieren** in der Spalte **Bearbeiten** auf das Symbol **Importieren** des CSRs klicken, das Sie zum Signieren an die Zertifizeriungsinstanz geschickt haben.

    Um ein Zertifikat importieren zu können, müssen Sie es zuvor exportiert haben.

    Ähnlich wie beim Exportieren von CSRs können Sie auch beim **Importieren** den Inhalt des signierten Zertifikats mit Copy&Paste aus einer Textdatei in den angezeigten Bereich unter **SIGNIERTES ZERTIFIKAT IMPORTIEREN** kopieren oder das Zertifikat als Datei importieren, indem Sie auf **Durchsuchen** klicken und den gewünschten Dateinamen auswählen.

    Passwort für den privaten Schlüssel eingeben

16) Geben Sie das **Passwort für den privaten Schlüssel** ein und klicken Sie dann auf **Weiter**. Nach erfolgreichem Importieren wird das importierte, signierte Zertifikat im Dialogfeld **Zertifikat über CSR generieren** als aktivierbares Zertifikat angezeigt.

    Die Aktionen **testen**, **exportieren**, **importieren**, **aktivieren** sind jeweils abhängig vom aktuellen Zustand eines Zertifikats ausführbar bzw. nicht ausführbar.

Importiertes, signiertes Zertifikat anzeigen

Nach erfolgtem Importieren wird der **Status** des importierten Zertifikats auf GRÜN gesetzt. GRÜN bedeutet, dass das Zertifikat importiert und signiert wurde und jetzt aktivierbar ist.

Der **Status** der angezeigten CSRs bzw. Zertifikate wird durch spezifische Farben angezeigt. Die **Farben** haben folgende Bedeutung:

rot = signiertes Zertifikat, im Server aktiviert

grün = signiertes Zertifikat vorhanden, aktiv, bereit zur Aktivierung

gelb = CSR exportiert, Zertifikat noch ohne Signatur

blau = CSR generiert, noch nicht exportiert

Um ein importiertes Zertifikat zu aktivieren, gehen Sie so vor wie im Abschnitt Aktivieren - Bei NICHT INSTALLIERTER HG35xx-Baugruppe beschrieben. Nur signierte Zertifikate können aktiviert werden.

Feldbeschreibungen

Server Name (Tabellenspalte)

CA Name (Tabellenspalte**)**

Gültigkeit (von / bis) (Tabellenspalte**)**

Generiert (Tabellenspalte)

Exportiert (Tabellenspalte)

Importiert (Tabellenspalte)

Bearbeiten (Tabellenspalte)

Testen (Schaltfläche)

Exportieren (Schaltfläche)

Importieren (Schaltfläche)

Aktivieren (Schaltfläche)

Zertifikatsinformationen

Zertifikat löschen (Schaltfläche)

Server-Name (Eingabefeld)

Mail-Adresse

Organisationseinheit

Organisation

Stadt

Bundesland

Land

Signatur-Algorithmus

Schlüssellänge

Gültigkeitsdauer

Passwort für privaten Schlüssel

Bestätigung des Passworts

Weiter (Schaltfläche)

Zurück (Schaltfläche)

2.13.2 Zertifikate für Netzverwaltung

Der Bereich **Zertifikate für Netzverwaltung** umfasst Leistungsmerkmale zur Verwaltung von SSL-Sicherheitszertifikaten innerhalb eines OpenScape/HiPath 4000-Netzwerks. Diese Leistungsmerkmale sind für Nutzer erforderlich, die

über ein OpenScape/HiPath 4000-Netzwerk verfügen, in dem ein OpenScape 4000 Manager-Server eine oder mehrere OpenScape/HiPath 4000-Assistant-Anlagen verwaltet.

Folgende Leistungsmerkmale stehen zur Verfügung:

Stammzertifikat

CSR signieren

Import der Zertifizierungsstelle (CA) zur Verteilung an die Clients

2.13.2.1 Stammzertifikat

Dieses Leistungsmerkmal bietet Ihnen die Möglichkeit, ein eigenes Stammzertifikat (Root Certificate) einzurichten, das zum Signieren aller externen Zertifikatsanforderungen (CSRs) für sämtliche Anlagen innerhalb eines OpenScape/HiPath 4000-Netzwerks verwendet werden kann.

Ziel dieses Features ist, die SSL-Sicherheitszertifikate für alle Anlagen innerhalb eines OpenScape/HiPath 4000-Netzwerks von nur einer Zertifizierungsinstanz signieren und zertifizieren zu lassen.

Nur die Root-CA muss in die einzelnen Browser importiert werden, nicht das Zertifikat selbst.

Ein Stammzertifikat ist ein selbstsigniertes Zertifikat eines besonderen Typs. Der Unterschied zwischen selbstsigniertem Zertifikat und Stammzertifikat besteht darin, dass beim selbstsignierten Zertifikat der Server-Name anzugeben ist, während beim Stammzertifikat ein Name für die Zertifizierungsinstanz (CA) angegeben wird. Der Name des Stammzertifikats bezieht sich nicht auf einen bestimmten Server.

Dialog Stammzertifikat öffnen

- Klicken Sie auf **Startseite -> Zugangsverwaltung -> Zertifikate für Netzverwaltung**.

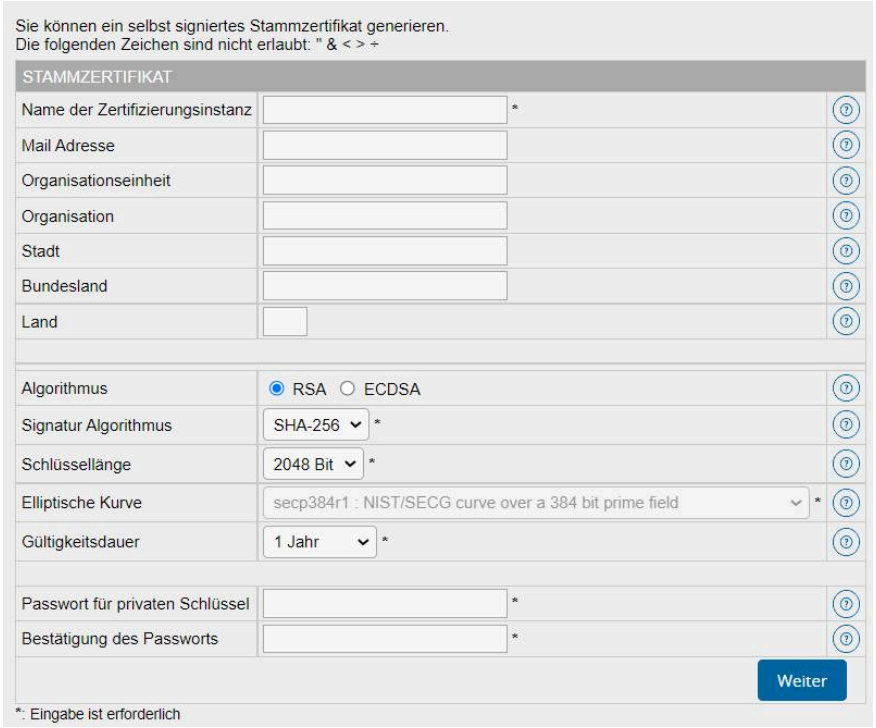
  Das Dialogfeld **Stammzertifikat** wird angezeigt.

  – **Es existiert noch kein Stammzertifikat**

  Falls noch kein Stammzertifikat für diesen Server erzeugt wurde, wird das Dialogfeld **Stammzertifikat** mit leeren Feldern angezeigt.

  – **Stammzertifikat existiert bereits**

  Falls bereits ein selbstsigniertes Stammzertifikat für diesen Server existiert, werden die Daten des vorhandenen Zertifikats zusammen mit einem entsprechenden Hinweis im Browser unter **Stammzertifikat** angezeigt.



Stammzertifikate signieren, herunterladen, erzeugen

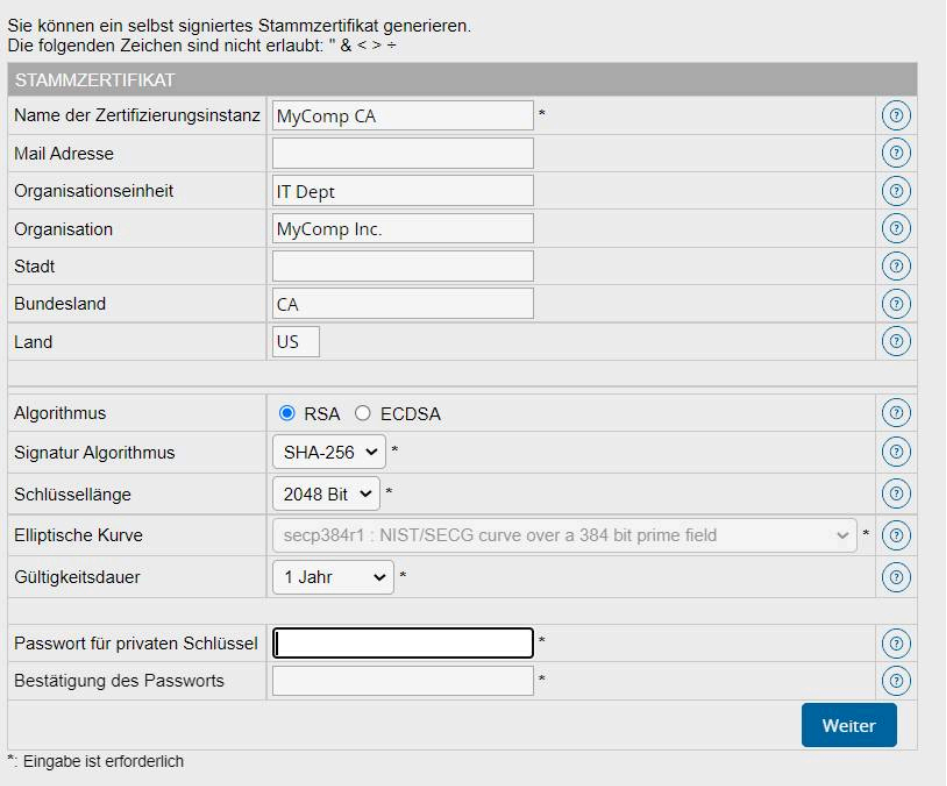
WARNING: Falls bereits ein selbstsigniertes Stammzertifikat für diesen Server existiert und Sie trotzdem ein neues erzeugen, wird das vorhandene Stammzertifikat überschrieben.

1) Falls Sie das vorhandene Stammzertifikat zum Signieren von Zertifikatsanforderungen verwenden möchten, klicken Sie auf CSR signieren.

   Mit diesem Stammzertifikat können Sie externe Zertifikatsanforderungen signieren.
2) Sie können das Stammzertifikat herunterladen, es zu den Vertrauenswürdigen Stammzertifikaten (Trusted Root CA store) und in die Java Runtime Environment (Java Laufzeitumgebung) importieren, indem Sie auf den **Link 'Stammzertifikat'** klicken.
3) Falls Sie ein neues Stammzertifikat erzeugen und das vorhandene Stammzertifikat überschreiben möchten, klicken Sie auf Neues Stammzertifikat (Schaltfläche).

Neues Stammzertifikat erzeugen

Nach Klick auf **Neues Stammzertifikat** wird im Dialogfeld **Stammzertifikat** das Dialogfeld **Stammzertifikat generieren** angezeigt.



Die Daten des existierenden Stammzertifikats werden - sofern vorhanden - in den Eingabefeldern angezeigt und können übernommen werden.

1) Geben Sie alle erforderlichen Daten ein.

   Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

   Folgende Zeichen dürfen in den Eingabefelder nicht verwendet werden: **" & < > Ã·** sowie Akzente und Sonderzeichen.
2) Zusätzliche Kontext-Informationen zu den einzelnen Eingabefeldern erhalten Sie, indem Sie auf das Symbol "**?**" rechts neben dem jeweiligen Feld klicken. Die kontext-spezifischen Infos werden als "Tooltips" neben den Eingabefeldern eingeblendet.
3) Klicken Sie auf **Weiter**.

Neu erzeugtes Stammzertifikat anzeigen

Die Daten des neu erzeugten Stammzertifikats sowie die folgende Meldung werden angezeigt:

"Das Zertifikat wurde erzeugt. Mit diesem Stammzertifikat können Sie nun externe Zertifikatsanforderungen signieren."

1) Klicken Sie auf CSR signieren, um externe Zertifikatsanforderungen mit dem neu erzeugten Stammzertifikat zu signieren.

Feldbeschreibungen

Link "Stammzertifikat"

Neues Stammzertifikat (Schaltfläche)

Name der Zertifizierungsinstanz (Eingabefeld)

Mail-Adresse

Organisationseinheit

Organisation

Stadt

Bundesland

Land

Signatur-Algorithmus

Schlüssellänge

Gültigkeitsdauer

Passwort für privaten Schlüssel

Bestätigung des Passworts

Weiter (Schaltfläche)

2.13.2.2 CSR signieren

Dieses Leistungsmerkmal bietet Ihnen die Möglichkeit, alle externen Zertifikatsanforderungen (CSRs) für sämtliche Anlagen innerhalb eines OpenScape/HiPath 4000-Netzwerks zu signieren.

Voraussetzung ist, dass Sie zuvor ein eigenes selbstsigniertes Stammzertifikat erzeugt haben.

Ziel dieses Features ist, die Zertifikatsanforderungen (CSRs) für alle Anlagen innerhalb eines OpenScape/HiPath 4000-Netzwerks unter Verwendung eines eigenen, selbstsignierten Stammzertifikats von nur einer lokalen Zertifizierungsstelle signieren und zertifizieren zu lassen.

1) Klicken Sie auf **Startseite -> Zugangsverwaltung -> CSR signieren**.

   Das Dialogfeld **Zertifikatsanforderung (CSR)** signieren wird angezeigt.

Es existiert noch kein Stammzertifikat

Falls noch kein Stammzertifikat für diesen Server erzeugt wurde, wird folgende Fehlermeldung auf dem ansonsten leeren Bildschirm angezeigt:

Fehler: Es wurde noch kein Stammzertifikat angelegt, um die Zertifikatsanforderungen zu signieren.

Erzeugen Sie ein neues Stammzertifikat - siehe Schrittanweisung unter Stammzertifikate signieren, herunterladen, erzeugen - und fahren Sie dann mit Schritt 2 oder 3 auf page 195 fort.

Zertifikatsanforderung mit Copy&Paste importieren

1) **Öffnen** Sie die Zertifikatsanforderung (CSR).

   Sie können den Inhalt des signierten Zertifikats entweder mit Copy&Paste aus einer Textdatei in den Bereich unter **Zertifikat einfügen** kopieren oder das Zertifikat als Datei importieren, indem Sie auf **Durchsuchen** klicken und den Dateinamen <dateiname.csr> auswählen.

   NOTICE: Wichtig: Es werden nur BASE64-kodierte PKCS#10-Requests akzeptiert. Bitte achten Sie darauf, auch die Begrenzungszeilen (BEGIN und END) zu kopieren!

Zertifikatsanforderung aus Datei importieren

1) Wenn Sie auf **Durchsuchen** klicken, öffnet sich das Dialogfeld **Dateidownload**. Wählen Sie in diesem Fenster den gewünschten Pfad und Dateinamen aus (z. B. server.csr) und klicken Sie dann auf **Speichern**, **nicht** auf **Öffnen**.

Passwort für privaten Schlüssel des Stammzertifikats eingeben

1) Geben Sie hier das **Passwort für den privaten Schlüssel** des Stammzertifikats ein und klicken Sie auf **Zertifikatsanforderung signieren**.
2) Das Programm springt zurück zum Dialogfeld **Zertifikat anzeigen** und zeigt die **Zertifikats-Informationen** an. Klicken Sie auf **Weiter**.
3) Das Dialogfeld **Zertifikatsanforderung (CSR) signieren** wird geöffnet. Der Inhalt des signierten Zertifikats (verschlüsselter Code) wird im Bereich **Signiertes Zertifikat exportieren** angezeigt. Die folgende Meldung wird angezeigt: "Das signierte Zertifikat wird angezeigt. Sie können das signierte Zertifikat nun in Ihrem externen Web Server importieren."
4) Klicken Sie auf **Signiertes Zertifikat als Datei exportieren** oder kopieren Sie den Inhalt des Zertifikats mit Copy&Paste in eine Textdatei, um diese anschließend zu speichern.

   NOTICE: Beachten Sie bitte, dass Sie beim Kopieren mit Copy&Paste die erste Zeile (---BEGIN CERTIFICATE REQUEST ---) und die letzte Zeile (---END CERTIFICATE REQUEST ---) mit kopieren und sichern müssen. Der verwendete Server-Typ ist "Apache + mod_ssl + OpenSSL".

5) Wenn Sie auf **Signiertes Zertifikat als Datei exportieren** klicken, öffnet sich das Dialogfeld **Dateidownload**. Klicken auf **Speichern**, und **nicht** auf **Öffnen**.
6) Der Dateiname **server.csr** im Feld **Dateiname** wird vom Programm vorgegeben. Sie können diesen Namen übernehmen oder in einen beliebigen anderen Dateinamen ändern. Speichern Sie die Datei in einem Ordner Ihrer Wahl.

7) Sobald das Dialogfeld **Download beendet** angezeigt wird, klicken Sie auf **Schließen**, um den Vorgang zu beenden.
8) Klicken Sie im Dialogfeld **Zertifikatsanforderung (CSR) signieren** auf **Weiter**. Das Programm springt zurück zum ersten Dialogfeld **Zertifikatsanforderung (CSR) signieren**, und Sie können ein nächstes CSR zum Signieren auswählen oder den Vorgang beenden.
9) Das exportierte, signierte CSR können Sie nun in Ihren Web-Server importieren.

Feldbeschreibungen

CSR signieren

Zertifikatsanforderung (CSR) signieren (Dialogfeld)

Zertifikat einfügen

Oder Zertifikatsanforderung von Datei importieren

Durchsuchen (Schaltfläche)

Passwort für privaten Schlüssel des Stammzertifikats

Zertifikatsanforderung signieren (Schaltfläche)

Signiertes Zertifikat als Datei exportieren (Schalffläche)

Weiter (Schaltfläche)

2.13.2.3 Import der Zertifizierungsstelle (CA) zur Verteilung an die Clients

Mit dieser Applikation können Sie die Zertifizierungsstelle (Certificate Authority, CA) an Clients importieren und an diese verteilen. Die Verteilung kann nur aktiviert werden, wenn das auf diesem Web-Server aktive Zertifikat durch ein CA-Zertifikat signiert ist. Die Applikation ist deaktiviert, wenn ein vordefiniertes oder selbstsigniertes Zertifikat auf dem Web-Server aktiv ist.

Die Verteilung eines importierten CA-Zertifikats an die Clients erfolgt in Schritt 4 der Client-Vorbereitung. Nur der öffentliche Schlüssel des CA-Zertifikats wird auf dem System gespeichert und bei der Verteilung bereitgestellt.

Konfiguration:

1) Navigieren Sie zu **Startseite -> Zugangsverwaltung -> Verwalten von Web-Server-Zertifikaten -> Zertifikate für Netzverwaltung -> Zertifizierungsstelle für die Verteilung importieren**

2) Importieren Sie den öffentlichen Schlüssel des an die Clients zu verteilenden CA-Zertifikats.
3) Aktivieren Sie die Verteilung, indem Sie das Kontrollkästchen aktivieren, und speichern Sie die Änderung.
4) Gehen Sie zur Client-Vorbereitung und stellen Sie sicher, dass das Zertifikat zur Verteilung bereitgestellt wird.

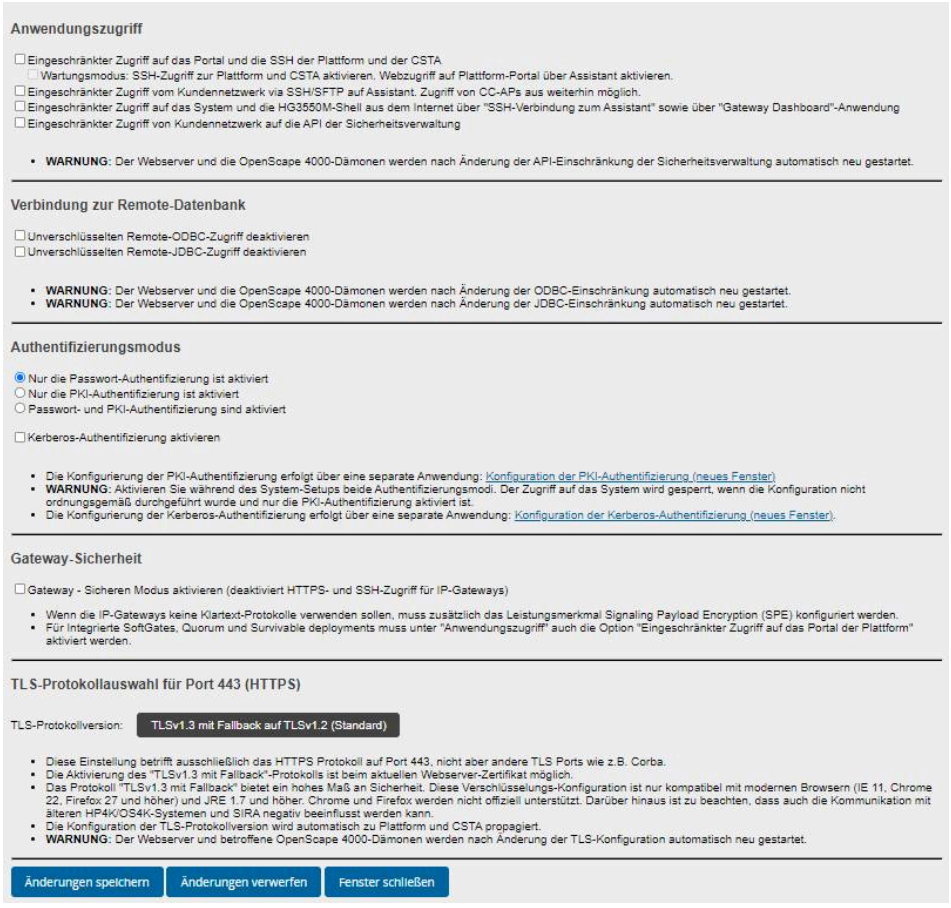
   An dieser Stelle können Sie eine Zertifizierungsstelle importieren, die auf einem anderen Host erstellt wurde. Unterstützt wird das Format X.509 PEM. Nur der öffentliche Schlüssel des Zertifikats wird benötigt.

2.14 Sicherheitsmoduskonfiguration

Starten Sie die Applikation.

Nur der Administrator hat Zugriff auf die Anwendung. Die Seite **Konfiguration** zum Konfigurieren des Sicherheitsmodus kann von der Startseite aus aufgerufen werden:

Sicherheitsmoduskonfiguration



NOTICE: Die Einstellungen für OpenScape 4000 Assistant und Manager können unterschiedlich sein.

Funktionalitäten

Die Seite **Konfiguration** zur Konfiguration des Sicherheitsmodus ist in folgende Steuerbereiche untergliedert:

2.14.1 Anwendungszugriff

Überblick

In diesem Bereich der Seite Sicherheitsmoduskonfiguration können Sie den Zugriff auf folgende Elemente steuern:

- Checkbox **Eingeschränkter Zugang zum Plattformportal**
  - Der Zugriff kann für alle Verbindungen zum Plattformportal (Protokoll http, Port: 443) und ssh (Port: 22) eingeschränkt werden.
  - Der Anwendungszugriff muss sowohl auf dem HHS als auch auf dem AP-E möglich sein. Die Sicherheitskonfiguration des AP-E wird bei der Wiederherstellung der APE automatisch durch die Einstellungen des HHS überschrieben.
  - DUPLEX-Szenario: Jede Plattform (einschließlich des Quorum-Knotens bei getrenntem Duplex) wird automatisch informiert / eingeschränkt.
- Checkbox **Wartungsmodus**: Aktivieren Sie den ssh- und Web-Zugang vom Assistant und den Zugang vom DLS.
  - Für Verbindungen vom Assistant kann Zugriff über ssh und Web (auf das Portal der Plattform) gewährt werden
  - Dies ist die neue Standardeinstellung ab V11 R1. Bei einem Update auf V11 R1 (oder neuer) von V11 R0 (oder älter) wird der Wartungsmodus automatisch aktiviert, wenn der "Eingeschränkte Zugriff" vorher nicht aktiviert war.

    NOTICE: Wenn der uneingeschränkte Zugriff auf das Plattformportal erforderlich ist, muss er nach jedem RLC-Update erneut aktiviert werden.
- Kontrollkästchen **Eingeschränkter Zugriff von Comwin auf ADP**
  - Der Zugriff von ComWin auf ADP ist gesperrt.
  - ComWin zeigt einen Fehler-Dialog (mit der Meldung "Connecticut Refused" (Verbindung abgelehnt) angezeigt, wenn der Zugriff eingeschränkt ist.
- Checkbox **Eingeschränkter Zugang zur System-Shell aus dem Kunden-Networking**

  Alle Verbindungen vom Kundennetzwerk zur System-Shell werden blockiert.

- Kontrollkästchen **SSH-Zugriff auf System und HG3550M aus den Anwendungen "SSH-Connect zum %%assistant%%" und "Gateway Dashboard" einschränken**
  - OpenScape 4000 stellt ein webbasiertes SSH-Terminal mit One-Click-Zugriff auf das System und HG3550M-Gateways bereit.
  - Der direkte SSH-Zugriff auf die Baugruppen (z. B. über Putty) ist weiterhin möglich, außer wenn 'Gateway - Sicherer Modus' aktiviert ist.
  - Webbasiertes SSH-Terminal zum System ist über die Anwendung *"Expertenmodus --> SSH-Connect zum Manager/%%assistant%%"* zugänglich.

    NOTICE: Wenn das Kontrollkästchen aktiviert ist, wird der Zugriff über das webbasierte Terminal deaktiviert.

  - Webbasiertes SSH-Terminal für HG3550M-Gateways ist über die Anwendung *"Gateway Dashboard"* zugänglich.

    NOTICE: Wenn das Kontrollkästchen aktiviert ist, wird der Zugriff über das webbasierte Terminal deaktiviert.

- Checkbox **Eingeschränkter Zugriff auf die Sicherheit Management-API aus dem Kundennetzwerk**
  - Verbindungen über die API der Sicherheitsverwaltung (secm.dll, secmcj.jar) werden blockiert.
  - Darf nur zum Härten der eigenständigen Systeme verwendet werden (nicht mit dem Manager verbunden)
  - Remote-Kommunikation zwischen Assistant und Manager wird blockiert
    - Erfassung von CDR-Daten (COL)
    - Remote-Login (Single Sign On) bei GUI / Applikationen
    - Ausführung von Stapelaufträgen
    - Remote-Verbindung zum RMX / Dipas-Batch
    - usw …

Nur Manager:

- Kontrollkästchen **Unterstützung von HiPath 4000-Altsystemen (Port 102 aktivieren)**
  - Wird benötigt, um die Abwärtskompatibilität zu älteren HiPath 4000-Systemen zu gewährleisten.
  - Der Standardwert ist "ausgeschaltet" (Sicherheit).

Anwendungszugriff aktivieren/deaktivieren

So aktivieren/deaktivieren Sie den Zugriff auf Anwendungen:

- Markieren Sie das entsprechende Kontrollkästchen, oder entfernen Sie die Markierung.
- Klicken Sie auf **Änderungen speichern**.

Die folgende Tabelle zeigt die Auswirkung des Kontrollkästchens "Eingeschränkter Zugriff auf die Sicherheitsmanagement-API aus dem Kundennetzwerk" auf Funktionen, die mit der Fernverbindung zwischen Manager und %%assistant%% zusammenhängen. Wie Sie sehen können, hängt diese Funktion ausschließlich von der Einstellung des %%assistant%

% ab. Wenn dieses Einschränkungs-Kontrollkästchen aktiviert ist, führt die Verwendung von Direktzugangsschaltflächen in der Systemverwaltung zu folgendem Fehler:

"Fehler: Automatische Anmeldung am Zielserver in Konto ERROR_FATAL_ERROR:cookie=non%20valid via NSL level

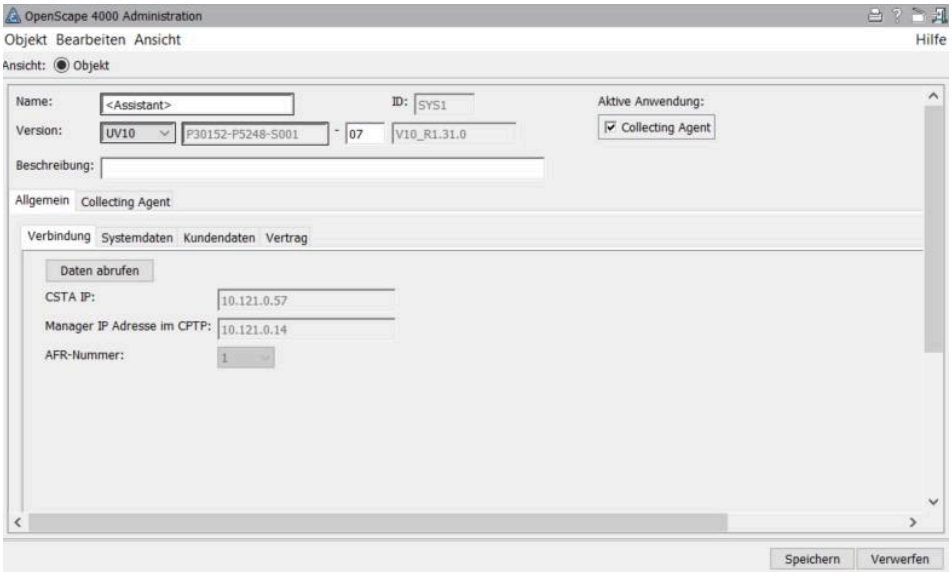
ERROR_FATAL_ERROR:cookie=non%20valid ist fehlgeschlagen."

Table 1: Übersicht über den Direktzugang der Systemverwaltung

Eingeschränkter Zugriff auf das Sicherheitsmanagement-API vom Kunden-Networking-Manager. V6R2 & V7 und neuer	Eingeschränkter Zugriff auf das Sicherheitsmanagement-API aus dem Kunden-Networking Assi. V6R2 & V7 und neuer	Remote-Verbindung vom Mgr. zum Asst.
		OK
	x	Nicht OK
x		OK
x	x	Nicht OK

Die Konfiguration der NLS-Kennungen beeinflusst die Funktion Direktzugang. NSL-Kennungen müssen entsperrt und Passwörter korrekt festgelegt werden. Die Änderung des Passworts für NSL-Konten ist obligatorisch und betrifft sowohl den Manager als auch den kooperierenden Assistenten (siehe auch Sicherheitscheckliste für OpenScape 4000 Assistant).

Direktzugang in der Systemverwaltung



Die folgende Tabelle zeigt die Auswirkungen des Kontrollkästchens "SSL für Comwin" in Kombination mit dem Kontrollkästchen "Eingeschränkter Zugriff von Comwin auf ADP" im Assistant V6 R2 & V7 auf die Verschlüsselung von Comwin (Expert Access). Der Expertenzugang über den Manager besteht einerseites aus der Verbindung von der Desktop-Anwendung zum Manager und andererseits aus der Verbindung vom Manager zum Assistant. Beide werden für alle unterstützten Assistant-Versionen in dieser Tabelle aufgelistet. Die

Steuerverbindungen über Port 7777 oder 7778 erfolgen immer im Klartext. Bei der Payload (AMO-Befehle und ihre Ausgabe) handelt es sich um eine mpcid-basierte Verbindung, die denselben Prinzipien unterliegt wie zuvor beschrieben.

Table 2: Übersicht über die ComWin-Verschlüsselung

SSL für Comwin Manager V6R2 & V7	Expert Access-Client <-> Mgr., Verschlüsselung bei Steuerverbindunge	Expert Access-Client <-> Mgr., Verschlüsselung bei Payloadverbindung	Eingeschränkte Zugriff von Comwin auf ADP Assi. V6R2 & V7	mpcid-basierte Connect zu Assi. V6R2 & V7	mpcid-basierte Connect zu Assi. V5 & V6R1
	Klartext	Klartext		SSL	proprietär
			x	SSL	
x	Klartext	SSL		SSL	
			x	SSL	

Siehe auch

Verbindung zur Remote-Datenbank

Authentifizierungsmodus

Gateway-Sicherheit

TLS-Protokollauswahl

2.14.2 Verbindung zur Remote-Datenbank

In diesem Bereich der Seite **Sicherheitsmoduskonfiguration** können Sie den nicht verschlüsselten ODBC/JDBC-Fernzugriff auf das System aktivieren bzw. deaktivieren. Bei Änderungen an dieser Konfiguration werden Webserver und OpenScape 4000-Dämonen neu gestartet.

Datenbankverbindung aktivieren/deaktivieren

So aktivieren/deaktivieren Sie unverschlüsselte Datenbankverbindungen:

- Aktivieren bzw. deaktivieren Sie das Kontrollkästchen für den gewünschten Datenbanktyp.
- Klicken Sie auf **Änderungen speichern**.

Siehe auch

Anwendungszugriff

Verbindung zur Remote-Datenbank

Authentifizierungsmodus

Gateway-Sicherheit

TLS-Protokollauswahl

2.14.3 Authentifizierungsmodus

In diesem Bereich der Seite **Sicherheitsmoduskonfiguration** können Sie die PKI-Authentifizierung und die Kerberos-Authentifizierung des Systems steuern.

Die detaillierte Konfiguration der PKI-Authentifizierung erfolgt unter Konfiguration der PKI-Authentifizierung.

PKI-Authentifizierungsmodus aktivieren/deaktivieren

So aktivieren bzw. deaktivieren Sie die PKI-Authentifizierung:

- Wählen Sie einen der folgenden Authentifizierungsmodi aus:
  - **Nur Passwort-Authentifizierung**
  - **Nur PKI-Authentifizierung**
  - **Passwort- und PKI-Authentifizierung**
- Klicken Sie auf **Änderungen speichern**.

WARNING: Aktivieren Sie während des System-Setups beide Authentifizierungsmodi, um Probleme bei der Authentifizierung zu vermeiden. Der Zugriff auf das System wird gesperrt, wenn die Konfiguration nicht ordnungsgemäß durchgeführt wurde und nur die PKI-Authentifizierung aktiviert ist.

Kerberos-Authentifizierung aktivieren

So aktivieren Sie die Kerberos-Authentifizierung:

- Aktivieren Sie das entsprechende Kontrollkästchen
- Klicken Sie auf **Änderungen speichern**.

Einzelheiten zur Kerberos-Authentifizierung finden Sie im Chapter 2.16, "Single Sign-On (SSO)".

Siehe auch

Anwendungszugriff

Verbindung zur Remote-Datenbank

Authentifizierungsmodus

Gateway-Sicherheit

TLS-Protokollauswahl

2.14.4 Gateway-Sicherheit

In diesem Bereich der Seite **Sicherheitsmoduskonfiguration** können Sie alle Gateways in den sicheren Modus umschalten.

Durch Aktivierung des Kontrollkästchens "Gateway - Sicheren Modus aktivieren" wird der HTTPS-, SSH- und DLS-Zugriff für IP-Gateways deaktiviert.

- Wenn die IP-Gateways keine Klartext-Protokolle verwenden sollen, muss zusätzlich das Leistungsmerkmal Signaling Payload Encryption (SPE) konfiguriert werden.

- Für Standalone Simplex SoftGate und Survivable SoftGate muss unter "Anwendungszugriff" auch die Option "Eingeschränkter Zugriff auf das Portal der Plattform" aktiviert werden.

So aktivieren bzw. deaktivieren Sie den sicheren Gateway-Modus:

- Aktivieren oder deaktivieren Sie die Option **Gateway** - Sicheren Modus aktivieren.
- Klicken Sie auf **Änderungen speichern**.

Siehe auch

Anwendungszugriff

Verbindung zur Remote-Datenbank

Authentifizierungsmodus

Gateway-Sicherheit

TLS-Protokollauswahl

2.14.5 TLS-Protokollauswahl

In diesem Bereich der Seite **Sicherheitsmoduskonfiguration** können Sie das Protokoll für die HTTPS-Kommunikation mit dem Webserver auswählen.

Die Standardkonfiguration des Webservers in V10 ermöglicht die Kommunikation in TLSv1.3 mit Fallback auf TLSv1.2.

Nur auf dem Assistant:

Die gleiche Konfiguration der TLS-Protokolle wird automatisch auf der Plattform und in CSTA eingestellt. Bei einer Konfigurationsänderung werden Plattform und CSTA mit der vom Assistant verwendeten Konfiguration automatisch neu konfiguriert.

Verfügbare Protokolle:

- In Openscape 4000 V10 wird TLSv1.0 nicht mehr angeboten. Die einzige in Assistant verfügbare Option wird TLSv1.3 mit Fallback auf TLSv1.2 sein.

Bei Änderungen an dieser Konfiguration werden Webserver und OpenScape 4000-Dämonen neu gestartet.

Siehe auch

Anwendungszugriff

Verbindung zur Remote-Datenbank

Authentifizierungsmodus

Gateway-Sicherheit

TLS-Protokollauswahl

2.15 Konfiguration der PKI-Authentifizierung

Übersicht

Die Konfigurierung der PKI-Authentifizierung ist die zentrale Anwendung zum Konfigurieren der PKI-Authentifizierung und der Validierungsmethode.

Starten Sie die Applikation.

Die Seite **Konfiguration** zum Konfigurieren des PKI-Authentifizierung kann von der Startseite aus aufgerufen werden:

Kennungsverwaltung -> Konfiguration der PKI-Authentifizierung

Mithilfe der **Konfiguration der PKI-Authentifizierung** können die folgenden Aktionen konfiguriert werden:

- Importieren des Vertrauensanker-(Root-CA-)Zertifikats
- Importieren/Löschen von Zwischen-CA-Zertifikaten
- Anzeigen der Beschreibung aller importierten Zertifikate
- Herunterladen aller importierten Zertifikate
- Umschalten zwischen CRL- und OCSP-Zertifikatssperrverwaltung. Zu jedem beliebigen Zeitpunkt ist immer nur ein Szenario aktiv.

Der auf Zertifikatssperrliste (CRL) basierende Sperrmodus ist immer aktiv. Zusätzlich kann der auf dem Online Certificate Status Protocol (OCSP) basierende Sperrmodus aktiviert werden.

Die Gültigkeit aller importierten Zertifikate wird überprüft. Vor Ablauf des Zertifikats wird der Administrator über den bevorstehenden Ablauf der Gültigkeit benachrichtigt und eine entsprechende Alarmmeldung ausgegeben.

Funktionalitäten

Die Seite **Konfiguration** zur Konfiguration der PKI-Einstellungen ist in folgende Hauptbereiche untergliedert:

Zertifikatsvalidierung

OCSP - Online Certificate Status Protocol-Verwaltung

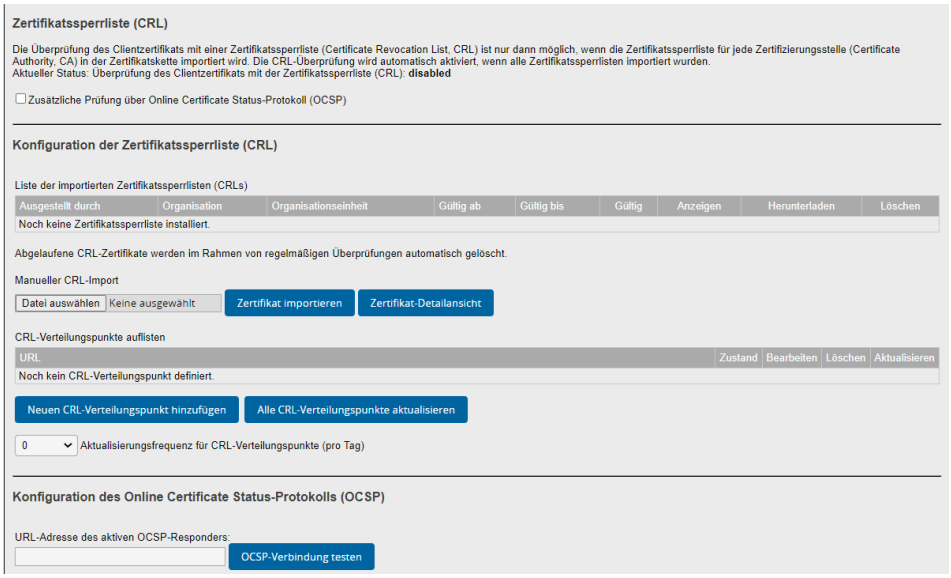
Verwaltung der Zertifikatssperrliste

Verbindungstest mit aktuellem PKI-Zertifikat

2.15.1 Zertifikatsvalidierung

Für TLS-Sitzungen verwendete Zertifikate müssen ordnungsgemäß überprüft (validiert) werden. Für den Inhalt der Zertifikate sowie die Zertifikate selbst muss eine Sperrstatusprüfung durchgeführt werden. Eine Sperrstatusprüfung umfasst eine oder beide der folgenden Mechanismen:

- Überprüfung des Zertifikatssperrstatus einer heruntergeladenen Zertifikatssperrliste (CRL).
- Überprüfung des Zertifikatssperrstatus mithilfe eines OCSP-Responders.



OpenScape 4000 stellt beide Mechanismen für die Zertifikatsüberprüfung zur Verfügung. Der Zertifikatsüberprüfungsmechanismus kann im Bereich **Zertifikatssperrliste (CRL)** festgelegt werden; über die Auswahl eines der Optionsfelder kann dabei immer nur ein Szenario aktiviert werden:

- **Zertifikatssperrliste (CRL)** oder
- **Online Certificate Status Protocol (OCSP)**Wenn das OCSP-Responder-Szenario aktiviert ist, wird das Zertifikat automatisch auch mit CRL überprüft.

Die Kommunikation mit dem OCSP-Responder erfolgt über die OpenSSL-API/CLI.

Die OpenSSL-Schnittstelle für Zertifikatsperrlisten (CRL) ist Teil des Web-Servers (Apache, mod_ssl). mod_ssl beinhaltet die erforderlichen Konfigurationseinstellungen für die Zertifikatssperrliste (CRL), unterstützt aber nicht das automatische Herunterladen der Zertifikatssperrliste (CRL). Das Herunterladen der Zertifikatsperrliste (CRL) erfolgt über einen zeitgesteuerten Auftrag. Das Zeitintervall für das Herunterladen der Zertifikatsperrliste (CRL) wird konfiguriert im Bereich **Konfiguration der Zertifikatssperrliste (CRL)**; siehe Verwaltung der Zertifikatssperrliste.

Siehe auch

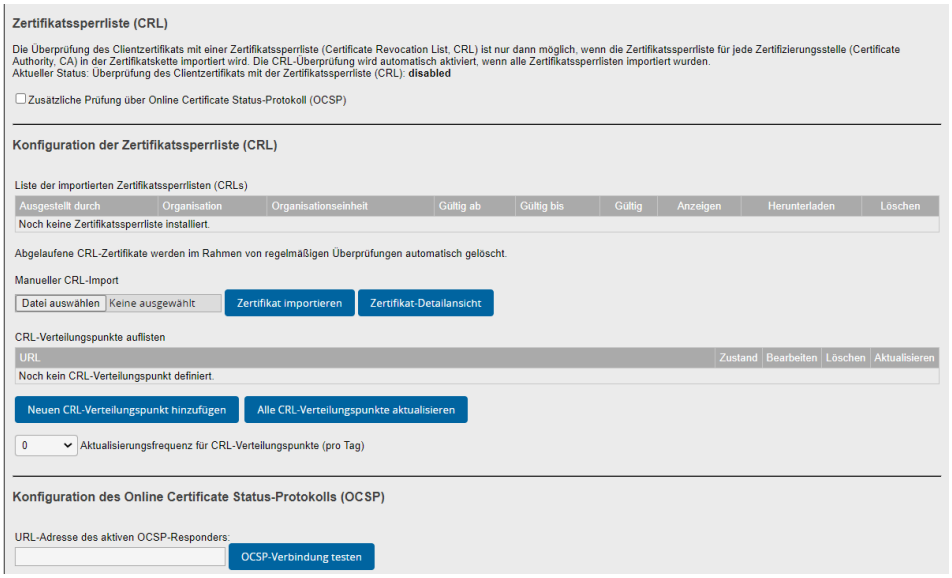
Konfiguration der PKI-Authentifizierung

2.15.2 OCSP - Online Certificate Status Protocol-Verwaltung

Die Konfiguration eines OCSP-Responders erfolgt über die Anwendung Konfiguration der PKI-Authentifizierung. Der OCSP-Responder überprüft den Sperrstatus des Clientzertifikats.

Die Verbindung zum OCSP wird anhand der folgenden Angaben hergestellt:

- Vorkonfigurierte Adresse des OCSP-Responders
- (optional) OCSP-Responder-Standort, ausgewiesen im OCSP-Feld der AIA (Authority Information Access)-Erweiterung des Zertifikats



Wenn beide Angaben vorliegen, kann über die OpenScape 4000 konfiguriert werden, welche der beiden Angaben Vorrang haben soll.

Im OCSP-Verwaltungsbereich der Anwendung Konfiguration der PKI-Authentifizierung können folgende Einstellungen konfiguriert werden:

- die IP-Adresse oder FQDN des OCSP-Responders
- die IP-Adresse oder FQDN des OCSP-Responders wird dem OCSP-Feld der AIA-Erweiterung des Root CA-Zertifikats (falls vorhanden) entnommen
- der bevorzugte OCSP-Responder-Server
- die Standardaktion für den Sitzungsaufbau, wenn der OCSP-Responder nicht reagiert (Sitzungsanforderung annehmen/ablehnen)
- die Standardaktion für den Sitzungaufbau, wenn das Clientzertifikat dem OCSP-Responder nicht bekannt ist

Beim Aufbau der SSL/TLS-Verbindung überprüft das OpenScape 4000-System das Clientzertifikat durch Senden einer Validierungsmeldung an den Online-OCSP-Responder. Wenn der OCSP-Responder nicht innerhalb eines vorgegebenen Zeitraums antwortet, wird die SSL/TLS-Sitzung konfigurationsabhängig entweder akzeptiert oder abgelehnt

Dabei werden folgende Alarm-/Protokollmeldungen generiert:

- Der OCSP-Responder ist aufgrund von Netzwerkproblemen nicht erreichbar.
- Bei der Bearbeitung der OCSP-Anforderung gab es eine Zeitüberschreitung.
- Das OCSP-Antwortformat ist ungültig.

Siehe auch

Zertifikatsvalidierung

Verwaltung der Zertifikatssperrliste

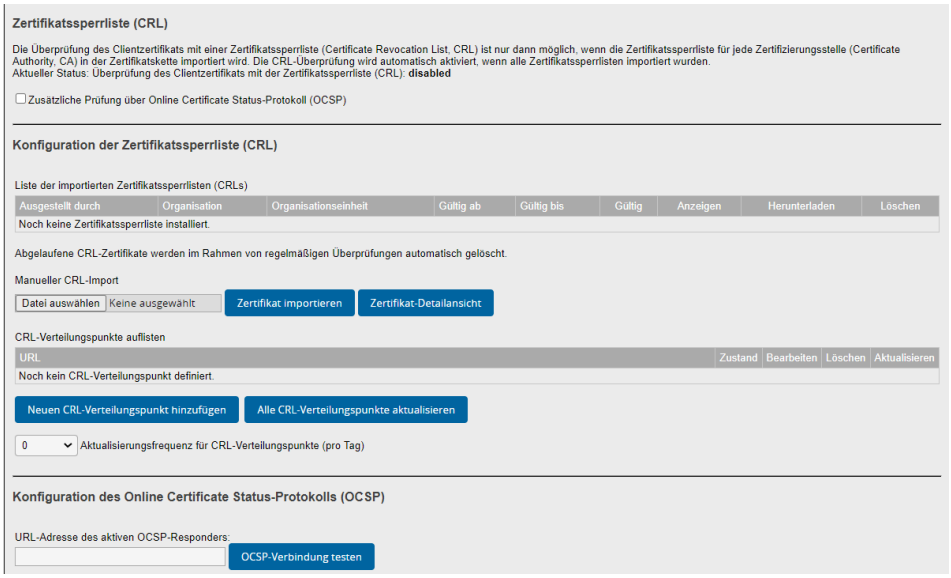
Konfiguration der PKI-Authentifizierung

Verbindungstest mit aktuellem PKI-Zertifikat

2.15.3 Verwaltung der Zertifikatssperrliste

Die Konfiguration von Zertifikatssperrlisten (Certificate Revocation Lists, CRL) erfolgt über die Anwendung Konfiguration der PKI-Authentifizierung. Die Anwendung lädt die Listen auf Anfrage herunter und hält sie auf dem neuesten Stand.

Die Anwendung Konfiguration der PKI-Authentifizierung akzeptiert nur CRL-Download-Anforderungen für Zertifikate, deren Zertifikatskette auf eine bestimmte (vorkonfigurierte) Stammzertifizierungsstelle (Root CA) hinweisen.



Der Bereich **Konfiguration der Zertifikatssperrliste (CRL)** gliedert sich in folgende Unterbereiche:

- Importierte/heruntergeladene Zertifikatssperrlisten (CRLs)
- Manueller Import von CRL-Zertifikaten
- Anzeigen/Löschen von CRL-Zertifikaten
- Konfiguration der IP-Adresse oder FQDN des OCSP-Responders
- Ermittlung der IP-Adresse oder des FQDN des CRL-Servers anhand der installierten Zertifikate (falls vorhanden)
- **Download-Intervall für Zertifikatssperrliste (CRL)**: Dropdown-Liste zur Angabe der maximalen Anzahl automatischer CRL-Downloads pro Tag. Wenn dieses Intervall auf 0 gesetzt ist, wird die Zertifikatssperrliste nicht automatisch heruntergeladen.

- Schaltfläche **Aktuelle CRL herunterladen**, zum Herunterladen der aktuellen CRL-Version.

Jedes Mal, wenn eine Zertifikatsperrliste (CRL) heruntergeladen wird, deren 'CRL-Nummer' von der 'CRL-Nummer' der vorhergehenden Zertifikatsperrliste (CRL) abweicht, werden alle Sicherheitsverwaltungssitzungen auf eine mögliche Änderung des Sperrstatus hin überprüft.

Siehe auch

Konfiguration der PKI-Authentifizierung

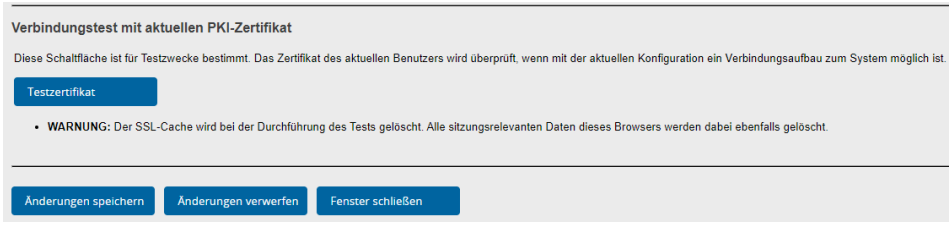
OCSP - Online Certificate Status Protocol-Verwaltung

Zertifikatsvalidierung

Verbindungstest mit aktuellem PKI-Zertifikat

2.15.4 Verbindungstest mit aktuellem PKI-Zertifikat

Durch einen Klick auf die Schaltfläche **Testzertifikat** kann das Zertifikat des gerade aktiven Benutzers getestet werden, sofern mit der aktuellen Konfiguration eine Verbindung zum System möglich ist.



WARNING: Der SSL-Cache wird gelöscht und alle sitzungsrelevanten Daten dieses Browsers werden während des Tests ebenfalls gelöscht!

Siehe auch

Konfiguration der PKI-Authentifizierung

OCSP - Online Certificate Status Protocol-Verwaltung

Zertifikatsvalidierung

Verwaltung der Zertifikatssperrliste

2.16 Single Sign-On (SSO)

Einführung

OpenScape 4000 Manager oder Assistant unterstützen "Single Sign-On" für Active Directory. Über diese Funktion können sich authentifizierte Domänenbenutzer nahtlos mit einem einzigen Klick am OpenScape 4000 Manager oder Assistant anmelden. Die Authentifizierung basiert auf Kerberos-Anmeldeinformationen (Authentifizierungstoken), die automatisch vom Client-Webbrowser bereitgestellt werden.

Die Authentifizierung ist möglich für ein Kerberos-Konto, das einem vorhandenen OpenScape 4000-Benutzerkonto zugeordnet ist (unter Zugangsverwaltung - Benutzerkennungsverwaltung).

Schema der Authentifizierung

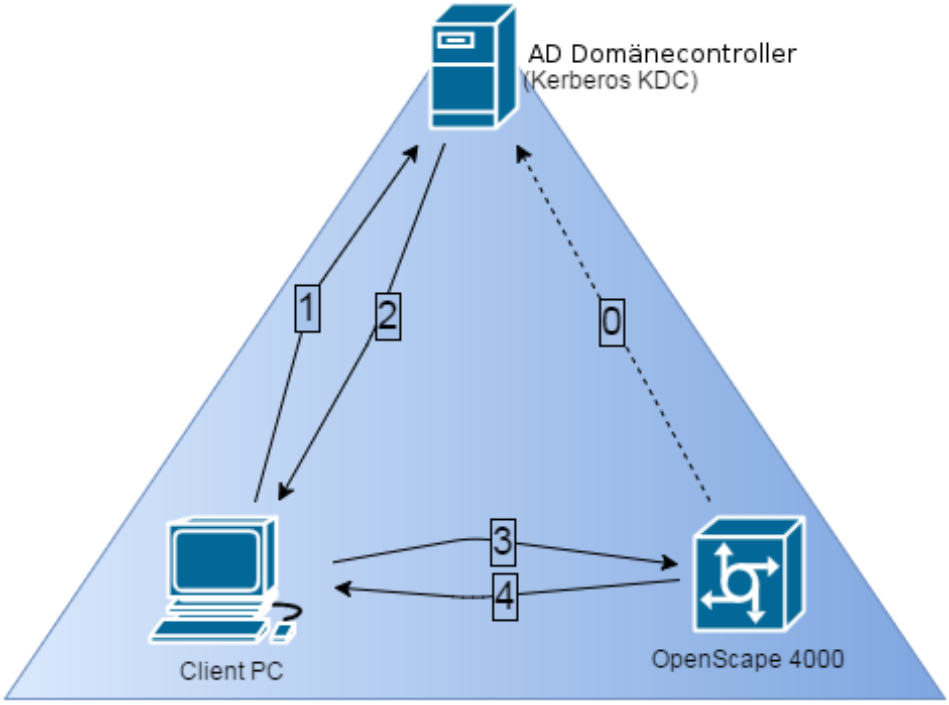


Figure 12: Schema der Kerberos-Authentifizierung

Schritt 0: Periodischer Abruf des Kerberos Ticket-Granting Tickets (TGT)

Schritt 1: Der Benutzer meldet sich auf dem Client-PC an der Domäne an.

Schritt 2: Das Kerberos-Schlüsselverteilungscenter (Key Distribution Center, KDC) überprüft die Anmeldeinformationen des Benutzers, authentifiziert den Benutzer und sendet ein Ticket-Granting Ticket (TGT) an den Client-PC.

Schritt 3: Der Benutzer stellt eine Verbindung zum OpenScape 4000-System her und verwendet dabei die Kerberos-Authentifizierungsoption. Die Kerberos-Anmeldeinformationen (Kerberos-Dienstticket) werden automatisch vom Browser bereitgestellt.

Schritt 4: Wenn die Kerberos-Anmeldeinformationen korrekt sind und das Domänenkonto des Benutzers einem OpenScape 4000-Benutzerkonto zugeordnet ist, authentifiziert das OpenScape 4000-System den Benutzer und erstellt ein Sitzungscookie.

NOTICE: Schritt 0, 3 und 4 erfordern eine Konfiguration des OpenScape 4000-Systems und des Domänencontrollers.

2.16.1 Voraussetzungen

- OpenScape 4000 Assistant/Manager V8 und höher
- Client-PC mit Windows-Domänenkonto

- Server-Betriebssystem mit Domänencontroller (DC) mit Active Directory (AD), Kerberos-Server (KDC) und DNS-Server-Funktionalität

Liste unterstützter Client-Betriebssysteme

- Windows XP und höher als Client-Betriebssystem

> **NOTICE:** Alternativ kann auch Windows Server OS als Client-Betriebssystem verwendet werden.

Liste unterstützter Server-Betriebssysteme

Unterstützt werden alle Server mit Windows-basiertem Serversystem:

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

2.16.2 OpenScape 4000-Konfiguration

Die globale Kerberos-Konfiguration für SLES auf dem OpenScape 4000-System wird nicht beeinträchtigt. Für die Authentifizierung auf OpenScape 4000 werden eigene Konfigurationsdateien verwendet.

2.16.2.1 Aktivierung der Kerberos-Authentifizierung

Die Kerberos-Konfigurationsapplikation kann über den Ordner Zugangsverwaltung aufgerufen werden (Figure 3).

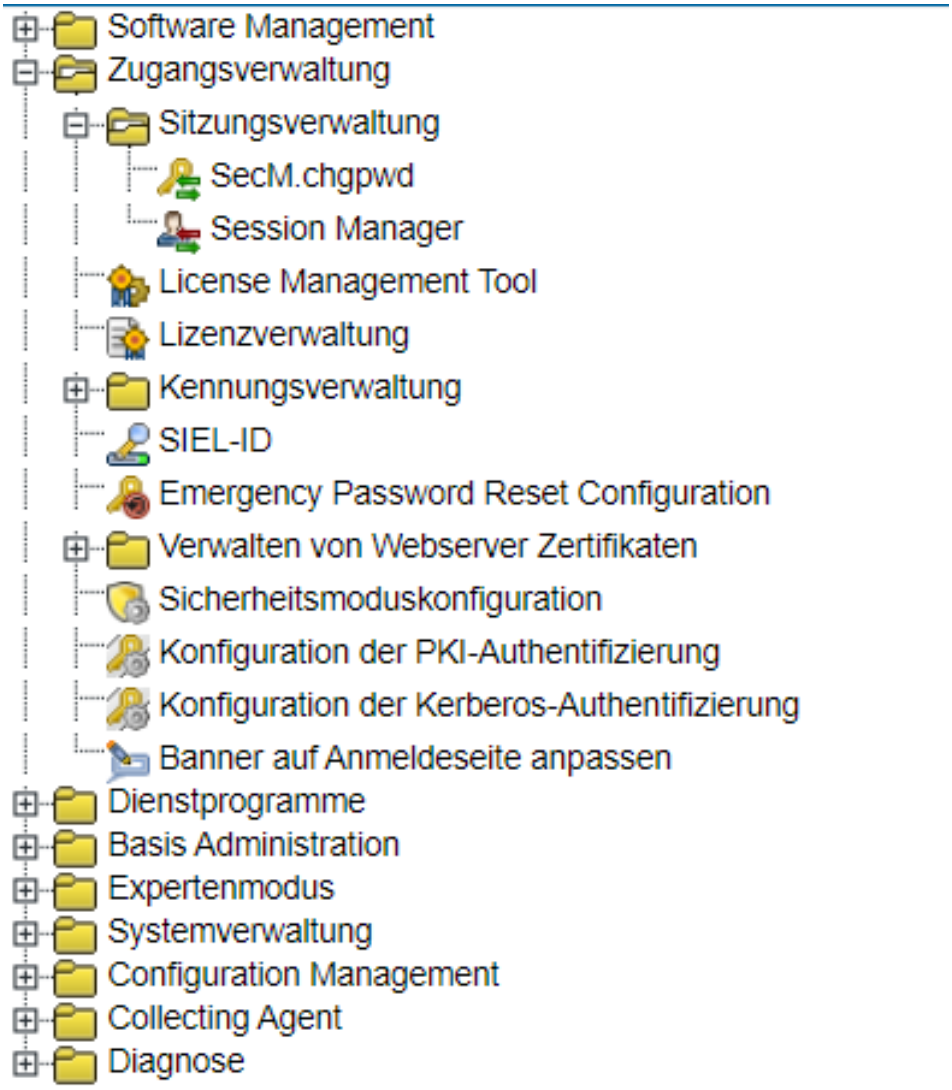


Figure 13: Zugriff auf "Konfiguration der Kerberos-Authentifizierung"

Die Kerberos-Authentifizierung ist nach der Installation von OpenScape 4000 **standardmäßig deaktiviert** (siehe Meldung in Figure 4). Daher müssen Sie die Authentifizierung zunächst aktivieren. Klicken Sie in der Meldung auf den Link Sicherheitsmoduskonfiguration, um die Applikation Sicherheitsmoduskonfiguration aufzurufen.

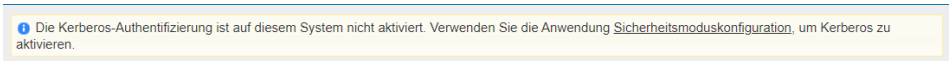


Figure 14: Standard-Kerberos-Authentifizierungsmeldung

Suchen Sie in der Applikation Sicherheitsmoduskonfiguration nach dem Bereich Authentifizierungsmodus und aktivieren Sie dort das Kontrollkästchen "Kerberos-Authentifizierung aktivieren" (Figure 5). Klicken Sie auf die Schaltfläche "**Änderungen speichern**", um die Einstellungen zu speichern.

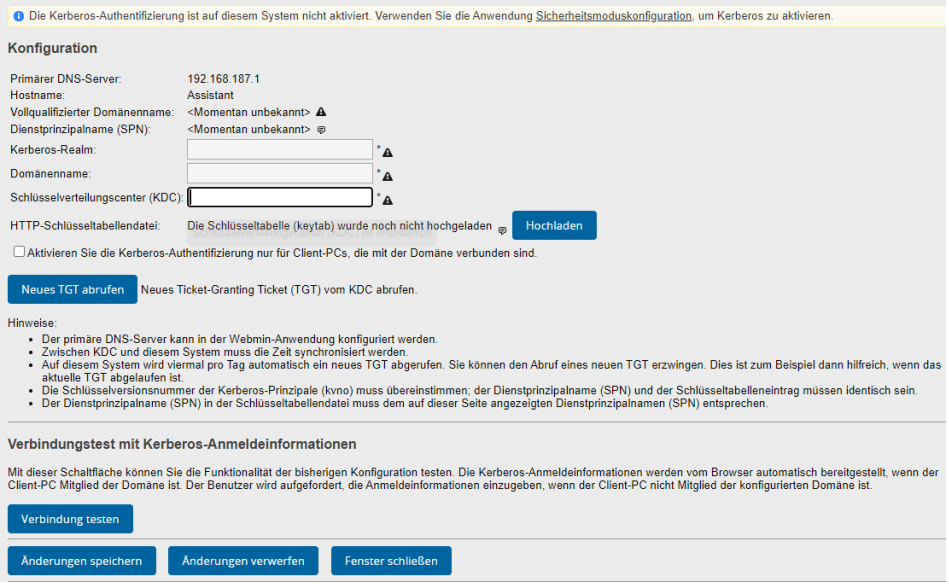


Figure 15: Kontrollkästchen "Kerberos-Authentifizierung aktivieren"

2.16.2.2 Konfiguration der Kerberos-Authentifizierung

Voraussetzungen

Das Linux-Paket **krb5-client** muss unter SLES installiert sein. Dieses Paket ist auf dem Assistant bereits vorinstalliert. Auf dem Manager muss es manuell nachinstalliert werden. Der Benutzer erhält eine Aufforderung zu Installation (Figure 6).

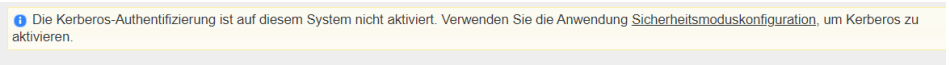


Figure 16: Meldung zur krb5-client-Paketinstallation

Außerdem muss die **Kerberos-Authentifizierung** in der Applikation Sicherheitsmoduskonfiguration **aktiviert** sein (siehe Chapter 2.16.2.1, "Aktivierung der Kerberos-Authentifizierung").

Konfigurationselemente

Die folgenden Elemente müssen konfiguriert werden (Figure 7):

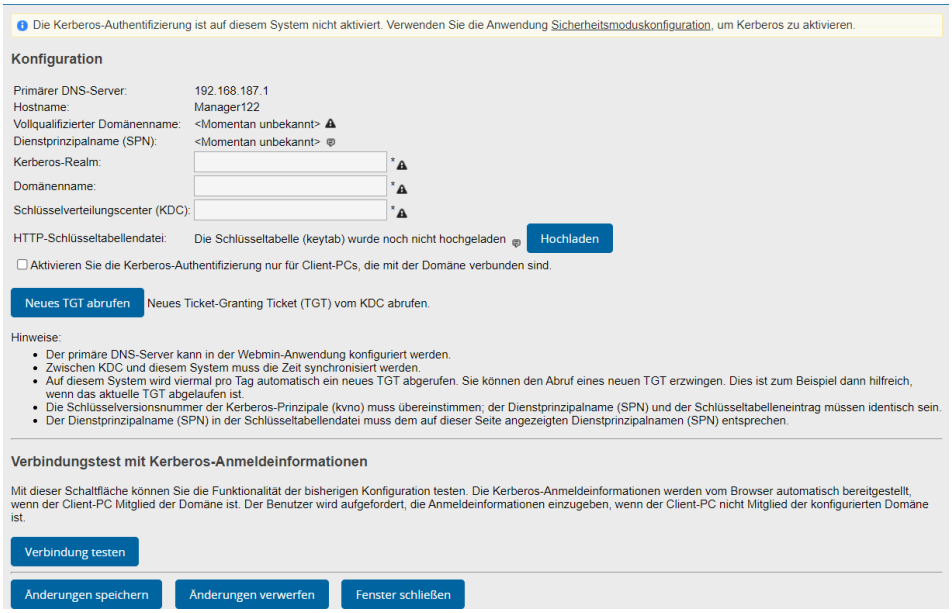


Figure 17: Fenster "Konfiguration der Kerberos-Authentifizierung"

- Der **primäre DNS-Server** kann in der Webmin-Anwendung konfiguriert werden. Empfohlen wird die Angabe eines DNS-Servers, der auf einem Windows-Domänencontroller läuft.
- Der **Hostname** des aktuellen Systems kann in der Webmin-Anwendung konfiguriert werden.
- Der **vollqualifizierte Domänenname (FQDN)** besteht aus einem Hostnamen und einem Domänennamen. Da der Domänenname noch konfiguriert werden muss, ist der vollständige FQDN nach der Installation zunächst unbekannt.
- Der **Dienstprinzipalname (SPN)** ist ein Bezeichner für einen von einem bestimmten Host innerhalb einer Authentifizierungsdomäne angebotenen Dienst. Allgemeiner Wert: *<service>/<FQDN>@<REALM>* (Beispiel: HTTP/mgr-V8.os4k-kerb.com@OS4K-KERB.COM).
- Der SPN muss im Schlüsselverteilungscenter(KDC) des REALMs registriert sein. Der Dienstprinzipalname wird nach Eingabe der erforderlichen Parameter automatisch ermittelt.
- **Kerberos-Realm**. In der Windows-Umgebung entspricht das Kerberos-Realm einer Windows-Domäne in Großbuchstaben, z. B.: OS4K-KERB:COM;
- **Domänenname** der Windows-Domäne, z.B. os4k-kerb.com.
- Das **Schlüsselverteilungscenter (KDC)** ist ein Dienst, der auf allen Domänencontrollern läuft und Authentifizierungsdienste für Clients, Server und Dienste bereitstellt.

  Der Wert ist: dc.*<Name des Domänencontrollers>* (z.B. dc.os4k-kerb.com).
- **HTTP-Schlüsseltabellendatei** enthält den gemeinsamen geheimen Schlüssel des SPN. Diese Datei wird mit dem ktpass-Tool auf Domänencontroller erstellt. Die Schlüsseltabellendatei muss vom Domänencontroller zu OpenScape 4000 übertragen und dort geladen werden (siehe Dienstkonto für das OpenScape 4000-System auf page 231).
- Kontrollkästchen **Aktivieren Sie die Kerberos-Authentifizierung nur für Client-PCs, die mit der Domäne** verbunden sind: Bei Auswahl dieser

Option wird die Standardauthentifizierung deaktiviert (siehe Chapter 2.16.5, "Authentifizierungsszenario").

Hinweis: Die Standardauthentifizierung erfolgt (über ein Dialogfenster mit Eingabeoptionen für den Benutzernamen und das Passwort der Domäne), wenn der Client-PC NICHT mit der Domäne verbunden ist.

Wenn der Client-PC mit der Domäne verbunden ist, werden die Kerberos-Anmeldeinformationen des Benutzers beim Authentifizierungsversuch automatisch vom Browser bereitgestellt (Aushandlungsauthentifizierung).

- Über die Schaltfläche **Neues TGT abrufen** (Ticket-Granting Ticket) können Sie die aktuelle Version des Tickets für OpenScape 4000 herunterladen. Verwenden Sie diese Funktion, nachdem die Kerberos-Konfiguration abgeschlossen ist.

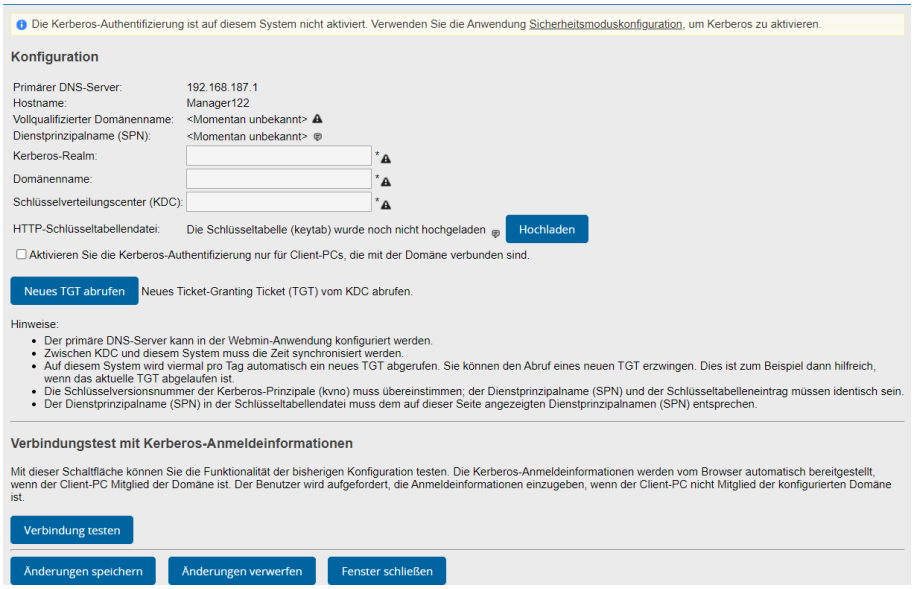


Figure 18: Beispiel: Konfiguration der Kerberos-Authentifizierung

Jede Änderung des Kerberos-Realms, des Domänennamens, des Schlüsselverteilungscenters (KDC) oder der Schlüsseltabellendatei erfordert einen Neustart des Webservers, damit die Änderungen wirksam werden. Durch Klicken auf die Schaltfläche "Webserver neu starten" kann der Webserver neu gestartet werden; die Schaltfläche ist nur verfügbar, wenn ein Neustart erforderlich ist.

Konfigurationstest

Mit der Schaltfläche **Verbindung testen** können Sie überprüfen, ob die Konfigurationseinstellungen korrekt sind. Ist dies der Fall, erscheint ein Popup-Fenster mit dem Kerberos-Kontonamen des aktuellen Benutzers (Figure 8).

2.16.2.3 Zuordnung des Kerberos-Kontos zu einem OpenScape 4000-Konto

Die Liste der OpenScape 4000-Benutzerkonten finden Sie in der Applikation **Benutzerkennungsverwaltung**. Sie können das Kerberos-Konto jedem beliebigen OpenScape 4000-Benutzerkonto zuweisen. Dies ist möglich entweder während der Kontoerstellung (Figure 8, durchgezogen umrandete

Optionen) oder später über den rechten Konfigurationsbereich des Fensters Benutzerkennungsverwaltung (Figure 8, gestrichelt umrandete Optionen).

Es kann jeweils nur ein Kerberos-Konto einem OpenScape 4000-Konto zugewiesen werden.

NOTICE: Die Zuweisung eines Kerberos-Kontos zu OpenScape 4000-**Systemkonten** ist **NICHT** möglich.

Das allgemeine Format eines Kerberos-Kontos lautet:
<Benutzername>@<REALM>

2.16.3 Das allgemeine Format eines Kerberos-Kontos lautet: <Benutzername>@<REALM>Active Directory-Domänencontroller und Kerberos-Schlüsselverteilungscenter (KDC)-Konfiguration

Der Domänencontroller läuft auf einem Windows Server-Betriebssystem.

DNS-Server

1) DNS-Manager öffnen.
2) OpenScape 4000-Datensatz zum DNS hinzufügen:

   DNS --> Forward-Lookupzonen --> Ihre Zone --> Neuer Host mit OpenScape 4000-Datensatz. Option "Verknüpften Datensatz vom Typ 'Pointer' erstellen" aktivieren.
3) Überprüfen, ob der Reverse-Datensatz für das OpenScape-4000 System erstellt wurde:

   DNS --> Reverse-Lookup-Zonen--> Ihre Zone --> PTR mit OpenScape 4000-Datensatz

Dienstkonto für das OpenScape 4000-System

Für jedes OpenScape 4000-System ist ein Dienstkonto erforderlich.

1) "Active Directory-Benutzer und -Computer" öffnen.
2) Erstellen Sie ein Dienstkonto in der Domäne (<BENUTZERNAME>). Dieses Konto wird für die Zuordnung des Dienstprinzipalnamens (SPN) zum Domänenkonto verwendet. Nach der Erstellung des Kontos und Ausführung von ktpass im nächsten Schritt erscheint unter Benutzereigenschaften eine neue Registerkarte mit der Bezeichnung "Stellvertretung" (Delegierung).
3) Generieren Sie die Schlüsseltabellendatei mit der Konfiguration des SPN für das OpenScape 4000-System und mit dem gemeinsamen geheimen Schlüssel des SPN. Die Schlüsseltabellendatei muss in CMD auf einem Server in der Domäne erstellt werden. Als <BENUTZERNAME> sollte das im vorherigen Schritt erstellte Dienstkonto gewählt werden.

   Mithilfe des ktpass-Befehlszeilenprogramms können nicht-Windows-Dienste, die die Kerberos-Authentifizierung unterstützen, die vom Kerberos-Schlüsselverteilungscenter (KDC) auf dem Windows-Server bereitgestellten Interoperabilitätsfunktionen verwenden.

   Allgemeines Format:
   ```
   ktpass -princ <SPN> -mapuser <Benutzername>@<REALM> -
   crypto
   ```

```
all -ptype KRB5_NT_PRINCIPAL -pass <PASSWORT> -out
http.keytab
```

Beispiel:

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

NOTICE: Der Benutzer speichert die sog. Schlüsselversionsnummer (Key Version Number, kvno). Wenn die Schlüsseltabellendatei neu erstellt wird, muss die neue Datei zum OpenScape 4000-System hochgeladen werden. Die in der Schlüsseltabellendatei gespeicherte kvno muss mit der kvno in OpenScape 4000 übereinstimmen.

Hinweise:

- Der dem Dienstkonto zugeordnete Dienstprinzipalname (SPN) kann wie folgt abgefragt werden:
  ```
  setspn <BENUTZERNAME>
  ```
  setspn – liest, ändert und löscht die SPN-Verzeichnis-Eigenschaft für ein Active Directory (AD)-Dienstkonto.
- Zuordnung des SPN zu einem AD-Dienstkonto:
  ```
  setspn -A <SPN> <BENUTZERNAME>
  ```
  Beispiel:
  ```
  setspn -A HTTP/mgr-V8.os4k-kerb.com@OS4K-KERB.COM
  <BENUTZERNAME>
  ```
- Wenn der gleiche Datensatz bereits existiert, z.B. für ein anderes Dienstkonto, erhalten Sie eine doppelte Meldung. Sie können die Zuordnung mit folgendem Befehl löschen:
  ```
  setspn -D <SPN> <ALTER_BENUTZERNAME>
  ```

2.16.4 Clientkonfiguration

Betriebssystemkonfiguration

Bevorzugte Methode für die Kerberos-Authentifizierung ist ein Client-PC-Zugriff mit folgenden Optionen:

- Der Client-PC ist an der Domäne angemeldet
- Der Client-PC ist so konfiguriert, dass er den DNS-Server auf dem Domänencontroller verwendet

Browserkonfiguration

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Im Browser ist unter Internetoptionen --> Erweitert die Option "**Integrierte Windows-Authentifizierung**" aktiviert.
- Der Zugriff auf das OpenScape 4000-System erfolgt im Browser über den **Hostnamen** (z. B. mgr-v8) oder über den **FQDN** (z. B.mgr-v8.os4k-kerb.com). Der Hostname des OpenScape 4000-Systems wird in der Webmin-Anwendung angegeben. Der entsprechende DNS-Eintrag muss auf dem DNS-Server eingerichtet werden.

- Stellen Sie sicher, dass der Browserzugriff auf das OpenScape 4000-System **über die lokale Intranetzone** erfolgt. Die Liste der Intranet-Systeme kann im Browser unter Internetoptionen --> Sicherheit konfiguriert werden. In der Regel werden sie vom Administrator vordefiniert.

2.16.5 Authentifizierungsszenario

Auf der Anmeldeseite des OpenScape 4000-Systems ist der Bereich Single Sign On mit der Schaltfläche "Anmelden" hinzugekommen. Das Authentifizierungstoken, das den Domänenbenutzer identifiziert, wird auf dem OpenScape 4000-System automatisch vom Browser bereitgestellt, wenn der Client-PC mit der Domäne verbunden ist (**Aushandlungsauthentifizierung**).

Wenn der Client-PC NICHT mit der Domäne verbunden ist, erscheint das Fenster **Standardauthentifizierung**. Der Benutzer muss seine Anmeldeinformationen (Domänenbenutzername und -passwort) eingeben, um mit der Kerberos-Anmeldung fortzufahren.

NOTICE: Die Standard-Kerberos-Authentifizierung kann auf der Konfigurationsseite **deaktiviert** werden (siehe Chapter 2.16.2.2, "Konfiguration der Kerberos-Authentifizierung").

Der Benutzer wird über das Ergebnis der Authentifizierung informiert und automatisch auf die Hauptseite des OpenScape 4000-Systems umgeleitet.

NOTICE: Sollte eine Passwortänderung erforderlich sein, wird der Benutzer mit folgender Meldung darüber benachrichtigt: "*Ihr Passwort ist abgelaufen. Melden Sie sich mit dem Benutzernamen/Passwort am System an und ändern Sie Ihr Passwort.*"

2.17 Banner auf Anmeldeseite anpassen

Übersicht

Die Anmeldeseite des OpenScape 4000-Systems kann an die Bedürfnisse unterschiedlicher Benutzer angepasst werden. Benutzerspezifische Informationen sind zum Beispiel Banner mit Warnmeldungen, Einschränkungshinweise, Systemnachrichten, kundenspezifische Details.

Der benutzerdefinierte Text wird im oberen Teil der Seite vor der Anmeldemaske angezeigt. Der Anmeldeprozess kann so konfiguriert werden, dass der Benutzer nur bei Zustimmung zu dieser Meldung mit der Anmeldung fortfahren kann.

Durch Anzeige einer entsprechenden Warnmeldung vor dem eigentlichen Benutzeranmeldedialog könnte zum Beispiel die rechtliche Grundlage für eine Strafverfolgung bei rechtswidrigem Zugang zum Computersystem gelegt werden.

Starten Sie die Applikation.

Benutzer mit der Sicherheitsstufe "engr" können die Seite **Konfiguration** für das Anpassen des Anmeldeseitentextes von der Startseite aus aufrufen:

Kennungsverwaltung -> Banner auf Anmeldeseite anpassen

Anmelde-Text anpassen

Im Textfeld **Aktueller Bannerinhalt** wird der aktuelle Anmelde-Text angezeigt.

So können Sie den Anmelde-Text anpassen:

- Markieren Sie das Kontrollkästchen **Banner auf Anmeldeseite anzeigen**.
- Markieren Sie das Kontrollkästchen **Der Benutzer muss die Meldung auf dem Banner akzeptieren, um mit der Anmeldung fortfahren zu können**, um zu erreichen, dass der Benutzer nur dann mit der Anmeldung fortfahren kann, wenn er die Meldung akzeptiert.
- Geben Sie den Anmelde-Text in das Textfeld **Bannerinhalt ändern** ein. Der Text wird grafisch genauso dargestellt wie in diesem Feld angezeigt.
- Klicken Sie auf **Änderungen speichern** und dann auf **Fenster schließen**.

Empfehlungen für die Anpassung des Anmelde-Textes

Warnmeldungen sollten mindestens die folgenden Angaben enthalten: den Namen der Organisation, die Eigentümer des Systems ist; die Tatsache, dass das System überwacht wird und dass diese Überwachung im Einklang mit lokalen Gesetzen erfolgt; und schließlich ein Hinweis, dass durch die Benutzung des Systems dieser Überwachung implizit zugestimmt wird.

Alternativ bzw. zusätzlich dazu könnte auch ein Hinweis darauf gegeben werden, welche Nutzer berechtigt sind, das System zu benutzen, z. B. "Autorisierte Benutzer sind berechtigt, das System gemäß den für das System gültigen Nutzungsbedingungen zu benutzen."

2.18 Registerkarte "Zugangsverwaltung" in der Systemverwaltung

Die Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** ist eine Plug-In-Komponente für das **Einrichten bzw. Ändern der NSL-Passwörter für die Einzelanmeldung** bei untergeordneten OpenScape 4000-Servern. Um die NSL-Funktionalität zu nutzen, müssen die hier eingegebenen Passwörter mit den Passwörtern auf dem Zielsystem übereinstimmen. Siehe **Systemkennungsverwaltung** auf dem ausgewählten System.

Auf OpenScape 4000 Manager und RSP (Remote Service Platform) wird die Registerkarte **Zugangsverwaltung** als zusätzliches Plug-In in der Benutzeroberfläche der Applikation **Systemverwaltung** zur Verfügung gestellt.

Die Registerkarte **Zugangsverwaltung** wird nur dann in der **Systemverwaltung** angezeigt, wenn Sie einen OpenScape 4000-Server als Anlagentyp gewählt haben und wenn in der **Systemverwaltung** im Bereich **Aktive Anwendung** das Kontrollkästchen der **Zugangsverwaltung** markiert ist.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die

Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Änderungen, die Sie in der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** vornehmen, werden in der **Systemverwaltung** gespeichert.

Die Berechtigung eines Benutzers, NSL-Passwörter zu vergeben und/oder zu ändern, hängt von der Benutzerkennung und den damit verbundenen Zugriffsrechten ab.

Verwandte Themen

Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.18.1 Registerkarte "Zugangsverwaltung" in der Systemverwaltung, Benutzeroberfläche

Die Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** ist eine Plug-In-Komponente für das Einrichten bzw. Ändern der NSL-Passwörter für die Einzelanmeldung bei untergeordneten OpenScape 4000-Servern. Um die NSL-Funktionalität zu nutzen, müssen die hier eingegebenen Passwörter mit den Passwörtern auf dem Zielsystem übereinstimmen. Siehe **Systemkennungsverwaltung** auf dem ausgewählten System.

Die Registerkarte **Zugangsverwaltung** wird nur dann in der **Systemverwaltung** angezeigt, wenn Sie einen OpenScape 4000-Server als Anlagentyp gewählt haben und wenn in der **Systemverwaltung** im Bereich **Aktive Anwendung** das Kontrollkästchen der **Zugangsverwaltung** markiert ist.

Änderungen, die Sie in der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** vornehmen, werden in der **Systemverwaltung** gespeichert.

Die Berechtigung eines Benutzers, NSL-Passwörter zu vergeben und/oder zu ändern, hängt von der Benutzerkennung und den damit verbundenen Zugriffsrechten ab. Abhängig vom Benutzerkennwort, mit dem Sie sich angemeldet haben, werden nur gleichrangige und untergeordnete Benutzerebenen (User Levels) angezeigt. Übergeordnete Benutzerebenen werden nicht angezeigt, und NSL-Passwörter höherer Ebenen können folglich auch nicht editiert werden.

Die Benutzeroberfläche der Registerkarte **Zugangsverwaltung** umfasst drei Bereiche, die das Festlegen bzw. Ändern von NSL-Passwörtern für die drei unterschiedlichen Kategorien von Benutzerkennungen ermöglichen:

- Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung" Dieser Bereich umfasst die NSL-Kennungen für Service-Administratoren.
- Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung" Dieser Bereich umfasst die NSL-Kennungen für Kunden-Administratoren.
- Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung" Dieser Bereich enthält die NSL-Kennung für Server-Server-Kommunikation.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Verwandte Themen

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.18.1.1 Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Der Bereich **Zugang für den Service** auf der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** verwaltet die NSL-Kennungen und Passwörter für Service-Administratoren.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Der Registerkartenbereich **Zugang für den Service** umfasst folgende NSL-Kennungen:

- Experte (nsl-engr)
- L2-Service (nsl-rsta)
- L1-Service (nsl-rsca)

Um für alle NSL-Kennungen im Service-Bereich ein (identisches) Passwort zu vergeben, markieren Sie das Kontrollkästchen Gleicher Wert für alle Service-Passwörter.

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Weitere Informationen zu NSL-Kennungen und -Passwörtern finden Sie unter:

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Feldbeschreibungen

engr (Bereich "Zugang für den Service")

rsta (Bereich "Zugang für den Service")

rsca (Bereich "Zugang für den Service")

Gleicher Wert für alle Service-Passwörter (Bereich "Zugang für den Service")

cusa (Bereich "Zugang für den Kunden")

cust (Bereich "Zugang für den Kunden")

Gleicher Wert für alle Kunden-Passwörter (Bereich "Zugang für den Kunden")

syst (Bereich "Systemzugang (Server-Server-Kommunikation)")

Speichern (Schaltfläche)

Verwerfen (Schaltfläche)

Neu (Schaltfläche)

Löschen (Schaltfläche)

Siehe auch

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.18.1.2 Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Der Bereich **Zugang für den Kunden** auf der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** verwaltet die NSL-Kennungen und Passwörter für Kunden-Administratoren.

Auf dem RSP wird dieser Bereich nicht angezeigt, da der NSL-Zugang für Kunden-Kennungen vom Service-Tool (RSP) aus nicht unterstützt wird.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Der Registerkartenbereich **Zugang für den Service** umfasst folgende NSL-Kennungen:

- Kundenadministrator (nsl-cusa)
- Kunde (nsl-cust)

Um für alle NSL-Kennungen im Service-Bereich ein (identisches) Passwort zu vergeben, markieren Sie das Kontrollkästchen Gleicher Wert für alle Service-Passwörter.

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Weitere Informationen zu NSL-Kennungen und -Passwörtern finden Sie unter:

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Feldbeschreibungen

engr (Bereich "Zugang für den Service")

rsta (Bereich "Zugang für den Service")

rsca (Bereich "Zugang für den Service")

Gleicher Wert für alle Service-Passwörter (Bereich "Zugang für den Service")

cusa (Bereich "Zugang für den Kunden")

cust (Bereich "Zugang für den Kunden")

Gleicher Wert für alle Kunden-Passwörter (Bereich "Zugang für den Kunden")

syst (Bereich "Systemzugang (Server-Server-Kommunikation)")

Speichern (Schaltfläche)

Verwerfen (Schaltfläche)

Neu (Schaltfläche)

Löschen (Schaltfläche)

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.18.1.3 Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Im Bereich **Systemzugang (Server-Server-Kommunikation)** auf der Registerkarte **Zugangsverwaltung** können Sie das NSL-Passwort für die Benutzerkennung für Server-Server-Kommunikation eingegeben oder ändern.

Auf dem RSP wird dieser Bereich nicht angezeigt, da der NSL-Zugang für Kunden-Kennungen vom Service-Tool (RSP) aus nicht unterstützt wird.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Der Registerkartenbereich **Systemzugang (Server-Server-Kommunikation)** enthält nur die NSL-Kennung **syst** für Server-Server-Kommunikation.

Die NSL-Kennung **syst** ist als Netzwerkeinzelanmeldung auf Systemebene für die interne Server-Server Kommunikation von OpenScape 4000 Komponenten wie z. B. Systemverwaltung, Expert Access/MPCID, Logging Management vorgesehen.

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Weitere Informationen zu NSL-Kennungen und -Passwörtern finden Sie unter:

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Feldbeschreibungen

engr (Bereich "Zugang für den Service")

rsta (Bereich "Zugang für den Service")

rsca (Bereich "Zugang für den Service")

Gleicher Wert für alle Service-Passwörter (Bereich "Zugang für den Service")

cusa (Bereich "Zugang für den Kunden")

cust (Bereich "Zugang für den Kunden")

Gleicher Wert für alle Kunden-Passwörter (Bereich "Zugang für den Kunden")

syst (Bereich "Systemzugang (Server-Server-Kommunikation)")

Speichern (Schaltfläche)

Verwerfen (Schaltfläche)

Neu (Schaltfläche)

Löschen (Schaltfläche)

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

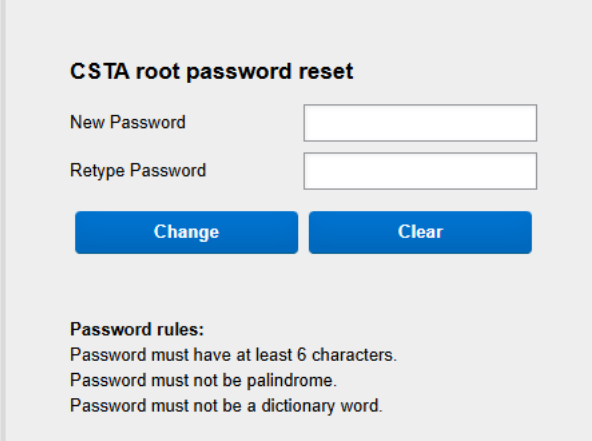
Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

2.19 CSTA-Root-Passwort-Resets

In diesem Abschnitt wird der Vorgang zum Ändern des **CSTA-Root-Passwort-Resets** beschrieben.



Tasten

Ändern	Durch Klicken auf diese Schaltfläche werden die vorgenommenen Änderungen übernommen und das neue Passwort wird für zukünftige Sitzungen gültig.
Löschen	Durch Klicken auf **Löschen** wird der Inhalt der Eingabefelder gelöscht und bleibt für neue Eingaben leer.

Passwortregeln

Die Regeln zur Eingabe gültiger Passwörter werden im CSTA-Root-Passwort-Reset-Dialog angezeigt:

- Das Passwort muss mindestens 6 Zeichen lang sein.
- Das Passwort darf kein Palindrom sein.
- Das Passwort darf kein Wörterbuchwort sein.

Feldbeschreibungen

Altes Passwort

Neues Passwort

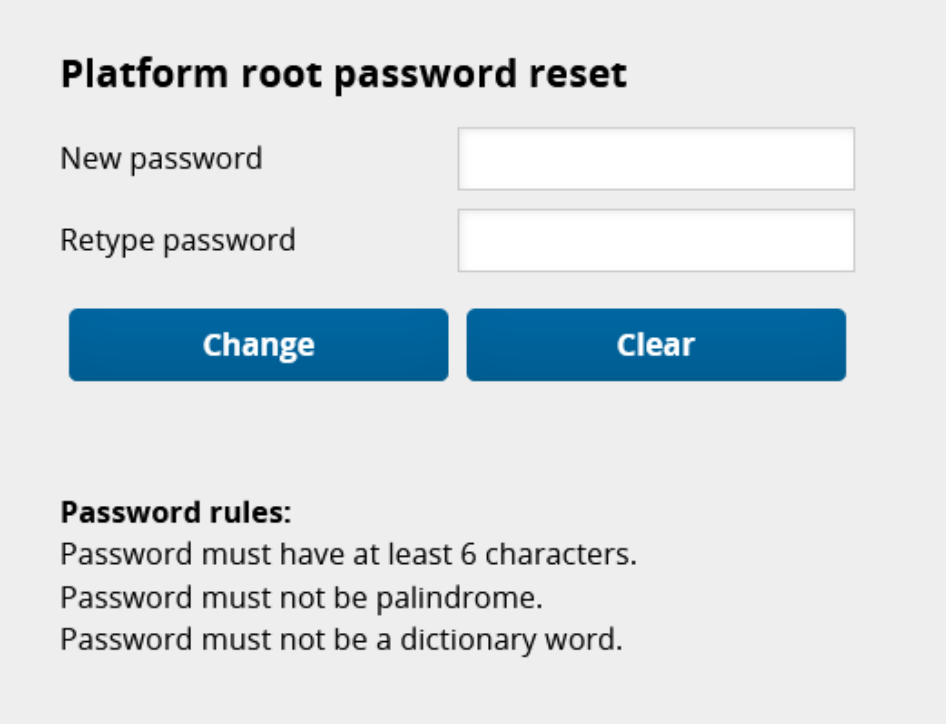
Passwort-Eingabe wiederholen

Ändern

Löschen

2.20 Plattform Root Passwort Resets

In diesem Abschnitt wird der Vorgang zum Ändern des **Plattform-Root-Passwort-Resets** beschrieben.



Tasten

Ändern	Durch Klicken auf diese Schaltfläche werden die vorgenommenen Änderungen übernommen und das neue Passwort wird für zukünftige Sitzungen gültig.
Löschen	Durch Klicken auf **Löschen** wird der Inhalt der Eingabefelder gelöscht und bleibt für neue Eingaben leer.

Passwortregeln

Die Regeln zur Eingabe gültiger Passwörter werden im CSTA-Root-Passwort-Reset-Dialog angezeigt:

- Das Passwort muss mindestens 6 Zeichen lang sein.
- Das Passwort darf kein Palindrom sein.
- Das Passwort darf kein Wörterbuchwort sein.

Feldbeschreibungen

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Ändern

Löschen

2.21 Automatisches Sperren von OpenScape 4000 Linux-Konten

Ab V11 R1 werden die wichtigsten OpenScape 4000 Linux-Konten:

- root auf Platform (jede Bereitstellung inklusive Manager)

- TRM auf STMIX und STMIY
- root auf CSTA (zentraler Host und Survivable SoftGate und Enterprise Gateway)
- `engr/rsta/rsca`
  auf Assistant und Manager

werden vorübergehend gesperrt, nachdem 5 Mal hintereinander ein falsches Passwort über SSH eingegeben wurde, um Brute-Force-Sicherheit-Angriffe über SSH zu verhindern.

Nach 5 Minuten wird das Konto automatisch wieder entsperrt.

Die Meldungen über die Sperrung finden Sie in `/var/log/messages`

Feldbeschreibungen

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Ändern Sie

Löschen

3 Zugangsverwaltung - Beschreibung der Felder

Dieser Abschnitt enthält die nach Themen sortierte Feldhilfe zur Zugangsverwaltung.

3.1 Web Session Manager - Beschreibung der Felder

Sitzungseinstellungen

Zeitüberschreitungswert für nicht aktive Sitzungen.

- **Nicht aktive Sitzungen werden nach xx Minute(n)/Stunde(n)/ Tag(en)/Woche(n)/Monat(en) automatisch ungültig.** In dem hier angezeigten Dropdown-Listenfeld können Sie den eingestellten aktuellen Zeitüberschreitungswert wählen und einstellen, nach dessen Ablauf nicht aktive Sitzungen ungültig (und damit automatisch gelöscht) werden. Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern. Wenn der Wert geändert wird, werden alle laufenden Sitzungen aller Benutzer sofort beendet; für alle danach eröffneten Sessions gilt der neue Wert.

  Werte: 15 Min. (kleinster Wert) bis 1 Monat (größter Wert).

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern.

  Gleichzeitige Sitzungen: maximale Anzahl 250.

- **Die maximale Anzahl gleichzeitiger Sitzungen pro Benutzer ist: xx**. Hier wird der aktuell eingestellte Wert für die maximal zulässige Anzahl gleichzeitiger Sitzungen pro Benutzerkennung angegeben.

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern.
- **Die maximale Anzahl gleichzeitiger Sitzungen für Ihre Benutzerkennung ist: xxx** Hier wird der aktuell eingestellte Wert für die maximal zulässige Anzahl gleichzeitiger Sitzungen angegeben.

  Nur Administratoren mit entsprechenden Zugriffsrechten sind berechtigt, diesen Wert zu ändern.
- **Sitzungskonfiguration speichern** Durch Klicken auf diese Schaltfläche können Sie die Einstellungen für die Sitzung speichern

(Laufende Nummer)

In der ersten Spalte von links wird die laufende Nummer angezeigt, die jeder Sitzung zugeordnet ist.

Beenden

Klicken Sie in der Spalte **Beenden** auf das angezeigte Symbol **Beenden**, um die in der ausgewählten Zeile angezeige Sitzung zu beenden bzw. zu löschen.

Um mehrere Sitzungen gleichzeitig zu beenden, markieren Sie erst alle gewünschten Sitzungen durch Anklicken des Kontrollkästchens jeder einzelnen Sitzung in der Spalte **Markieren** und klicken dann unter der Tabelle auf die Schaltfläche **Alle markierten Sitzungen beenden**. Siehe nächster Punkt **Markieren** sowie Kontrollkästchen und Schaltflächen.

Markieren

Durch Anklicken dieses Kontrollkästchens markieren Sie die in dieser Zeile angezeigte Sitzung, um sie nachher zu beenden.

Kennung

Zeigt die Kennung an, unter welcher der Benutzer sich angemeldet hat, z. B. **cusa**.

Klicken Sie auf den Spaltentitel, um die Tabelle nach dieser Spalte zu sortieren.

Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalte kann sortiert, aber nicht bearbeitet werden.

Anzeige von NSL-Kennungen bei Netzwerk-Einzelanmeldung mit NSL-Kennung

Über die **Netzwerk-Einzelanmeldung** (Network Single Logon) können Sie vom HTS oder vom OpenScape-Manager aus ohne Passwort auf eine Anlage zugreifen. Angezeigt wird eine solche Session im Session Manager in der Spalte **Kennung** beispielsweise als **htsadm@218.1.16.35**. Es wird also nicht

nur die Kennung **htssvc0** oder **htsadm** angezeigt, sondern **Kennung@IP-Adresse** des Ausgangs-Servers, von dem aus der Zugriff erfolgte, d. h. des Servers, auf dem der Benutzer sich tatsächlich eingeloggt hat. Bei der bisher verwendeten Lösung wurde die Session bei solchen Zugriffen sozusagen auf eine existierende Kennung umadressiert bzw. "gemappt". Bei der neuen Lösung wird eine dynamische Kennung erzeugt, die sich aus **Kennung@IP-Adresse** zusammensetzt. Im **Logging Management** wird die Kennung in der Spalte **User** entsprechend als **Kennung@IP-Adresse** angezeigt. Unter **Details** wird im Logging Management der gesamte Pfad und das Mapping des Network Single Logon angezeigt.

Siehe auch: Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Sitzung

In dieser Spalte wird für jede Sitzung eine eindeutige Referenznummer angezeigt. Wenn ein Benutzer sich mehrfach anmeldet, wird pro Sitzung (engl. Session) eine eindeutige Session-Referenznummer vergeben und in dieser Spalte angezeigt. Hilfreich ist die Session-Referenznummer auch fürs **Logging Management**, um die Querbeziehung zu den Aktivitäten im Logging Management herzustellen. Im Logging Management wird die Session-Referenznummer als **Session Ref.** angezeigt.

Klicken Sie auf den Spaltentitel, um die Tabelle nach dieser Spalte zu sortieren.

Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalte kann sortiert, aber nicht bearbeitet werden.

Client

Hier wird die IP-Adresse des Client-Systems angezeigt, von dem aus der Benutzer sich angemeldet hat.

Klicken Sie auf den Spaltentitel, um die Tabelle nach dieser Spalte zu sortieren.

Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalte kann sortiert, aber nicht bearbeitet werden.

Anmeldezeit

Zeigt Datum und Uhrzeit der Anmeldung an, d. h. den Zeitpunkt, wann ein Benutzer sich beim Server angemeldet hat, z. B. 2003-07-16 12:44.

Dieser Wert bleibt unverändert, solange die Session läuft.

Klicken Sie auf den Spaltentitel, um die Tabelle nach dieser Spalte zu sortieren.

Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalte kann sortiert, aber nicht bearbeitet werden.

Letzter Zugriff

Zeigt den Zeitpunkt (Datum und Uhrzeit) des letzten Browser-Zugriffs innerhalb der jeweiligen Session an. Der Wert wird bei jedem Neuzugriff entsprechend aktualisiert, alle anderen Werte bleiben pro Session unverändert.

Hierüber kann man ermitteln, welcher User wann zuletzt zugegriffen hat.
Ein Administrator, der viele Sessions verwaltet, kann nach **Letzter Zugriff** sortieren und dann feststellen, wann die Session ungültig wird - abhängig vom eingestellten Wert in "Session Inactivity Timeout".

Klicken Sie auf den Spaltentitel, um die Tabelle in aufsteigender oder absteigender Reihenfolge nach dieser Spalte zu sortieren.

Ein Pfeil neben dem Spaltentitel zeigt die Spalte an, nach der die Tabelle zur Zeit sortiert ist, und ob in aufsteigender oder absteigender Reihenfolge sortiert wird. Ein erneutes Klicken auf den Spaltentitel invertiert die Sortierreihenfolge und sortiert die Tabelle neu.

Standardeinstellung für Sortierung: Standardmäßig wird nach der Spalte **Letzter Zugriff** sortiert, und als oberster Eintrag wird der "älteste" Eintrag angezeigt, also der, auf den am längsten nicht mehr zugegriffen wurde.

Diese Spalte kann sortiert, aber nicht bearbeitet werden.

Alle markierten Sitzungen beenden

Ein Klick auf diese Schaltfläche beendet alle Sitzungen, die (siehe Kontrollkästchen **Markieren**) in der Tabelle **Bestehende Sitzungen** dementsprechend markiert sind.

3.2 Passwort ändern - Beschreibung der Felder

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Ändern

Löschen

Altes Passwort

Um das Passwort ändern zu können, muss in diesem Feld zunächst das alte Passwort eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die Mindestlänge beträgt 6 Zeichen, die maximale Länge beträgt 16 Zeichen.

Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Das Eingabefeld **Altes Passwort** wird nur angezeigt, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Neues Passwort

Das neue Passwort muss in diesem Feld eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Das Eingabefeld **Neues Passwort** wird nur angezeigt, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Passwort-Eingabe wiederholen

In diesem Feld muss das neue Passwort erneut eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Der Aufruf des Dialogfelds **Passwort-Eingabe wiederholen** ist nur möglich, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Ändern

Wenn Sie auf diese Schaltfläche klicken, werden die gewünschten Änderungen vorgenommen; das neue Passwort gilt ab sofort für alle weiteren Sitzungen.

Löschen

Wenn Sie auf Löschen klicken, wird der Inhalt der Eingabefelder entfernt und Sie können neue Werte eingeben.

3.3 Passwortverteilung (nur OpenScape 4000 Manager) - Beschreibung der Felder

Altes Passwort

Neues Passwort

Passwort-Eingabe wiederholen

Passwort auch ändern am Assistant(s) (Passwortverteilung)

Ändern

Löschen

Altes Passwort

Um das Passwort ändern zu können, muss in diesem Feld zunächst das alte Passwort eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die Mindestlänge beträgt 6 Zeichen, die maximale Länge beträgt 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Das Eingabefeld **Altes Passwort** wird nur angezeigt, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Neues Passwort

Das neue Passwort muss in diesem Feld eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Das Eingabefeld **Neues Passwort** wird nur angezeigt, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Passwort-Eingabe wiederholen

In diesem Feld muss das neue Passwort erneut eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Der Aufruf des Dialogfelds **Passwort-Eingabe wiederholen** ist nur möglich, wenn der Benutzer über die erforderlichen "Privilegien" (Zugriffsrechte) für das Ändern von Passwörtern verfügt.

Passwort auch ändern am Assistant(s) (Passwortverteilung)

Wenn Sie das Kontrollkästchen **Passwort auch ändern am Assistant(s) (Passwortverteilung) nicht** markieren, wird die Passwortänderung nur lokal am Manager angestossen.

Wenn Sie das Kontrollkästchen **Passwort auch ändern am Assistant(s) (Passwortverteilung)** markieren, werden auch alle Passwörter auf den zugeordneten Assistants geändert.

Ändern

Wenn Sie auf diese Schaltfläche klicken, werden die gewünschten Änderungen vorgenommen; das neue Passwort gilt ab sofort für alle weiteren Sitzungen.

Löschen

Wenn Sie auf Löschen klicken, wird der Inhalt der Eingabefelder entfernt und Sie können neue Werte eingeben.

3.4 Passwort-Einstellungen - Feldbeschreibungen

Erweiterte Passwort-Regeln verwenden (Passwortchronik; erweiterte Passwortkomplexität)

Um die Verwendung der erweiterten Passwort-Regeln zu aktivieren, markieren Sie das Feld "Erweiterte Passwort-Regeln verwenden" (Passwortchronik; erweiterte Passwortkomplexität) und geben die Werte für folgende Parameter ein:

- **Mindestlänge des Passworts: xx Zeichen**

  In diesem Eingabefeld legen Sie die Mindestlänge des Passworts fest. Zulässige Werte: 6 bis 20.
- **Das Passwort muss mindestens xx Großbuchstaben enthalten.**

  Dieses Eingabefeld bestimmt die minimale Anzahl von Großbuchstaben, die das Passwort enthalten muss. Zulässige Werte: 0 bis 20.
- **Das Passwort muss mindestens xx Kleinbuchstaben enthalten.**

  Dieses Eingabefeld bestimmt die minimale Anzahl von Kleinbuchstaben, die das Passwort enthalten muss. Zulässige Werte: 0 bis 20.
- **Das Passwort muss mindestens xx Ziffern enthalten.**

  Dieses Eingabefeld bestimmt die minimale Anzahl von Ziffern, die das Passwort enthalten muss. Zulässige Werte: 0 bis 20.
- **Das Passwort muss mindestens xx Sonderzeichen enthalten.**

  Dieses Eingabefeld bestimmt die minimale Anzahl von Sonderzeichen, die das Passwort enthalten muss. Zulässige Werte: 0 bis 20.
- **Länge der Passwortchronik: xx Passwörter**

  In diesem Eingabefeld legen Sie die Mindestanzahl an Passwortänderungen fest, nach der das gleiche Passwort (d.h. das erste in einer ganzen Reihe von Passwörtern) wieder verwendet werden kann. Zulässige Werte: 0 bis 10.
- **Mindestzeit zwischen Passwortänderungen: xx Tage**

  Dieses Eingabefeld legt die Anzahl der Tage fest, nach denen ein Passwort geändert werden kann. Zulässige Werte: 0 bis 30
- **Mindestanzahl der Zeichen, in denen sich das neue Passwort vom bisherigen Passwort unterscheiden muss: xx Zeichen**

  Dieses Eingabefeld bestimmt die Mindestanzahl von Ziffern, Buchstaben oder Sonderzeichen in denen sich das neue Passwort vom vorherigen Passwort unterscheiden muss. Zulässige Werte: 0 bis 20.

Geschäftszeiten aktivieren

Um einen Gültigkeitszeitraum (Tages- bzw. Geschäftszeiten) für die rechtmäßige Verwendung eines Kontos zu definieren, markieren Sie dieses Kontrollkästchen und nehmen folgende Einstellungen vor:

- **Arbeitstag beginnt um**

- Startzeit für die Verwendung des Kontos.
- **Arbeitstag endet um**
- Endezeit für die Verwendung des Kontos.
- **Wochenarbeitstage**
- Eine Nutzung des Kontos ist nur an markierten Wochentagen möglich.

Konto wird gesperrt nach: xx Tagen Inaktivität

Um die Gültigkeitsdauer der Kontonutzung zeitlich einzuschränken, markieren Sie dieses Kontrollkästchen und geben die Anzahl der Tage an, an denen kein Login erfolgt, also keine Aktivität vorliegt, und nach denen das Konto gesperrt wird.

Passwort muss ablaufen nach: xx Tagen

Um einen Gültigkeitszeitraum für ein Passwort zu definieren, also die Anzahl der Tage, nach denen das Passwort spätestens geändert werden muss, markieren Sie dieses Kontrollkästchen und geben die Anzahl der Tage an, für die das Passwort gültig sein soll.

3.5 Benutzerkennungsverwaltung und Systemkennungsverwaltung - Beschreibung der Felder

Kennung

Beschreibung

Sicherheitsprofil (nur in der "Benutzerkennungsverwaltung")

Neues Passwort

Passwort-Eingabe wiederholen

Passwort löschen

Änderung des Passworts erzwingen

Max. Passwort-Gültigkeit

Passwort ist unbegrenzt gültig

Kennung sperren

Passwort-Änderung erlaubt

Zugang nur über Network Single Logon

Kennung automatisch sperren

während

Automatisch wieder entsperren

Anwenden

Verwerfen

Aktualisieren

Kennung

Anzeigefeld für die Benutzerkennung im Bereich **Identifizierung** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**.

Siehe auch Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung".

Beschreibung

Eingabefeld für die Beschreibung des Benutzernamens im Bereich **Identifizierung** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die Beschreibung kann für die vordefinierten, im Dialogfeld **Systemkennungsverwaltung** aufgeführten Kennungen nicht geändert werden.

Sicherheitsprofil

Zeigt das Sicherheitsprofil der Benutzerkennung an: engr, rsca, rsta, cusa oder custa

Neues Passwort

Eingabefeld im Bereich **Aktionen** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. In diesem Feld muss das neue Passwort für den/die gewählten Benutzer eingegeben werden. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden. Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).

Passwort-Eingabe wiederholen

Eingabefeld im Bereich **Aktionen** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. In diesem Feld muss das neue Passwort für den/die gewählten Benutzer erneut eingegeben werden. Dadurch werden versehentliche Tippfehler vermieden, da Passwörter am Bildschirm nicht angezeigt werden.

Passwort löschen

Kontrollkästchen im Bereich **Aktionen** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Ist dieses Kontrollkästchen aktiviert (d.h. markiert), werden die Felder **Neues Passwort** und **Passwort-Eingabe wiederholen** ausgeblendet. Ebenso wird das Kontrollkästchen **Änderung des Passworts erzwingen** automatisch aktiviert und ausgeblendet. Wird das vorhandene Passwort für einen Benutzer bzw. eine Benutzergruppe gelöscht, dann ist bei der nächsten Anmeldung dieses Benutzers bzw. dieser Benutzergruppe keine Passwort-Eingabe notwendig. Da "Änderung erzwingen" jedoch automatisch zusammen mit "Passwort löschen" aktiviert wird, wird der Benutzer beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Im Dialogfeld **Systemkennungsverwaltung** ist dieses Kontrollkästchen für Systemkennungen und NSL-Kennungen nicht verfügbar: diese Kennungen müssen immer ein Passwort gesetzt haben.

Änderung des Passworts erzwingen

Kontrollkästchen im Bereich **Aktionen** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Ist dieses Kontrollkästchen aktiv, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Dieses Kontrollkästchen wird automatisch aktiviert, wenn **Passwort löschen** aktiv ist. Im Dialogfeld **Systemkennungsverwaltung** ist dieses Kontrollkästchen für Systemkennungen und NSL-Kennungen nicht verfügbar: erzwungene Passwortänderung wird nur bei interaktiver Anmeldung unterstützt.

Max. Passwort-Gültigkeit

Eingabefeld im Bereich **Eigenschaften** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**.
Der eingegebene Wert definiert die maximale Gültigkeitsdauer des Passworts (in Tagen). Wenn das Passwort ungültig wird, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Im Dialogfeld **Systemkennungsverwaltung** ist dieses Eingabefeld für Systemkennungen und NSL-Kennungen nicht verfügbar: erzwungene Passwortänderung wird nur bei interaktiver Anmeldung unterstützt.

Passwort ist unbegrenzt gültig

Kontrollkästchen im Bereich **Eigenschaften** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**.
Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), wird das Benutzer-Passwort nie ungültig, und das Eingabefeld **Max. Passwort-Gültigkeit** ist deaktiviert. Im Dialogfeld **Systemkennungsverwaltung** ist dieses Kontrollkästchen für Systemkennungen und NSL-Kennungen immer aktiviert.

Kennung sperren

Kontrollkästchen im Bereich **Eigenschaften** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), kann sich der Benutzer nicht anmelden.

Passwort-Änderung erlaubt

Kontrollkästchen im Bereich **Eigenschaften** des Dialogfelds **Benutzerkennungsverwaltung**. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), kann der Benutzer sein eigenes Passwort ändern - d. h., er hat Zugriff auf die Funktion **Passwort ändern**.

Zugang nur über Network Single Logon

Nur für RSP gibt es im Bereich **Eigenschaften** das zusätzliche Kontrollkästchen Zugang nur über Network Single Logon.

Durch Aktivieren dieses Kontrollkästchens legen Sie fest, dass der/die markierte/n Benutzer sich nicht mehr direkt am Server anmelden kann/können, d. h. die Anmeldung ist nur noch über NSL von einem übergeordneten RSP (SIRA)-Server aus möglich.

Wenn dieses Kontrollkästchen deaktiviert ist, können sich die markierten Benutzer direkt am Server anmelden.

Kennung automatisch sperren

Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach wieviel Anmeldefehlern der Zugriff für diese Benutzerkennung automatisch gesperrt wird.

Ist eine Kennung aufgrund von Anmeldefehlern automatisch gesperrt, so wird nach Eingabe des richtigen Passworts im Eingabebildschirm eine entsprechende Meldung angezeigt, die darauf hinweist, dass die Kennung aufgrund falsch eingegebener Parameter gesperrt wurde.

Siehe auch Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung.

Zulässige Werte: Nie; 1 bis max. 15 Anmeldefehler.

während

Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, innerhalb welcher Zeitspanne die fehlerhaften Anmeldungsversuche erfolgen müssen, um das automatische Sperren der Kennung zu aktivieren.

Ist eine Kennung aufgrund von Anmeldefehlern automatisch gesperrt, so wird nach Eingabe des richtigen Passworts im Eingabebildschirm eine entsprechende Meldung angezeigt, die darauf hinweist, dass die Kennung aufgrund falsch eingegebener Parameter gesperrt wurde.

Siehe auch Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung.

Zulässige Werte: Beliebige Zeitdauer; 30 Sekunden bis max. 1 Woche.

Automatisch wieder entsperren

Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach welcher Zeitspanne der Zugriff für die gesperrte Benutzerkennung wieder entsperrt wird.

Ist eine Kennung aufgrund von Anmeldefehlern automatisch gesperrt, so wird nach Eingabe des richtigen Passworts im Eingabebildschirm eine entsprechende Meldung angezeigt, die darauf hinweist, dass die Kennung aufgrund falsch eingegebener Parameter gesperrt wurde.

Siehe auch Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung.

Zulässige Werte: Nie; 30 Sekunden bis max. 1 Monat.

Anwenden

Die Schaltfläche **Anwenden** in den Dialogfeldern Benutzerkennungsverwaltung und Systemkennungsverwaltung wird verwendet, um die festgelegten Eigenschaften für alle gewählten Kennungen zu übernehmen. Dieser Befehl hat

die gleiche Funktion wie der Eintrag **Anwenden** im Menü **Bearbeiten** und das Symbol **Änderungen übernehmen** in der Symbolleiste.

Siehe auch:

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Verwerfen

Die Schaltfläche **Verwerfen** in den Dialogfeldern Benutzerkennungsverwaltung und Systemkennungsverwaltung wird verwendet, um die festgelegten bzw. geänderten Eigenschaften für alle gewählten Kennungen zu verwerfen. Dieser Befehl hat die gleiche Funktion wie der Eintrag **Verwerfen** im Menü **Bearbeiten** und das Symbol **Änderungen verwerfen** in der Symbolleiste.

Siehe auch

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Aktualisieren

Wenn Sie im Menü **Bearbeiten** auf **Aktualisieren** klicken, wird der Inhalt der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung** aktualisiert. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt.

Dieser Befehl hat die gleiche Funktion wie das Symbol **Daten vom Server aktualisieren** in der Symbolleiste.

Siehe hierzu auch

Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

3.6 Neue Benutzerkennung hinzufügen - Beschreibung der Felder

Neue Kennung

Beschreibung

Neue Kennung

Eingabefeld für die neue Benutzerkennung.

Eine Kennung muss mit einem alphabetischen Zeichen (a-z oder A-Z) beginnen, und darf nur aus alphanumerischen Zeichen (a-z, A-Z, 0-9), sowie aus Unterstrichen (_) und Bindestrichen (-) bestehen.

Beschreibung

Eingabefeld für die Beschreibung der Benutzerkennung.

Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen.

3.7 "Liste der Benutzerkennungen", Fenster "Export von Benutzerdaten"

Die in dieser Liste angezeigten Daten stimmen mit den Daten im Bereich **Benutzerkennungsverwaltung** überein.

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der Benutzerkennungen

Kennung

Beschreibung

Gesperrt

Max. Passwort-Gültigkeit

Passwort-Änderung erlaubt

 # eur.cgi v1.0

Diese Zeile ist immer die erste Zeile und gibt die Version des Ausgabeformats der Liste an. Eine geänderte Versionsnummer deutet auf ein geändertes Ausgabeformat hin, z.B. kann es dann neue oder geänderte Spalten beinhalten. Die folgende Beschreibung gilt für die Version "v1.0".

"**eur**" steht für "Export User Reports".

Export von Benutzerdaten: Liste der Benutzerkennungen

Dies ist der Titel der Liste. Er gibt an, welche Arten von Daten exportiert wurden; in diesem Fall also eine Liste der Benutzerkennungen. In der Titelzeile stehen neben dem Titel noch folgende Angaben:

- Erstellungsdatum und die Erstellungsuhrzeit der Datenliste
- Name des Servers, wie auf der Anlage konfiguriert
- Versionsnummer der Software auf dem Server, z.B. **0.520**

Kennung

Anzeigefeld für die Benutzerkennung. Diese Daten werden im Bereich **Identifizierung** des Dialogfelds **Benutzerkennungsverwaltung** unter **Zugangsverwaltung** definiert und verwaltet.

Der Eintrag **#0** am Ende der Spalte **Kennung** gibt an, dass der Datenexport fehlerfrei und vollständig durchgeführt wurde. Jeder andere Wert außer 0 weist auf einen Fehler während des Datenexports hin.

Siehe auch

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche.

Beschreibung

Kurze Beschreibung der Benutzerkennung. Die Beschreibung wird im Bereich **Identifizierung** des Dialogfelds **Benutzerkennungsverwaltung** unter **Zugangsverwaltung** definiert und verwaltet.

Siehe auch

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche.

Gesperrt

Hier wird der aktuelle Status des Kontrollkästchens **Kennung sperren** aus dem Bereich **Eigenschaften** der **Benutzerkennungsverwaltung** unter **Zugangsverwaltung** angezeigt. Ein "Ja" bedeutet, dass sich der Benutzer derzeit nicht anmelden kann.

Siehe auch

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche.

Max. Passwort-Gültigkeit

Zeigt den aktuellen Eingabewert des Feldes **Max. Passwort-Gültigkeit** im Bereich **Eigenschaften** an. Der Wert definiert die maximale Gültigkeitsdauer des Passworts (in Tagen). Der Wert "-1" zeigt an, dass das Passwort unbeschränkt gültig ist.

Siehe auch

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche.

Passwort-Änderung erlaubt

Zeigt den aktuellen Status des Kontrollkästchens **Passwort-Änderung erlaubt** im Bereich **Eigenschaften** des Dialogfelds **Benutzerkennungsverwaltung** unter **Zugangsverwaltung** an. Ein "Ja" bedeutet, dass der Benutzer sein eigenes Passwort ändern kann.

Siehe auch

Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche.

3.8 "Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen", Fenster "Export von Benutzerdaten"

Die in dieser Liste angezeigten Daten stimmen mit den Daten im Bereich **Zugriffsrechtekonfiguration** überein.

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen

Kennung

Beschreibung

ID der Zugriffsrechtegruppe

Beschreibung der Zugriffsrechtegruppe

 # eur.cgi v1.0

Diese Zeile ist immer die erste Zeile und gibt die Version des Ausgabeformats der Liste an. Eine geänderte Versionsnummer deutet auf ein geändertes Ausgabeformat hin, z.B. kann es dann neue oder geänderte Spalten beinhalten. Die folgende Beschreibung gilt für die Version "v1.0".

"**eur**" steht für "Export User Reports".

Export von Benutzerdaten: Liste der Benutzerkennungen und zugewiesener Zugriffsrechtegruppen

Dies ist der Titel der Liste. Er gibt an, welche Arten von Daten exportiert wurden; in diesem Fall also eine Liste der Benutzerkennungen und der Zugriffsrechtegruppen, die diesen Kennungen zugewiesen wurden. In der Titelzeile stehen neben dem Titel noch folgende Angaben:

- Erstellungsdatum und die Erstellungsuhrzeit der Datenliste
- Name des Servers, wie auf der Anlage konfiguriert
- Versionsnummer der Software auf dem Server, z.B. **0.520**

Kennung

Anzeigefeld für die Benutzerkennung. Diese Daten werden im Bereich **Benutzer** des Dialogfelds **Zugriffsrechtekonfiguration** unter **Zugangsverwaltung** definiert und verwaltet.

Der Eintrag **#0** am Ende der Spalte **Kennung** gibt an, dass der Datenexport fehlerfrei und vollständig durchgeführt wurde. Jeder andere Wert außer 0 weist auf einen Fehler während des Datenexports hin.

Siehe auch

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche.

Beschreibung

Kurze Beschreibung der Benutzerkennung. Die Beschreibung wird im Bereich **Benutzer** des Dialogfelds **Zugriffsrechtekonfiguration** unter **Zugangsverwaltung** definiert und verwaltet.

Siehe auch

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche.

ID der Zugriffsrechtegruppe

Zeigt die interne Kennung (ID) einer Zugriffsrechtegruppe an, z. B. **arg3** für eine selbst erstellte oder **All-SysM** für eine vorgegebene Zugriffsrechtegruppe.

Siehe auch

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche.

Beschreibung der Zugriffsrechtegruppe

Enthält eine kurze Beschreibung der Zugriffsrechtegruppe, z. B. "Alle Zugriffsrechte von "Configuration Management"", oder den Namen, wie er für eine selbst erstellte Gruppe vergeben wurde.

Siehe auch

Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche.

3.9 "Liste der selbst erstellten Zugriffsrechtegruppen", Fenster "Export von Benutzerdaten"

Die in dieser Liste angezeigten Daten stimmen mit den Daten im Bereich **Zugriffsrechtegruppen-Konfiguration** überein. Es werden jedoch nur die selbst erstellten Zugriffsrechtegruppen exportiert. Vordefinierte Gruppen werden nicht exportiert, da diese im System vorinstalliert und nicht änderbar sind.

Beschreibung der Tabellenzeilen und -spalten

eur.cgi v1.0

Export von Benutzerdaten: Liste der selbst erstellten Zugriffsrechtegruppen

ID der Zugriffsrechtegruppe

Beschreibung der Zugriffsrechtegruppe

ID der Komponente

Beschreibung der Komponente

ID des Zugriffsrechts

Beschreibung des Zugriffsrechts

eur.cgi v1.0

Diese Zeile ist immer die erste Zeile und gibt die Version des Ausgabeformats der Liste an. Eine geänderte Versionsnummer deutet auf ein geändertes Ausgabeformat hin, z.B. kann es dann neue oder geänderte Spalten beinhalten. Die folgende Beschreibung gilt für die Version "v1.0".

"**eur**" steht für "Export User Reports".

Export von Benutzerdaten: Liste der selbst erstellten Zugriffsrechtegruppen

Dies ist der Titel der Liste. Er gibt an, welche Arten von Daten exportiert wurden; in diesem Fall also eine Liste der im System selbst erstellten Zugriffsrechtegruppen. In der Titelzeile stehen neben dem Titel noch folgende Angaben:

- Erstellungsdatum und die Erstellungsuhrzeit der Datenliste
- Name des Servers, wie auf der Anlage konfiguriert
- Versionsnummer der Software auf dem Server, z.B. **0.520**

ID der Zugriffsrechtegruppe

Zeigt die interne Kennung (ID) einer selbst erstellten Zugriffsrechtegruppe an, z. B. **arg3**.

Der Eintrag **#0** am Ende dieser Spalte gibt an, dass der Datenexport fehlerfrei und vollständig durchgeführt wurde. Jeder andere Wert außer 0 weist auf einen Fehler während des Datenexports hin.

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

Beschreibung der Zugriffsrechtegruppe

Enthält den Namen, wie er für eine selbst erstellte Gruppe vergeben wurde.

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

ID der Komponente

Enthält die interne Kennung (ID) der Software-Komponente, z. B. HBR für "Backup & Restore".

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

Beschreibung der Komponente

Enthält eine kurze Beschreibung der davor angegebenen ID, z. B. "Direkter Zugriff (Direct Access)" für "DA".

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

ID des Zugriffsrechts

Jedes einzelne Zugriffsrecht innerhalb einer Zugriffsrechtegruppe verfügt über eine eigene interne ID (Kennung), die in dieser Spalte angezeigt wird, z. B. "HBR-Backup" für die Backup-Funktionalität von Backup & Restore oder "sendBroadcast" für die Funktion "Nachricht senden" der Startseite.

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

Beschreibung des Zugriffsrechts

Enthält eine kurze Beschreibung des davor angegebenen Zugriffsrechts, z. B. "Netzwerk-Einzelanmeldung" für "nsl-own" oder "Lizenzdaten installieren" für "storeLicData".

Siehe auch

Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche.

3.10 Verwalten von Web-Server-Zertifikaten - Feldbeschreibungen

3.10.1 Zertifikate für diesen Webserver -> Aktivieren

Aktivieren (Link auf Startseite der Zugangsverwaltung)

Navigieren: **Startseite -> Zugangsmanagement -> Webserver-Zertifikate verwalten -> Zertifikate für diesen Webserver -> Aktivieren**

Klicken oder doppelklicken Sie auf den Link **Aktivieren**, um das Dialogfeld **Server-Zertifikat aktivieren** zu öffnen.

In diesem Dialogfeld werden folgende Arten von SSL-Sicherheitszertifikaten angezeigt:

- Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)
- Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

Momentan aktives Zertifikat (Tabelle in Dialogfeld “Server-Zertifikat aktivieren”)

Das Derzeit aktive SSL-Sicherheitszertifikat, d. h. das Derzeit vom HTTP-Server verwendete Zertifikat, wird in einer Tabelle mit den folgenden **Spalten**angezeigt:

Herkunft (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Server-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zertifikatsinformationen (Dialogfeld “Zertifikat anzeigen”, erreichbar durch Klicken auf Link in Spalte “Server Name”)

CA-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Gültigkeitsdauer (von/bis) (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Herkunft (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zeigt an, auf welche Weise das momentan aktive SSL-Zertifikat erstellt wurde.

Mögliche Modi/Werte: **Vorinstalliert**, **Generiert**, **Importiert**, **Über CSR generiert**.

Anmerkung: Die Software wird standardmäßig mit vorinstalliertem Sicherheitszertifikat ausgeliefert. Bei vorinstalliertem Zertifikat muss kein Passwort eingegeben werden. Das Feld **Passworteintrag** wird nicht mit vorinstallierten Zertifikaten angezeigt.

Server-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Klicken Sie in der Spalte **Server-Name** auf den als **Link** angezeigten Namen, um weitere Details zum Derzeit aktiven Zertifikat anzuzeigen. Die vollständige Liste der Detaildaten dieses Zertifikats wird dann im Browser in der Tabelle **Zertifikatsinformation** angezeigt.

Zertifikatsinformationen (Dialogfeld “Zertifikat anzeigen”, erreichbar durch Klicken auf Link in Spalte “Server Name”)

Klicken Sie in der Spalte **Server-Name** auf den Namen (als Link angezeigt) des Derzeit aktiven Zertifikats. Die vollständige Liste der Detaildaten des Derzeit aktiven Zertifikats wird dann im Browser in der Tabelle **Zertifikatsinformation** angezeigt, die nach den folgenden Kategorien gruppiert sind:

- **Name und Gültigkeit**
  - Version des Zertifikats
  - Seriennummer
  - Signatur-Algorithmus
  - Beginn und Ende der Zertifikatsgültigkeit
- **Ausstellende CA**
  - CA Name
  - Land
  - Organisation
  - Organisatorische Einheit
- **Server**
  - Server-Name
  - Land
  - Organisation
  - Organisatorische Einheit
  - Mail-Adresse
- **Verschlüsselungsdaten**
  - Verschlüsselungsalgorithmus
  - Elliptische Kurve für ECDSA
  - Schlüssellänge
  - MD5 Fingerprint
  - SHA1 Fingerprint

Zertifikat löschen (Schaltfläche in Ansicht “Zertifikatsinformationen”, Dialogfeld “Zertifikat anzeigen”)

Die Schaltfläche **Zertifikat löschen** wird in der Tabelle **Zertifikatsinformationen** in roter Farbe angezeigt.

Klicken Sie auf diese Schaltfläche, um dieses Zertifikat, dessen Daten Derzeit in der Tabelle **Zertifikatsinformationen** angezeigt werden, zu löschen.

CA-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Name der Zertifizierungsstelle, die das Zertifikat geprüft und signiert hat.

Gültigkeitsdauer (von/bis) (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zeigt die Gültigkeitsdauer des momentan aktiven Zertifikats an.

Aktives Zertifikat verteilen (Schaltfläche unter Tabelle Derzeit aktives Zertifikat, Dialogfeld Server-Zertifikat aktivieren)

Diese Schaltfläche wird nur angezeigt, wenn mindestens eine HG3550 v2-Platine mit einem unabhängig ausgeführten Webserver installiert ist.

Klicken Sie auf **Aktives Zertifikat verteilen**, um das aktive Zertifikat auf alle vorhandenen HG3550 v2-Platinen zu verteilen.

Sie werden aufgefordert, das Passwort für den privaten Schlüssel des Zertifikats einzugeben und Ihre Aktion durch Klicken auf die Schaltfläche **Zertifikat verteilen** fortzusetzen.

Im Dialogfeld **Serverzertifikat aktivieren** wird dann eine der folgenden Meldungen angezeigt:

- die Bestätigungsmeldung über das erfolgreiche Verteilen des Zertifikats

oder

- eine Fehlermeldung, die angibt, dass beim Übertragen des aktiven Server-Zertifikats auf die HG3550 v2-Baugruppen ein Fehler aufgetreten ist.

  Die vom System ausgegebene Fehlermeldung wird am Bildschirm angezeigt und Sie werden aufgefordert, den Vorgang zu wiederholen und - falls der Fehler erneut auftreten sollte - die Konfiguration über den HG3550 v2 Manager zu überprüfen, die Baugruppenliste zu aktualisieren und eine Verbindung zu allen aufgelisteten Baugruppen herzustellen.

  Falls der Fehler weiterhin auftritt, sollten Sie die angezeigte Fehlermeldung an Ihren Systemadministrator oder an den Service weiterleiten.

Übersicht aller aktivierbaren Zertifikate (Tabelle im Dialogfeld “Server-Zertifikat aktivieren”)

In dieser Tabelle werden alle aktivierbaren Zertifikate angezeigt. Sie können aus dieser Liste ein neues Zertifikat zur Aktivierung auswählen, falls Sie vorher ein solches generiert oder importiert haben. Das ausgewählte Zertifikat wird Ihnen dann zur Überprüfung angezeigt.

Nur signierte Zertifikate können aktiviert werden.

Anmerkung: Die HG35xx-Platinen, die nicht auf Linux (STMI und NCUI) basieren, unterstützen nur RSA-Zertifikate für die webbasierte Verwaltung. Wenn der ausgewählte Zertifikattyp ECDSA ist, wird er nicht an diese Platinentypen verteilt. Alle SoftGate-basierten Platinen unterstützen ECDSA.

Anmerkung: Die Software wird standardmäßig mit vorinstalliertem Sicherheitszertifikat ausgeliefert. Bei vorinstalliertem Zertifikat muss kein Passwort eingegeben werden. Das Feld **Passworteintrag** wird nicht mit vorinstallierten Zertifikaten angezeigt.

Die Tabelle aller aktivierbaren Zertifikate umfasst folgende Spalten:

Herkunft (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Server-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Zertifikatsinformationen (Dialogfeld “Zertifikat anzeigen”, erreichbar durch Klicken auf Link in Spalte “Server Name”)

CA-Name (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Gültigkeitsdauer (von/bis) (Spalte in Tabellen Derzeit aktives Zertifikat und Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Aktivieren (Optionsschaltfläche in Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren**)**

Aktivieren (Optionsschaltfläche in Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Klicken Sie auf diese Optionsschaltfläche in der Spalte **Aktivieren**, um das zu aktivierende Zertifikat auszuwählen.

Nur signierte Zertifikate können aktiviert werden.

Verteilen des ausgewählten Zertifikats an alle verfügbaren HG35xx-Baugruppen (Kontrollkästchen unter Tabelle "Übersicht aller aktivierbaren Zertifikate", Dialogfeld "Server-Zertifikat aktivieren")

Wenn dieses Kontrollkästchen aktiviert ist (Standard: aktiviert), wird das ausgewählte Zertifikat auf dem Server wie üblich durch Klicken auf die Schaltfläche **Ausgewähltes Zertifikat aktivieren** aktiviert und gleichzeitig an alle verfügbaren HG35xx-Platinen verteilt.

Dieses Kontrollkästchen wird nur angezeigt, wenn mindestens eine HG35xx-Platine mit einem unabhängig ausgeführten Webserver auf diesem System installiert ist.

Nur signierte Zertifikate können aktiviert werden.

Standardeinstellung: Markiert.

Siehe auch

Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant

---

Anmerkung: Die HG35xx-Platinen, die nicht auf Linux (STMI und NCUI) basieren, unterstützen nur RSA-Zertifikate für die webbasierte Verwaltung. Wenn der ausgewählte Zertifikattyp ECDSA ist, wird er nicht an diese Platinentypen verteilt. Alle SoftGate-basierten Platinen unterstützen ECDSA.

Ausgewähltes Zertifikat aktivieren (Schaltfläche unter Tabelle Übersicht aller aktivierbaren Zertifikate, Dialogfeld Server-Zertifikat aktivieren)

Klicken Sie auf diese Schaltfläche, um das durch Aktivieren der Optionsschaltfläche in der Spalte **Aktivieren** markierte Zertifikat zu aktivieren und mit dem nächsten Prozessschritt fortzufahren.

Wählen Sie im Dialogfeld **Server-Zertifikat aktivieren** in der Tabelle **Übersicht aller aktivierbaren Zertifikate** in der Spalte **Aktivieren** die Optionsschaltfläche des Zertifikats, das Sie aktivieren möchten, aus und klicken Sie auf **Ausgewähltes Zertifikat aktivierene**.

Die Zertifikat-Details des ausgewählten Zertifikats werden dann im Dialogfeld **Server-Zertifikat aktivieren** angezeigt.

Siehe auch

Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant

und

Aktivieren - HG35xx-Platine NICHT installiert

Zertifikat aktivieren (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

Die Schaltfläche neben der Tabelle zeigt die Detaildaten im Dialogfeld **Server-Zertifikat aktivieren**.

1) Wählen Sie im Dialogfeld **Server-Zertifikat aktivieren** in der Tabelle **Übersicht aller aktivierbaren Zertifikate** in der Spalte **Aktivieren** die Optionsschaltfläche des Zertifikats, das Sie aktivieren möchten, aus.

   Nur signierte Zertifikate können aktiviert werden.
2) Klicken Sie auf **Ausgewähltes Zertifikat aktivieren**.

   Die Zertifikat-Details werden dann im Dialogfeld **Server-Zertifikat aktivieren** angezeigt, und das Programm fordert Sie auf, das Kennwort für den privaten Schlüssel einzugeben.

   Bei vorinstallierten Zertifikaten ist die Eingabe des Passworts nicht erforderlich, und daher wird keine Eingabeaufforderung und kein Passwort-Eingabefeld angezeigt.
3) Geben Sie das **Passwort** für den privaten Schlüssel ein - falls erforderlich - und klicken Sie auf **Zertifikat aktivieren**.

   Anmerkung: Der Web-Server muss nach dem Aktivieren eines neuen Zertifikats immer neu gestartet werden. Dabei werden alle laufenden Sitzungen auf dem Server beendet, auch die eigene Sitzung.

   Eine Warnmeldung des Servers wird angezeigt und weist darauf hin, dass der Web-Server nach dem Aktivieren eines neuen Zertifikats neu gestartet werden muss, und dass dabei alle laufenden Sitzungen - auch die eigene Sitzung - auf dem Server beendet werden.

   Das ausgewählte Zertifikat wird als neues **Derzeit aktives Zertifikat** im Dialogfeld **Server-Zertifikat aktivieren** angezeigt.

   oder
4) Klicken Sie auf **Zurück** im Dialogfeld **Server-Zertifikat aktivieren**, wenn Sie das neue Zertifikat nicht aktivieren möchten.

Siehe auch

Aktivieren - Bei INSTALLIERTER HG35xx-Baugruppe - Nur auf OpenScape 4000 Assistant

und

Aktivieren - HG35xx-Platine NICHT installiert

Zurück (Schaltfläche, Dialogfeld “Server-Zertifikat aktivieren”)

Die Schaltfläche untedr der Tabelle zeigt die Detaildaten im Dialogfeld **Server-Zertifikat aktivieren**.

Mit dieser Schaltfläche gelangen Sie zurück zum vorherigen Prozessschritt.

3.10.2 Zertifikate für diesen Web-Server -> Generieren

Server-Name

Mail-Adresse

Organisatorische Einheit

Organisation

Location (Standort)

Status

Land

Alternativer Name des Betreffs (subjectAltName)

Signatur-Algorithmus

Schlüssellänge - nur für RSA

Gültigkeit

Passwort für privaten Schlüssel

Bestätigung des Passworts

Server-Name

Der Server-Name muss angegeben werden und muss dem eindeutigen realen Host-Namen entsprechen (DNS-Name), mit dem der Server in der Adressleiste des Browsers angesprochen wird (ohne http:// bzw. https://). Wildcards (z. B. *.domain.com), IP-Adressen und Portnummern sind nicht erlaubt.

Beispiel: openscape4k.Firmenname.com

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Mail-Adresse

Optionale Mail-Adresse, z. B. des Web-Server-Administrators.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisatorische Einheit

Optionale Organisationseinheit innerhalb Ihrer Organisation, z. B. Abteilung.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisation

Optionaler Name Ihrer Organisation, z. B. Firma, Behörde.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Location (Standort)

Optionaler Name der Stadt, in der Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Status

Optionaler Name des Bundeslandes, in dem Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Land

Optionaler Ländercode (2 Buchstaben), z. B. DE für Deutschland.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Alternativer Name des Betreffs (subjectAltName)

Der alternative Name des Betreffs ist eine Erweiterung auf X.509, mit der Sie verschiedene Werte, die den Server beschreiben, z. B. IP -Adressen, URLs, DNS-Namen, hinzufügen können.

Assistant fügt automatisch die IP-Adressen von Assistant, CSTA GUI und Plattform-Portal in das Feld subjectAltName ein.

Standalone Appliances Portal/YAST IPs werden ebenfalls standardmäßig hinzugefügt. DNS-Namen werden ebenfalls standardmäßig für alle IP-Adressen hinzugefügt, wenn sie durch Abfrage in den DNS-Servern des Systems gefunden werden.

Darüber hinaus können Sie eigene Adressen für Server, die mit dem Zertifikat bereitgestellt werden sollen, hinzufügen.

Gateway-Adressen einschließen

Fügen Sie die Liste aller Gateway-IP-Adressen zu subjectAltName hinzu. Für das Webserver-Zertifikat müssen die Management-IP-Adressen hinzugefügt werden. Für das SPE-Zertifikat sollen die Voice-IP-Adressen hinzugefügt werden.

Signatur-Algorithmus

Gibt die für die Zertifikatsignatur verwendete Hash-Verschlüsselungsfunktion an.

Die Zahl im Funktionsnamen gibt die Länge des Hash-Werts in Bits an.

Die Dropdown-Liste ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: SHA-1, SHA-256 (empfohlen), SHA-384, SHA-512.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Schlüssellänge - nur für RSA

Gibt den Verschlüsselungsgrad als Schlüssellänge (in Bits) an.

2048 Bit ist der empfohlene Wert, da einige Browser Probleme mit längeren Schlüsseln haben.

Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: 2048 Bit (empfohlen); 4096 Bit.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Elliptische Kurve - nur für ECDSA

Für ECDSA muss die elliptische Kurve angegeben werden. Alle openssl-unterstützten elliptischen Kurven für ECDSA-Algorithmus sind hier aufgeführt. Die populärsten Kurven sind NIST-genehmigte Suite B, z. B. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Gültigkeit

Zertifikate werden immer mit einer beschränkten Gültigkeitsdauer erzeugt. Nach Ablauf der Gültigkeitsdauer warnt der Browser den Benutzer. Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes. Der Mindestwert beträgt 1 Woche, der Maximalwert 3 Jahre.

Mögliche Werte: 1 Woche, 2 Wochen, 1 Monat, 3 Monate, 6 Monate, 1 Jahr, 2 Jahre, 3 Jahre.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Passwort für privaten Schlüssel

Der private Schlüssel wird verschlüsselt abgelegt und kann nur unter Angabe des Passworts gelesen werden.

NOTICE: Achtung! Dieses Passwort wird nirgendwo gespeichert! Es muss daher beim Aktivieren dieses Zertifikats erneut eingegeben werden, auch wenn dies Tage oder Monate später erfolgt. Ein Zertifikat ist unbrauchbar, wenn das Passwort vergessen wurde.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Bestätigung des Passworts

Mit der Bestätigung des Passworts werden Tippfehler vermieden.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Weiter (Schaltfläche)

Mit dieser Schaltfläche gelangen Sie zum nächsten Prozessschritt.

Nachdem Sie ein neues Zertifikat erstellt haben, kehrt das Programm zum **Dialog Serverzertifikat aktivieren** zurück. Das neu erzeugte Zertifikat wird angezeigt und ist in der Regel bereits vorausgewählt (markiert). In der Spalte **Herkunft** wird in diesem {{case}} der Eint**rag Erze**ugt angezeigt.

Siehe auch die allgemeine Funktionsbeschreibung unter Generieren**.**

3.10.3 Zertifikate für diesen Web-Server -> Importieren

Datei mit Schlüssel und Zertifikat (Eingabefeld)

Passwort für privaten Schlüssel (Eingabefeld)

Zertifikat importieren (Schaltfläche)

Datei mit Schlüssel und Zertifikat (Eingabefeld)

Eingabefeld im Dialogfeld **Server-Zertifikat und Schlüssel importieren**. Eingabefeld für Pfad und Dateiname des auf einem anderen Host erzeugten Zertifikats inklusive privatem Schlüssel. Es werden nur Dateien im Format x.509 PEM und PKCS#12 unterstützt. Zur Entschlüsselung des privaten Schlüssels ist das Passwort notwendig (siehe nächstes Feld).

Unter folgenden Bedingungen ist das Importieren eines auf einem anderen Host erzeugten Zertifikats inklusive privatem Schlüssel möglich:

- Unterstütztes Dateiformat: X. 509 PEM und PKCS#12. Falls die Dateinamenerweiterung *.p12 ist, wird die Datei als PKCS#12 behandelt, für andere Dateinamenerweiterungen wird das X.509 PEM Format vorausgesetzt.
- Privater Schlüssel und Passwort zum Entschlüsseln sind erforderlich und vorhanden.

Passwort für privaten Schlüssel (Eingabefeld)

Um den verschlüsselten privaten Schlüssel zu entschlüsseln, muss das Passwort eingegeben werden.

Unter folgenden Bedingungen ist das Importieren eines auf einem anderen Host erzeugten Zertifikats inklusive privatem Schlüssel möglich:

- Unterstütztes Dateiformat: X. 509 PEM und PKCS#12. Falls die Dateinamenerweiterung *.p12 ist, wird die Datei als PKCS#12 behandelt, für andere Dateinamenerweiterungen wird das X.509 PEM Format vorausgesetzt.
- Privater Schlüssel und Passwort zum Entschlüsseln sind erforderlich und vorhanden.

Zertifikat importieren (Schaltfläche)

Das Programm springt zurück zum Dialogfeld **Server-Zertifikat aktivieren**. Das importierte Zertifikat wird angezeigt und ist bereits ausgewählt (markiert). In der Spalte **Herkunft** steht in diesem Fall **Importiert**. Das importierte Zertifikat kann jetzt aktiviert werden.

Der **Status** des markierten Zertifikats wird jetzt zusätzlich durch eine **Farbe** angezeigt. Die Farben haben folgende Bedeutung:

rot = signiertes Zertifikat, im Server aktiviert

grün = signiertes Zertifikat vorhanden, aktivierbar

Siehe auch die allgemeine Beschreibung des Leistungsmerkmals unter Import**.**

3.10.4 Zertifikate für diesen Web-Server -> Über CSR generieren

Server-Name (Tabellenspalte)

CA-Name (Tabellenspalte**)**

Gültigkeitsdauer (von / bis) (Tabellenspalte**)**

Generiert (Tabellenspalte)

Exportiert (Tabellenspalte)

Importiert (Tabellenspalte)

Bearbeiten (Tabellenspalte)

Testen (Schaltfläche)

Exportieren (Schaltfläche)

Importieren (Schaltfläche)

Aktivieren (Schaltfläche)

Zertifikatsinformationen

Zertifikat löschen (Schaltfläche)

Server-Name (Eingabefeld)

Mail-Adresse

Organisatorische Einheit

Organisation

Standort

Staat

Land

Schlüssellänge - nur für RSA

Gültigkeitsdauer

Passwort für privaten Schlüssel

Bestätigung des Passworts

Weiter (Schaltfläche)

Zurück (Schaltfläche)

Server-Name (Tabellenspalte)

Klicken Sie in der Spalte **Server-Name** auf den als **Link** angezeigten Namen, um weitere Details zum Derzeit aktiven Zertifikat anzuzeigen. Die vollständige Liste der Detaildaten dieses Zertifikats bzw. CSR wird dann im Browser in der Tabelle **Zertifikat / Zertifikatsinformationen anzeigen** angezeigt. Die Schaltfläche "Zertifikat löschen" in diesem Dialogfeld ermöglicht das Löschen des Zertifikats bzw. des CSRs.

CA-Name (Tabellenspalte)

Name der Zertifizierungsstelle, die das Zertifikat geprüft und signiert hat.

Gültigkeitsdauer (von / bis) (Tabellenspalte)

Start- und Enddatum der Gültigkeitsdauer (aus: JJJJ-MM-TT - bis: JJJJ-MM-TT) des derzeit aktiven Zertifikats.

Generiert (Tabellenspalte)

Gibt den Benutzer (Konto) an, der dieses Zertifikat generiert hat, z. B. **von: rsta**, und das Datum und die Uhrzeit der Erstellung im folgenden Format JJJJ-MM-TT HH:MM, z.B. **bei: 2004-02-11 10:07**.

Exportiert (Tabellenspalte)

Gibt den Benutzer (Konto) an, der dieses Zertifikat exportiert hat, z. B. **von: rsta**, und das Datum und die Uhrzeit des Exports im folgenden Format JJJJ-MM-TT HH:MM, z.B. **bei: 2004-02-11 10:07**.

Importiert (Tabellenspalte)

Gibt den Benutzer (Konto) an, der dieses Zertifikat importiert hat, z. B. **von: rsta**, und das Datum und die Uhrzeit des Exports im folgenden Format JJJJ-MM-TT HH:MM, z.B. **bei: 2004-02-11 10:07**.

Bearbeiten (Tabellenspalte)

Enthält die Symbol-Schaltflächen **Test**, **Export**, **Import**, **Aktivieren**.

Abhängig vom aktuellen Status eines Zertifikats kann die Aktion ausgeführt oder nicht ausgeführt werden (ausgegraut).

Testen (Schaltfläche)

Symbol-Schaltfläche in der Spalte **Aktion**; dient zum Testen des neu erstellten und selbst signierten Zertifikats.

Abhängig vom aktuellen Status eines Zertifikats kann die Aktion ausgeführt oder nicht ausgeführt werden (ausgegraut).

Exportieren (Schaltfläche)

Symbol-Schaltfläche in der Spalte **Aktion**; dient zum Exportieren des neu erstellten und selbst signierten Zertifikats.

Abhängig vom aktuellen Status eines Zertifikats kann die Aktion ausgeführt oder nicht ausgeführt werden (ausgegraut).

Importieren (Schaltfläche)

Symbol-Schaltfläche in der Spalte **Aktion**; dient zum Importieren des neu erstellten und selbst signierten Zertifikats.

Abhängig vom aktuellen Status eines Zertifikats kann die Aktion ausgeführt oder nicht ausgeführt werden (ausgegraut).

Aktivieren (Schaltfläche)

Symbol-Schaltfläche in der Spalte **Aktion**; dient zum Aktivieren des neu erstellten und selbst signierten Zertifikats.

Abhängig vom aktuellen Status eines Zertifikats kann die Aktion ausgeführt oder nicht ausgeführt werden (ausgegraut).

Zertifikatsinformationen

Klicken Sie in der Spalte **Server-Name** auf den Namen (als Link angezeigt) des Derzeit aktiven Zertifikats. Die vollständige Liste der Detaildaten des Derzeit aktiven Zertifikats wird dann im Browser in der Tabelle **Zertifikatsinformation** angezeigt, die nach den folgenden Kategorien gruppiert sind:

- **Name und Gültigkeit**
  - Version des Zertifikats
  - Seriennummer
  - Signatur-Algorithmus
  - Beginn und Ende der Zertifikatsgültigkeit
- **Ausstellende CA**
  - CA Name
  - Land
  - Organisation
  - Organisatorische Einheit
- **Server**
  - Server-Name
  - Land
  - Organisation
  - Organisatorische Einheit
  - Mail-Adresse
- **Verschlüsselungsdaten**
  - Verschlüsselungsalgorithmus
  - Elliptische Kurve für ECDSA
  - Schlüssellänge
  - MD5 Fingerprint
  - SHA1 Fingerprint

Zertifikat löschen (Schaltfläche)

Klicken Sie auf diese Schaltfläche in der Tabelle **Zertifikatsinformationen**, um das auf der Registerkarte **Zertifikatsinformationen** angezeigte aktuelle Zertifikat/CSR zu löschen. Die Schaltfläche wird in roter Farbe angezeigt.

Server-Name (Eingabefeld)

Der Server-Name muss angegeben werden und muss dem eindeutigen realen Host-Namen entsprechen (DNS-Name), mit dem der Server in der Adressleiste des Browsers angesprochen wird (ohne http:// bzw. https://). Wildcards (z. B. *.domain.com), IP-Adressen und Portnummern sind nicht erlaubt.

Beispiel: openscape4k.Firmenname.com

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Mail-Adresse

Optionale Mail-Adresse, z. B. des Web-Server-Administrators.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisatorische Einheit

Optionale Organisationseinheit innerhalb Ihrer Organisation, z. B. Abteilung.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisation

Optionaler Name Ihrer Organisation, z. B. Firma, Behörde.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Standort

Optionaler Name der Stadt, in der Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Staat

Optionaler Name des Bundeslandes, in dem Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Land

Optionaler Ländercode (2 Buchstaben), z. B. DE für Deutschland.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Signatur-Algorithmus

Gibt die für die Zertifikatsignatur verwendete Hash-Verschlüsselungsfunktion an.

Die Zahl im Funktionsnamen gibt die Länge des Hash-Werts in Bits an.

Die Dropdown-Liste ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: SHA-1, SHA-256 (empfohlen), SHA-384, SHA-512.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Schlüssellänge - nur für RSA

Gibt den Verschlüsselungsgrad als Schlüssellänge (in Bits) an.

2048 Bit ist der empfohlene Wert, da einige Browser Probleme mit längeren Schlüsseln haben.

Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: 2048 Bits (empfohlen); 4096 Bits.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Elliptische Kurve - nur für ECDSA

Für ECDSA muss die elliptische Kurve angegeben werden. Alle openssl-unterstützten elliptischen Kurven für ECDSA-Algorithmus sind hier aufgeführt. Die populärsten Kurven sind NIST-genehmigte Suite B, z. B. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Gültigkeitsdauer

Zertifikate werden immer mit einer beschränkten Gültigkeitsdauer erzeugt. Nach Ablauf der Gültigkeitsdauer warnt der Browser den Benutzer. Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes. Der Mindestwert beträgt 1 Woche, der Maximalwert 3 Jahre.

Mögliche Werte: 1 Woche, 2 Wochen, 1 Monat, 3 Monate, 6 Monate, 1 Jahr, 2 Jahre, 3 Jahre.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Sie können ein Zertifikat **verlängern**, **indem Sie seine Gültigkeitsdauer erweitern**. Gehen Sie hierzu wie folgt vor:

Gültigkeit einer Zertifikatsanforderung bzw. eines Zertifikats verlängern

1) Bewegen Sie den Mauszeiger in der Spalte **Gültigkeitsdauer** auf das Enddatum des Zertifikats.

   Der Tooltip-Text **Zertifikat verlängern** wird angezeigt.
2) Kllicken Sie auf das angezeigte Enddatum.

   Das Dialogfeld **Zertifikat über CSR generieren** wird angezeigt. Die Daten des Zertifikats sind in den Feldern bereits eingetragen. Sie sollten die vorhandenen Werte nach Möglichkeit beibehalten und nur die Gültigkeitsdauer verlängern, da geänderte Werte mit der Zertifizierungsstelle abgestimmt und von dieser geprüft und bestätigt werden müssen.

   Sie erzeugen mit dieser Methode eine neue Zertifikatsanforderung (CSR), die Sie später an eine Zertifizierungsinstanz (CA) schicken können, um sie signieren zu lassen. Das signierte Zertifikat können Sie dann auf dem Server importieren und aktivieren. Zu Testzwecken wird die neue Zertifikatsanforderung automatisch in ein selbstsigniertes Zertifikat umgewandelt. Dieses selbstsignierte Zertifikat können Sie testen und dann exportieren, um es an die Zertifizierungsstelle zu schicken.

Passwort für privaten Schlüssel

Der private Schlüssel wird verschlüsselt abgelegt und kann nur unter Angabe des Passworts gelesen werden.

Anmerkung: Achtung: Dieses Passwort wird nirgendwo gespeichert! Es muss daher beim Aktivieren dieses Zertifikats erneut eingegeben werden, auch wenn dies Tage oder Monate später erfolgt. Ein Zertifikat ist unbrauchbar, wenn das Passwort vergessen wurde.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Bestätigung des Passworts

Mit der Bestätigung des Passworts werden Tippfehler vermieden.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Weiter (Schaltfläche)

Mit dieser Schaltfläche gelangen Sie zum nächsten Prozessschritt.

Nach dem Erstellen eines neuen Zertifikats springt das Programm zurück zum Dialogfeld **Server-Zertifikat aktivieren**. Das neu erzeugte Zertifikat wird angezeigt und ist in der Regel bereits vorausgewählt (markiert). In der Spalt **Herkunft** wird der Eintrag **Über CSR generiert** in diesem Fall angezeigt.

Zurück (Schaltfläche)

Klicken Sie auf diese Schaltfläche im Dialogfeld **Zertifikat über CSR generieren**, um zum vorherigen Prozessschritt zurückzukehren.

Siehe auch die generische Funktionsbeschreibung unter Über CSR generieren.

3.10.5 Zertifikat Netzwerkmanagement-> Stammzertifikat

Link 'Stammzertifikat'

Neues Stammzertifikat (Schaltfläche)

Name der Zertifizierungsinstanz (Eingabefeld)

Mail-Adresse

Organisatorische Einheit

Organisation

Standort

Staat

Land

Signatur-Algorithmus

Schlüssellänge - nur für RSA

Gültigkeitsdauer

Passwort für privaten Schlüssel

Bestätigung des Passworts

Weiter (Schaltfläche)

Link 'Stammzertifikat'

Über diesen Link können Sie das Stammzertifikat zu den vertrauenswürdigen Stammzertifikaten und in die Java Laufzeitumgebung importieren. Anschließend lässt es sich zur Verwendung an alle übrigen Clients verteilen, die Zugang zu Managern und Assistants benötigen. Alle verwenden dann dieses eine Zertifikat.

Der Vorteil gegenüber einem selbstsignierten Zertifikat besteht darin, dass dieses Stammzertifikat für alle Manager und Assistants verwendbar ist. So braucht jeder Client, der Zugang zu dem Stammzertifikat hat, dieses nur einmal importieren, anstatt dass je Manager und Assistant ein eigenes Zertifilat erstellt werden muss.

Neues Stammzertifikat (Schaltfläche)

Schaltfläche im Dialogfeld **Stammzertifikat**.

1) Klicken Sie auf **Neues Stammzertifikat** im Dialogfeld **STAMMZERTIFIKAT**, wenn Sie ein neues Stammzertifikat erstellen möchten.

   Wenn für diesen Server noch kein Stammzertifikat erstellt wurde, wird das leere Dialogfeld **Stammzertifikat** geöffnet.

   Wenn für diesen Server bereits ein selbstsigniertes Stammzertifikat erstellt wurde, werden die Daten des vorhandenen Zertifikats zusammen mit einem entsprechenden Hinweis im Dialogfeld **Stammzertifikat** im Browser angezeigt.

   Anmerkung: Warnung: Falls bereits ein selbstsigniertes Stammzertifikat für diesen Server existiert und Sie trotzdem ein neues erzeugen, wird das vorhandene Stammzertifikat überschrieben.

   ---

2) Wenn Sie das vorhandene Stammzertifikat zum Signieren von CSRs verwenden möchten, klicken Sie auf CSR signieren.

   Mit diesem Stammzertifikat können Sie externe Zertifikatsanforderungen signieren.

3) Falls Sie ein neues Stammzertifikat erzeugen und das vorhandene Stammzertifikat überschreiben möchten, klicken Sie auf **Neues Stammzertifikat**.

   Das Dialogfeld **Stammzertifikat generieren** wird angezeigt.

Name der Zertifizierungsinstanz (Eingabefeld)

Der Name der Ihrer Zertifizierungsinstanz muss angegeben werden.

Geben Sie hier einen Namen für Ihre Zertifizierzungsinstanz ein.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Mail-Adresse

Optionale Mail-Adresse, z. B. des Web-Server-Administrators.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisatorische Einheit

Optionale Organisationseinheit innerhalb Ihrer Organisation, z. B. Abteilung.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Organisation

Optionaler Name Ihrer Organisation, z. B. Firma, Behörde.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Standort

Optionaler Name der Stadt, in der Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Staat

Optionaler Name des Bundeslandes, in dem Ihre Organisation ansässig ist.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Land

Optionaler Ländercode (2 Buchstaben), z. B. DE für Deutschland.

Verwenden Sie keine Akzentzeichen (z. B. "umlauts" wie "Ã¤" oder "Ã¼") oder andere Sonderzeichen.

Optional.

Signatur-Algorithmus

Gibt die für die Zertifikatsignatur verwendete Hash-Verschlüsselungsfunktion an.

Die Zahl im Funktionsnamen gibt die Länge des Hash-Werts in Bits an.

Die Dropdown-Liste ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: SHA-1, SHA-256 (empfohlen), SHA-384, SHA-512.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Schlüssellänge - nur für RSA

Gibt den Verschlüsselungsgrad als Schlüssellänge (in Bits) an.

2048 Bit ist der empfohlene Wert, da einige Browser Probleme mit längeren Schlüsseln haben.

Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes.

Mögliche Werte: 2048 Bits (empfohlen); 4096 Bits.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Elliptische Kurve - nur für ECDSA

Für ECDSA muss die elliptische Kurve angegeben werden. Alle openssl-unterstützten elliptischen Kurven für ECDSA-Algorithmus sind hier aufgeführt. Die populärsten Kurven sind NIST-genehmigte Suite B, z. B. P-256 (prime256v1), P-384 (secp384r1), P-521 (secp521r1)

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Gültigkeitsdauer

Zertifikate werden immer mit einer beschränkten Gültigkeitsdauer erzeugt. Nach Ablauf der Gültigkeitsdauer warnt der Browser den Benutzer. Die Dropdown-Liste in der zweiten Spalte ermöglicht die Auswahl des gewünschten Wertes. Der Mindestwert beträgt 1 Woche, der Maximalwert 3 Jahre.

Mögliche Werte: 1 Woche, 2 Wochen, 1 Monat, 3 Monate, 6 Monate, 1 Jahr, 2 Jahre, 3 Jahre.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Sie können ein Zertifikat **verlängern**, **indem Sie seine Gültigkeitsdauer erweitern**. Gehen Sie hierzu wie folgt vor:

Gültigkeit einer Zertifikatsanforderung bzw. eines Zertifikats verlängern

1) Bewegen Sie den Mauszeiger in der Spalte **Gültigkeitsdauer** auf das Enddatum des Zertifikats.

   Der Tooltip-Text **Zertifikat verlängern** wird angezeigt.
2) Kllicken Sie auf das angezeigte Enddatum.

   Das Dialogfeld **Zertifikat über CSR generieren** wird angezeigt. Die Daten des Zertifikats sind in den Feldern bereits eingetragen. Sie sollten die vorhandenen Werte nach Möglichkeit beibehalten und nur die Gültigkeitsdauer verlängern, da geänderte Werte mit der Zertifizierungsstelle abgestimmt und von dieser geprüft und bestätigt werden müssen.

   Sie erzeugen mit dieser Methode eine neue Zertifikatsanforderung (CSR), die Sie später an eine Zertifizierungsinstanz (CA) schicken können, um sie signieren zu lassen. Das signierte Zertifikat können Sie dann auf dem Server importieren und aktivieren. Zu Testzwecken wird die neue Zertifikatsanforderung automatisch in ein selbstsigniertes Zertifikat umgewandelt. Dieses selbstsignierte Zertifikat können Sie testen und dann exportieren, um es an die Zertifizierungsstelle zu schicken.

Passwort für privaten Schlüssel

Der private Schlüssel wird verschlüsselt abgelegt und kann nur unter Angabe des Passworts gelesen werden.

Anmerkung: Achtung: Dieses Passwort wird nirgendwo gespeichert! Es muss daher beim Aktivieren dieses Zertifikats erneut eingegeben werden, auch wenn dies Tage oder Monate später erfolgt. Ein Zertifikat ist unbrauchbar, wenn das Passwort vergessen wurde.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Bestätigung des Passworts

Mit der Bestätigung des Passworts werden Tippfehler vermieden.

Eingabe erforderlich.

Pflichtfelder sind durch ein rotes Sternchen (*) gekennzeichnet.

Weiter (Schaltfläche)

Mit dieser Schaltfläche gelangen Sie zum nächsten Prozessschritt.

Nach dem Erzeugen des neu erzeugten Stammzertifikats werden die Daten des Zertifikats sowie die folgende Meldung im Dialogfeld Stammzertifikat angezeigt:

"Das Zertifikat wurde erzeugt. Mit diesem Stammzertifikat können Sie nun externe Zertifikatsanforderungen signieren."

Sie können nun in diesem Dialog auf den CSR-Link CSR signieren klicken, um externe CSRs mit dem neu erstellten Stammzertifikat zu signieren.

Siehe auch die generische Funktionsbeschreibung unter Stammzertifikat**.**

3.10.6 Zertifikate für Netzverwaltung -> CSR signieren

CSR signieren

Zertifikatsanforderung (CSR) signieren (Dialogfeld)

Zertifikat einfügen

Oder Zertifikatsanforderung von Datei importieren

Durchsuchen (Schaltfläche)

Passwort für privaten Schlüssel des Stammzertifikats

Zertifikatsanforderung signieren (Schaltfläche)

Signiertes Zertifikat als Datei exportieren (Schalffläche)

Weiter (Schaltfläche)

CSR signieren

Link auf Startseite der **Zugangsverwaltung** sowie im Dialogfeld **Stammzertifikat**.

Klicken Sie auf **CSR signieren**, um eine externe Zertifikatsanforderung (CSR) für eine Anlage innerhalb eines OpenScape/HiPath-Netzwerks signieren zu lassen.

Voraussetzung ist, dass Sie zuvor ein eigenes selbstsigniertes Stammzertifikat erzeugt haben.

Ziel dieses Features ist, die Zertifikatsanforderungen (CSRs) für alle Anlagen innerhalb eines OpenScape/HiPath 4000-Netzwerks unter Verwendung eines eigenen, selbstsignierten Stammzertifikats von nur einer lokalen Zertifizierungsstelle signieren und zertifizieren zu lassen.

Falls noch kein Stammzertifikat für diesen Server erzeugt wurde, wird folgende Fehlermeldung auf dem ansonsten leeren Bildschirm angzeigt:

Fehler: Es wurde noch kein Stammzertifikat angelegt, um die Zertifikatsanforderungen zu signieren.

Erzeugen Sie in diesem Fall zuerst ein neues Stammzertifikat, und klicken Sie dann erneut auf CSR signieren. Das Dialogfeld **Zertifikatsanforderung (CSR) signieren** wird angezeigt.

Zertifikatsanforderung (CSR) signieren (Dialogfeld)

Dieses Dialogfeld wird nach einem Klick auf den Link CSR signieren auf der Startseite der **Zugangsverwaltung** oder des Dialogfelds **Stammzertifikat** angezeigt.

Sie können den Inhalt des signierten Zertifikats entweder mit Copy&Paste aus einer Textdatei in den Bereich unter **Zertifikat einfügen** kopieren oder das Zertifikat als Datei importieren, indem Sie auf **Durchsuchen** klicken und den Dateinamen <dateiname.csr> auswählen.

NOTICE: Wichtig: Es werden nur BASE64-kodierte PKCS#10-Requests akzeptiert. Bitte achten Sie darauf, auch die Begrenzungszeilen (BEGIN und END) zu kopieren!

Zertifikat einfügen

Bereich zum Anzeigen des Inhalts eines mit Copy&Paste aus einer Textdatei kopierten Zertifikats.

Sie können den Inhalt des signierten Zertifikats entweder mit Copy&Paste aus einer Textdatei in den Bereich unter **Zertifikat einfügen** kopieren oder das Zertifikat als Datei importieren, indem Sie auf **Durchsuchen** klicken und den Dateinamen <dateiname.csr> auswählen.

NOTICE: Wichtig: Es werden nur BASE64-kodierte PKCS#10-Requests akzeptiert. Bitte achten Sie darauf, auch die Begrenzungszeilen (BEGIN und END) zu kopieren!

Oder Zertifikatsanforderung von Datei importieren

Eingabefeld für den Dateinamen der Zertifikatsanforderung, Dialogfeld **Zertifikatsanforderung (CSR) signieren**.

Klicken Sie auf **Durchsuchen** neben diesem Eingabefeld. Das Dialogfeld **Dateidownload** öffnet sich. Wählen Sie in diesem Fenster den gewünschten

Pfad und Dateinamen aus (z. B. server.csr) und klicken Sie dann auf **Speichern**, **nicht** auf **Öffnen**.

Durchsuchen (Schaltfläche)

Schaltfläche im Dialogfeld **Zertifikatsanforderung (CSR) signieren**.

Sie können den Inhalt des signierten Zertifikats entweder mit Copy&Paste aus einer Textdatei in den Bereich unter **Zertifikat einfügen** kopieren oder das Zertifikat als Datei importieren, indem Sie auf **Durchsuchen** klicken und den Dateinamen <dateiname.csr> auswählen.

NOTICE: Wichtig: Es werden nur BASE64-kodierte PKCS#10-Requests akzeptiert. Bitte achten Sie darauf, auch die Begrenzungszeilen (BEGIN und END) zu kopieren!

Passwort für privaten Schlüssel des Stammzertifikats

Eingabefeld im Dialogfeld **Zertifikatsanforderung (CSR) signieren**.

Geben Sie hier das Passwort für den das **Passwort für den privaten Schlüssel** des Stammzertifikats ein und klicken Sie auf **Zertifikatsanforderung signieren**.

Zertifikatsanforderung signieren (Schaltfläche)

Wenn Sie das **Passwort für den privaten Schlüssel** des Stammzertifikats eingegeben und auf **Zertifikatsanforderung signieren** geklickt haben, springt das Programm zurück zum Dialogfeld **Zertifikat anzeigen** und zeigt die Informationen des signierten an.

Klicken Sie auf **Weiter**.

Signiertes Zertifikat als Datei exportieren (Schalffläche)

Nachdem Sie eine externe Zertifikatsanforderung importiert und signiert haben, können Sie sie als Datei exportieren, indem Sie auf **Signiertes Zertifikat als Datei exportieren** klicken.

Das Dialogfeld **Dateidownload** öffnet sich. Klicken Sie in diesem Dialogfeld auf **Speichern**, und **nicht** auf **Öffnen**.

Der **Dateiname server.crt** wird vom Programm vorgegeben. Sie können diesen Namen übernehmen oder in einen beliebigen anderen Dateinamen ändern. Speichern Sie die Datei in einem Ordner Ihrer Wahl.

Sobald das Dialogfeld **Download beendet** angezeigt wird, klicken Sie auf **Schließen**, um den Vorgang zu beenden.

Klicken Sie im Dialogfeld **Zertifikatsanforderung (CSR) signieren** auf **Weiter**. Das Programm springt zurück zum ersten Dialogfeld **Zertifikatsanforderung (CSR) signieren**, und Sie können ein nächstes CSR zum Signieren auswählen oder den Vorgang beenden.

Das exportierte, signierte CSR können Sie nun in Ihren Web-Server importieren.

Weiter (Schaltfläche)

Mit dieser Schaltfläche gelangen Sie zum nächsten Prozessschritt.

Siehe auch die allgemeine Beschreibung des Leistungsmerkmals unter CSR signieren**.**

3.11 Registerkarte "Zugangsverwaltung" in der Systemverwaltung

engr (Bereich "Zugang für den Service")

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **engr** für Service-Administratoren ein.

Die NSL-Kennung **engr** ist als Netwerkeinzelanmeldung für den Fernzugriff von Servicetechnikern auf Expertenebene für Notfallsituationen vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt in der Systemverwaltung! Für andere Objekte muss dieser Schritt analog wiederholt werden.

rsta (Bereich "Zugang für den Service")

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **rsta** für Service-Administratoren ein.

Die NSL-Kennung **rsta** ist als Netwerkeinzelanmeldung für den Fernzugriff von "Upper level" Servicetechnikern vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

rsca (Bereich "Zugang für den Service")

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **rsca** für Service-Administratoren ein.

Die NSL-Kennung **rsca** ist als Netwerkeinzelanmeldung für den Fernzugriff von "Lower level" Servicetechnikern vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf

den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Gleicher Wert für alle Service-Passwörter (Bereich "Zugang für den Service")

Dieses Kontrollkästchen wird nur angezeigt, wenn mindestens 2 Felder in diesem Bereich einen Eintrag enthalten.

Markieren Sie das Kontrollkästchen **Gleicher Wert für alle Service-Passwörter**, um für alle NSL-Kennungen im Bereich Zugang für den Service eine (identische) Kennung zu vergeben.

Wenn dieses Kontrollkästchen markiert ist und Sie im obersten editierbaren Feld in diesem Bereich einen Wert eingeben, werden die Werte in den übrigen editierbaren Feldern in diesem Bereich automatisch ebenfalls geändert.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

---

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt in der Systemverwaltung! Für andere Objekte muss dieser Schritt analog wiederholt werden.

---

cusa (Bereich "Zugang für den Kunden")

Der Bereich **Zugang für den Kunden** wird auf RSP-Servern nicht angezeigt.

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **cusa** für Kunden-Administratoren ein.

Die NSL-Kennung **cusa** ist als Netwerkeinzelanmeldung für den Fernzugriff von von Kundensicherheitsadministratoren vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

---

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

---

cust (Bereich "Zugang für den Kunden")

Der Bereich **Zugang für den Kunden** wird auf RSP-Servern nicht angezeigt.

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **cust** für Standardbenutzer ein.

Die NSL-Kennung **cust** ist als Netwerkeinzelanmeldung für den Fernzugriff von Standardbenutzern vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

---

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt in der Systemverwaltung! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Gleicher Wert für alle Kunden-Passwörter (Bereich "Zugang für den Kunden")

Dieses Kontrollkästchen wird nur angezeigt, wenn mindestens 2 Felder in diesem Bereich einen Eintrag enthalten.

Markieren Sie das Kontrollkästchen **Gleicher Wert für alle Kunden-Passwörter**, um für alle NSL-Kennungen im Kunden-Bereich eine (identische) Kennung zu vergeben.

Wenn dieses Kontrollkästchen markiert ist und Sie im obersten editierbaren Feld in diesem Bereich einen Wert eingeben, werden die Werte in den übrigen editierbaren Feldern in diesem Bereich automatisch ebenfalls geändert.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die

Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt! Für andere Objekte muss dieser Schritt analog wiederholt werden.

syst (Bereich "Systemzugang (Server-Server-Kommunikation)")

Geben Sie in dieses Feld das Passwort für die NSL-Benutzerkennung **syst** für Server-Server-Kommunikation ein.

Die NSL-Kennung **syst** ist als Netwerkeinzelanmeldung auf Systemebene für die interne Server-Server Kommunikation von OpenScape 4000 Komponenten wie z.B. Systemverwaltung, Expert Access/MPCID, Logging Management vorgesehen.

NOTICE: Wichtig: Durch Einrichten von Passwörtern für diese Kennungen vermeiden Sie unberechtigten Zugriff auf den Server über Network Single Logon (NSL). Geben Sie die Passwörter nur an Administratoren von Master-Systemen weiter (z.B. OpenScape 4000 Manager oder RSP (Remote Service Platform) für Fernadministration (Remote Service Access)), auf denen der Zugriff über NSL akzeptiert wird.

Siehe auch

Bereich "Zugang für den Service", Registerkarte "Zugangsverwaltung"

Bereich "Zugang für den Kunden", Registerkarte "Zugangsverwaltung"

Bereich "Systemzugang (Server-Server-Kommunikation)", Registerkarte "Zugangsverwaltung"

Systemkennungen und Kennungen für Netzwerk-Einzelanmeldung (Network Single Logon, NSL)

Liste der Systemkennungen, Dialogfeld "Systemkennungsverwaltung"

Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung"

Zugangsverwaltung Sicherheitsebenen und Benutzerkennungen

Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

---

NOTICE: Die Änderung der NSL-Passwörter gilt nur für das aktuell gewählte Objekt in der Systemverwaltung! Für andere Objekte muss dieser Schritt analog wiederholt werden.

Speichern (Schaltfläche)

Die Schaltfläche **Speichern** wird aktiviert, sobald Sie in einem editierbaren Feld auf der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** einen Wert eingeben oder ändern.

Wenn Sie auf **Speichern** klicken, werden Ihre Änderungen übernommen und wirksam gemacht. Die neuen bzw. geänderten Passwörter gelten ab sofort für alle weiteren Sitzungen.

Änderungen, die Sie an anderer Stelle in der Systemverwaltung vorgenommen haben, werden dabei ebenfalls gespeichert.

Verwerfen (Schaltfläche)

Die Schaltfläche **Verwerfen** wird aktiviert, sobald Sie in einem editierbaren Feld auf der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung** einen Wert eingeben oder ändern.

Wenn Sie auf **Verwerfen** klicken, werden die vorgenommenen Änderungen rückgängig gemacht und die ursprünglichen Werte wieder in den Feldern angezeigt.

Änderungen, die Sie an anderer Stelle in der Systemverwaltung vorgenommen haben ohne sie zu speichern, werden dabei ebenfalls rückgängig gemacht.

Neu (Schaltfläche)

Klicken Sie auf die Schaltfläche **Neu** in der Registerkarte **Zugangsverwaltung** in der **Systemverwaltung**, um neue Werte für NSL-Passwörter zu vergeben.

Klicken Sie anschließend auf die Schaltfläche **Speichern**, um die neuen NSL-Passwörter zu aktivieren und wirksam zu machen.

Änderungen, die Sie an anderer Stelle in der Systemverwaltung vorgenommen haben, werden dabei ebenfalls gespeichert.

Löschen (Schaltfläche)

Wenn Sie auf **Löschen** klicken, wird der Inhalt der Eingabefelder entfernt und Sie können neue Werte eingeben.

4 Referenzinformationen

Im Einzelnen werden folgende Themen behandelt:

4.1 Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

4.1.1 Symbolschaltflächen in der Symbolleiste - Dialogfeld "Benutzerkennungsverwaltung"

Neue Benutzerkennung hinzufügen

Erstellt einen neuen Benutzer. Gleiche Funktion wie **Hinzufügen** im Menü **Benutzer**.

Siehe auch Neue Benutzerkennung hinzufügen.

Gewählte Benutzerkennungen löschen

Löscht die gewählten Benutzerkennungen. Gleiche Funktion wie **Löschen** im Menü **Benutzer**.

Siehe auch Benutzerkennungen löschen.

Änderungen für gewählte Benutzerkennungen übernehmen

Die vorgenommenen Änderungen werden den gewählten Benutzerkennungen zugewiesen. Gleiche Funktion wie **Anwenden** im Menü **Bearbeiten** und Schaltfläche Anwenden. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Änderungen verwerfen

Die Änderungen werden nicht zugewiesen, sondern verworfen. Alle Eingabefelder und Kontrollkästchen werden auf ihren Anfangszustand zurückgesetzt. Gleiche Funktion wie **Verwerfen** im Menü **Bearbeiten** und Schaltfläche Verwerfen. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Daten vom Server aktualisieren

Aktualisiert den Inhalt des Dialogfelds **Benutzerkennungsverwaltung**. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Gleiche Funktion wie **Aktualisieren** im Menü **Bearbeiten**. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Hilfethemen anzeigen

Öffnet die Online-Hilfe und zeigt die Hilfethemen an. Gleiche Funktion wie **Hilfethemen** im Menü **Hilfe**. Siehe auch Menü "Hilfe", Leistungsmerkmal "Benutzerkennungsverwaltung".

Startseite anzeigen

Öffnet ein neues Browserfenster, in dem die Startseite von OpenScape 4000 Assistant/Manager angezeigt wird. Dort sind alle Anwendungen aufgeführt, auf die der momentan angemeldete Benutzer Zugriff hat. Gleiche Funktion wie **Startseite** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Benutzerkennungsverwaltung".

Sitzung beenden

Meldet den aktuellen Benutzer ab, schließt die laufende Sitzung für alle zugehörigen Browserfenster, und springt zurück zum Anmeldebildschirm. Gleiche Funktion wie **Sitzung beenden** im Menü **Aktion**. Siehe auch Menü "Aktion", Leistungsmerkmal "Benutzerkennungsverwaltung".

Spalten im Dialogfeld "Benutzerkennungsverwaltung"

Kennung	Zeigt die Bezeichnung der Benutzerkennung an.
Sicherheitsprofil	Zeigt das Sicherheitsprofil der Benutzerkennung an: engr, rsca, rsta, cusa oder custa
Zertifikatsname	Zeigt den dem Benutzer zugewiesenen Zertifikatnamen an. Entspricht dem allgemeinen Namen im Clientzertifikat des jeweiligen Benutzers.
Beschreibung	Zeigt die im Feld **Beschreibung** des Bereichs **Identifizierung** eingegebene Beschreibung der Benutzerkennung an.
Max. Passwort-Gültigkeit	Zeigt den aktuellen Eingabewert des Felds **Max. Passwort-Gültigkeit** im Bereich **Eigenschaften**. Der Wert definiert die maximale Gültigkeitsdauer des Passworts (in Tagen).

Unbegrenzte Gültigkeit	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Passwort ist unbegrenzt gültig** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), wird das Benutzer-Passwort nie ungültig.
Gesperrt	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Kennung sperren** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), kann sich der Benutzer nicht anmelden.
Passwort-Änderung erlaubt	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Passwort-Änderung erlaubt** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), kann der Benutzer sein eigenes Passwort ändern - d. h., er hat Zugriff auf die Funktion "Passwort ändern".
Automatisch sperren	Zeigt den aktuellen Eingabewert des Feldes **Kennung automatisch sperren** im Bereich **Automatisches Sperren**. Der Wert definiert, nach wieviel Anmeldefehlern der Zugriff für diese Benutzerkennung automatisch gesperrt wird.
Zugang nur über Network Single Logon	Nur für RSP gibt es im Bereich **Eigenschaften** das zusätzliche Kontrollkästchen Zugang nur über Network Single Logon. Durch Aktivieren dieses Kontrollkästchens legen Sie fest, dass der/die markierte/n Benutzer sich nicht mehr direkt am Server anmelden kann/können, d. h. die Anmeldung ist nur noch über NSL von einem übergeordneten RSP (SIRA)-Server aus möglich. Wenn dieses Kontrollkästchen deaktiviert ist, können sich die markierten Benutzer direkt am Server anmelden.

Bereiche im Dialogfeld "Benutzerkennungsverwaltung"

Bereich "Identifizierung"

Kennung	Zeigt die Bezeichnung der Benutzerkennung an.
Sicherheitsprofil	Zeigt das Sicherheitsprofil der Benutzerkennung an: engr, rsca, rsta, cusa oder custa
Zertifikatsname	Eingabefeld für den dem Benutzer zuzuweisenden Zertifikatnamen. Muss dem allgemeinen Namen im Clientzertifikat des jeweiligen Benutzers entsprechen.
Beschreibung	Eingabefeld für eine Beschreibung der im linken Dialogbereich markierten Benutzer. Das Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen.

Bereich "Aktionen"

Neues Passwort	Eingabefeld für ein neues Passwort für die im linken Dialogbereich markierten Benutzer. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden. Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).
Passwort-Eingabe wiederholen	Eingabefeld um das neue Passwort für die gewählten Benutzer erneut einzugeben. Dadurch werden versehentliche Tippfehler vermieden, da Passwörter am Bildschirm nicht angezeigt werden.
Passwort löschen	Kontrollkästchen um das Passwort für die gewählten Benutzer zu löschen. Ist dieses Kontrollkästchen aktiviert (d.h. markiert), werden die Felder **Neues Passwort** und **Passwort-Eingabe wiederholen** ausgeblendet. Ebenso wird das Kontrollkästchen **Änderung erzwingen** automatisch aktiviert und ausgeblendet. Wird das vorhandene Passwort für einen Benutzer bzw. eine Benutzergruppe gelöscht, dann ist bei der nächsten Anmeldung dieses Benutzers bzw. dieser Benutzergruppe keine Passwort-Eingabe notwendig. Da Änderung erzwingen jedoch automatisch zusammen mit Passwort löschen aktiviert wird, wird der Benutzer beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben.
Änderung des Passworts erzwingen	Kontrollkästchen für den erzwungenen Passwort-Wechsel. Ist dieses Kontrollkästchen aktiv, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Dieses Kontrollkästchen wird automatisch aktiviert, wenn **Passwort löschen** aktiv ist.

Bereich "Eigenschaften"

Max. Passwort- Gültigkeit	Eingabefeld für die maximale Gültigkeitsdauer des Passworts (in Tagen). Wenn das Passwort ungültig wird, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben.
Passwort ist unbegrenzt gültig	Kontrollkästchen um eine unbegrenzte Gültigkeitsdauer für das Passwort festzulegen. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), wird das Benutzer-Passwort nie ungültig, und das Eingabefeld **Max. Passwort-Gültigkeit** ist deaktiviert.
Kennung sperren	Kontrollkästchen um die gewählten Benutzer zu sperren. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), kann sich der Benutzer nicht anmelden.
Passwort-Änderung erlaubt	Kontrollkästchen um den Zugang zur Funktion **Passwort ändern** zu kontrollieren. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), kann der Benutzer sein eigenes Passwort ändern - d. h., er hat Zugriff auf die Funktion **Passwort ändern**.
Zugang nur über Network Single Logon	Nur für RSP gibt es im Bereich **Eigenschaften** das zusätzliche Kontrollkästchen Zugang nur über Network Single Logon. Durch Aktivieren dieses Kontrollkästchens legen Sie fest, dass der/die markierte/n Benutzer sich nicht mehr direkt am Server anmelden kann/können, d. h. die Anmeldung ist nur noch über NSL von einem übergeordneten RSP (SIRA)-Server aus möglich. Wenn dieses Kontrollkästchen deaktiviert ist, können sich die markierten Benutzer direkt am Server anmelden.

Bereich "Automatisches Sperren"

Kennung automatisch sperren	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach wieviel Anmeldefehlern der Zugriff für diese Benutzerkennung automatisch gesperrt wird. Zulässige Werte: Nie; 1 bis max. 15 Anmeldefehler.
während	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, innerhalb welcher Zeitspanne die fehlerhaften Anmeldungsversuche erfolgen müssen, um das automatische Sperren der Kennung zu aktivieren. Zulässige Werte: Beliebige Zeitdauer; 30 Sekunden bis max. 1 Woche.
Automatisch wieder entsperren	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach welcher Zeitspanne der Zugriff für die gesperrte Benutzerkennung wieder entsperrt wird. Zulässige Werte: Nie; 30 Sekunden bis max. 1 Monat.

Steuerungselemente und Schaltflächen im Dialogfeld "Benutzerkennungsverwaltung"

Anwenden	Die vorgenommenen Änderungen werden den gewählten Benutzerkennungen zugewiesen. Gleiche Funktion wie **Anwenden** im Menü **Bearbeiten**. Siehe Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Verwerfen	Die vorgenommenen Änderungen werden nicht zugewiesen, sondern verworfen. Alle Eingabefelder und Kontrollkästchen werden auf ihren Anfangszustand zurückgesetzt. Gleiche Funktion wie **Verwerfen** im Menü **Bearbeiten**. Siehe Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

4.2 Dialogfeld "Systemkennungsverwaltung" - Beschreibung der Bedienoberfläche

4.2.1 Symbolschaltflächen in der Symbolleiste - Dialogfeld "Systemkennungsverwaltung"

Änderungen für gewählte Benutzerkennungen übernehmen

Die vorgenommenen Änderungen werden den gewählten Benutzerkennungen zugewiesen. Gleiche Funktion wie **Anwenden** im Menü **Bearbeiten** und Schaltfläche Anwenden. Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung".

Änderungen verwerfen

Die Änderungen werden nicht zugewiesen, sondern verworfen. Alle Eingabefelder und Kontrollkästchen werden auf ihren Anfangszustand zurückgesetzt. Gleiche Funktion wie **Verwerfen** im Menü **Bearbeiten** und Schaltfläche Verwerfen. Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung".

Daten vom Server aktualisieren

Aktualisiert den Inhalt des Dialogfelds **Systemkennungsverwaltung**. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Gleiche Funktion wie **Aktualisieren** im Menü **Bearbeiten**. Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung".

Hilfethemen anzeigen

Öffnet die Online-Hilfe und zeigt die Hilfethemen an. Gleiche Funktion wie **Hilfethemen** im Menü **Hilfe**. Siehe auch Menü "Hilfe", Leistungsmerkmal "Systemkennungsverwaltung".

Startseite anzeigen

Öffnet ein neues Browserfenster, in dem die Startseite von OpenScape 4000 Assistant/Manager angezeigt wird. Dort sind alle Anwendungen aufgeführt, auf die der momentan angemeldete Benutzer Zugriff hat. Gleiche Funktion wie **Startseite** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Systemkennungsverwaltung".

Sitzung beenden

Meldet den aktuellen Benutzer ab, schließt die laufende Sitzung für alle zugehörigen Browserfenster, und springt zurück zum Anmeldebildschirm. Gleiche Funktion wie **Sitzung beenden** im Menü **Aktion**. Siehe auch Menü "Aktion", Leistungsmerkmal "Systemkennungsverwaltung".

Spalten im Dialogfeld "Systemkennungsverwaltung"

Kennung	Zeigt die Benutzerkennung an.
Beschreibung	Zeigt die Beschreibung der Benutzerkennung an.
Max. Passwort-Gültigkeit	Zeigt den aktuellen Eingabewert des Felds **Max. Passwort-Gültigkeit** im Bereich **Eigenschaften**. Der Wert definiert die maximale Gültigkeitsdauer des Passworts (in Tagen).
Unbegrenzte Gültigkeit	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Passwort ist unbegrenzt gültig** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), wird das Benutzer-Passwort nie ungültig.
Gesperrt	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Kennung sperren** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), kann sich der Benutzer nicht anmelden.

Passwort-Änderung erlaubt	Das nicht editierbare Kontrollkästchen in dieser Spalte zeigt den aktuellen Status des Kontrollkästchens **Passwort-Änderung erlaubt** im Bereich **Eigenschaften**. Ist das Kontrollkästchen aktiviert (markiert), kann der Benutzer sein eigenes Passwort ändern - d. h., er hat Zugriff auf die Funktion "Passwort ändern".
Automatisch sperren	Zeigt den aktuellen Eingabewert des Feldes **Kennung automatisch sperren** im Bereich **Automatisches Sperren**. Der Wert definiert, nach wieviel Anmeldefehlern der Zugriff für diese Benutzerkennung automatisch gesperrt wird.

Bereiche im Dialogfeld "Systemkennungsverwaltung"

Bereich "Identifizierung"

Kennung	Zeigt die Benutzerkennung an.
Beschreibung	Zeigt die Beschreibung der Benutzerkennung an.

Bereich "Aktionen"

Neues Passwort	Eingabefeld für ein neues Passwort für die im linken Dialogbereich markierten Benutzer. Bei der Passwort-Eingabe wird zwischen Groß- und Kleinschreibung unterschieden. Dieses Eingabefeld akzeptiert alphanumerische Zeichen und Sonderzeichen. Die minimale Länge beträgt 6 Zeichen, die maximale Länge 16 Zeichen. Das Passwort muss mindestens ein Sonderzeichen enthalten (weder Ziffer noch Buchstabe).
Passwort-Eingabe wiederholen	Eingabefeld um das neue Passwort für die gewählten Benutzer erneut einzugeben. Dadurch werden versehentliche Tippfehler vermieden, da Passwörter am Bildschirm nicht angezeigt werden.

Passwort löschen	Kontrollkästchen um das Passwort für die gewählten Benutzer zu löschen. Ist dieses Kontrollkästchen aktiviert (d.h. markiert), werden die Felder **Neues Passwort** und **Passwort-Eingabe wiederholen** ausgeblendet. Ebenso wird das Kontrollkästchen **Änderung erzwingen** automatisch aktiviert und ausgeblendet. Wird das vorhandene Passwort für einen Benutzer bzw. eine Benutzergruppe gelöscht, dann ist bei der nächsten Anmeldung dieses Benutzers bzw. dieser Benutzergruppe keine Passwort-Eingabe notwendig. Da Änderung erzwingen jedoch automatisch zusammen mit Passwort löschen aktiviert wird, wird der Benutzer beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Dieses Kontrollkästchen ist nicht für Systemkennungen und NSL-Kennungen vergfügbar: diese Kennungen müssen immer ein Passwort gesetzt haben.
Änderung des Passworts erzwingen	Kontrollkästchen für den erzwungenen Passwort-Wechsel. Ist dieses Kontrollkästchen aktiv, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Dieses Kontrollkästchen wird automatisch aktiviert, wenn **Passwort löschen** aktiv ist. Dieses Kontrollkästchen ist nicht für Systemkennungen und NSL-Kennungen vergfügbar: erzwungene Passwortänderung wird nur bei interaktiver Anmeldung unterstützt.

Bereich "Eigenschaften"

Max. Passwort-Gültigkeit	Eingabefeld für die maximale Gültigkeitsdauer des Passworts (in Tagen). Wenn das Passwort ungültig wird, "erzwingt" das System einen Passwort-Wechsel - d. h., der Benutzer wird beim nächsten Anmeldeversuch aufgefordert, ein neues Passwort einzugeben. Dieses Eingabefeld ist nicht für Systemkennungen und NSL-Kennungen vergfügbar: erzwungene Passwortänderung wird nur bei interaktiver Anmeldung unterstützt.
Passwort ist unbegrenzt gültig	Kontrollkästchen um eine unbegrenzte Gültigkeitsdauer für das Passwort festzulegen. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), wird das Benutzer-Passwort nie ungültig, und das Eingabefeld **Max. Passwort-Gültigkeit** ist deaktiviert. Dieses Kontrollkästchen ist für Systemkennungen und NSL-Kennungen immer aktiviert.
Kennung sperren	Kontrollkästchen um die gewählten Benutzer zu sperren. Diese Eigenschaft kann ein- und ausgeschaltet werden. Ist das Kontrollkästchen aktiviert (markiert), kann sich der Benutzer nicht anmelden.

Bereich "Automatisches Sperren"

Kennung automatisch sperren	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach wieviel Anmeldefehlern der Zugriff für diese Benutzerkennung automatisch gesperrt wird. Zulässige Werte: Nie; 1 bis max. 15 Anmeldefehler.

während	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, innerhalb welcher Zeitspanne die fehlerhaften Anmeldungsversuche erfolgen müssen, um das automatische Sperren der Kennung zu aktivieren. Zulässige Werte: Beliebige Zeitdauer; 30 Sekunden bis max. 1 Woche.
Automatisch wieder entsperren	Eingabefeld im Bereich **Automatisches Sperren** der Dialogfelder **Benutzerkennungsverwaltung** und **Systemkennungsverwaltung**. Klicken Sie auf die Dropdown-Liste in diesem Feld, um festzulegen, nach welcher Zeitspanne der Zugriff für die gesperrte Benutzerkennung wieder entsperrt wird. Zulässige Werte: Nie; 30 Sekunden bis max. 1 Monat.

Steuerungselemente und Schaltflächen im Dialogfeld "Systemkennungsverwaltung"

Anwenden	Die vorgenommenen Änderungen werden den gewählten Benutzerkennungen zugewiesen. Gleiche Funktion wie **Anwenden** im Menü **Bearbeiten**. Siehe Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung".
Verwerfen	Die vorgenommenen Änderungen werden nicht zugewiesen, sondern verworfen. Alle Eingabefelder und Kontrollkästchen werden auf ihren Anfangszustand zurückgesetzt. Gleiche Funktion wie **Verwerfen** im Menü **Bearbeiten**. Siehe Menü "Bearbeiten", Leistungsmerkmal "Systemkennungsverwaltung".

4.3 Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration"

4.3.1 Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtekonfiguration"

Gruppen an gewählte Benutzer zuweisen

Gruppen den gewählten Benutzern entziehen

Gruppen der gewählten Benutzer ersetzen

Alle Gruppen den gewählten Benutzern entziehen

Daten vom Server aktualisieren

Hilfethemen anzeigen

Startseite anzeigen

Sitzung beenden

Gruppen an gewählte Benutzer zuweisen

Zuweisen aller im rechten Bereich gewählten Zugriffsrechtegruppen an alle im linken Bereich gewählten Benutzer. Gleiche Funktion wie **Zuweisen** im Menü **Bearbeiten**. Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

Gruppen den gewählten Benutzern entziehen

Entziehen aller im linken Bereich gewählten Zugriffsrechtegruppen von den zugehörigen Benutzern. Gleiche Funktion wie **Entziehen** im Menü **Bearbeiten**.

Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

Anmerkung: Entziehen wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.

Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Gruppen der gewählten Benutzer ersetzen

Wählen Sie im linken Bereich den/die gewünschten Benutzer und im rechten Bereich die Zugriffsrechtegruppen, die an Stelle der vorhandenen Zugriffsrechtegruppen eingesetzt werden sollen. Wenn Sie im Menü **Bearbeiten** auf **Ersetzen** klicken, werden die zuvor zugewiesenen Zugriffsrechtegruppen durch die aktuell markierten Zugriffsrechtegruppen ersetzt. Die vorher zugewiesenen Zuordnungen werden überschrieben. Unterschied zu **Zuweisen**: bei **Zuweisen** werden die neuen Zugriffsrechtegruppen zu den bereits zugewiesenen Zugriffsrechtegruppen hinzugefügt, und diese werden nicht überschrieben. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

NOTICE: Ersetzen wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.

Alle Gruppen den gewählten Benutzern entziehen

Markieren Sie im linken Bereich den/die Benutzer, denen alle Zugriffsrechte entzogen werden sollen. Wenn Sie im Menü **Bearbeiten** auf **Alle entziehen** klicken, werden den markierten Benutzern alle zugewiesenen Zugriffsrechte entzogen. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen. **Anmerkung: Alle entziehen** wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.

Daten vom Server aktualisieren

Aktualisiert den Inhalt des Dialogfelds **Zugriffsrechtekonfiguration**. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Gleiche Funktion wie **Aktualisieren** im Menü **Bearbeiten**. Siehe auch Menü "Bearbeiten", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Hilfethemen anzeigen

Öffnet die Online-Hilfe und zeigt die Hilfethemen an. Gleiche Funktion wie **Hilfethemen** im Menü **Hilfe**. Siehe auch Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Startseite anzeigen

Öffnet ein neues Browserfenster, in dem die Startseite von OpenScape 4000 Assistant/Manager angezeigt wird. Dort sind alle Anwendungen aufgeführt, auf die der momentan angemeldete Benutzer Zugriff hat. Gleiche Funktion wie **Startseite** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Sitzung beenden

Meldet den aktuellen Benutzer ab, schließt die laufende Sitzung für alle zugehörigen Browserfenster, und springt zurück zum Anmeldebildschirm. Gleiche Funktion wie **Sitzung beenden** im Menü **Aktion**. Siehe auch Menü "Aktion", Leistungsmerkmal "Zugriffsrechtekonfiguration".

Benutzerkennungen (linker Bereich)

Zeigt eine zweistufige Baumstruktur mit allen verfügbaren Benutzern (obere Ebene) sowie den zugehörigen Zugriffsrechtegruppen (untergeordnete Ebene) an. Jeder Benutzer ist durch einen Ordner dargestellt. Jeder Ordner enthält die diesem Benutzer zugewiesenen Zugriffsrechtegruppen. Jeder Ordner kann geöffnet werden, um die dem Benutzer zugewiesenen Zugriffsrechtegruppen anzuzeigen. Siehe auch Zugriffsrechtekonfiguration, Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration" und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Zugriffsrechtegruppen (rechter Bereich)

Zeigt alle Zugriffsrechtegruppen an, die Benutzern zugewiesen werden können. Siehe auch Zugriffsrechtekonfiguration, Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration" und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Vorschaufenster

Die **werden am unteren Rand des Dialogfelds** Zugriffsrechtekonfiguration angezeigt und können mit Hilfe der Option Vorschaufenster für Zugriffsrechte im eingeblendet und ausgeblendet werden. Die Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration" zeigen alle Zugriffsrechte, die derzeit der gewählten Zugriffsrechtegruppe zugeordnet sind. Falls - im linken Bereich - ein Benutzer statt einer Zugriffsrechtegruppe gewählt ist, werden im linken Vorschaufenster alle Zugriffsrechte angezeigt, die derzeit diesem Benutzer zugewiesen sind. Durch Aktivieren/Deaktivieren der Menüoption **Anzeigen/Verbergen der Liste mit Zugriffsrechten in Vorschaufenster** unter Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtekonfiguration" können Sie die Vorschaufenster ein- und ausblenden. Siehe auch Dialogfeld "Zugriffsrechtekonfiguration" - Beschreibung der Bedienoberfläche, Zuweisen/Entziehen von Zugriffsrechtegruppen, Dialogfeld "Zugriffsrechtekonfiguration" und Vorschaufenster im Dialogfeld "Zugriffsrechtekonfiguration".

Zugriffsrechte des gewählten Benutzers (Vorschaufenster, linke Seite)

Zeigt die Liste der einem Benutzer zugewiesenen Zugriffsrechte.

Zugriffsrechte der gewählten Zugriffs-rechtegruppe (Vorschaufenster, rechte Seite)

Zeigt die Liste der zu einer Zugriffsrechtegruppe gehörenden Zugriffsrechte.

4.4 Dialogfeld "Zugriffsrechtegruppen-Konfiguration" - Beschreibung der Bedienoberfläche

Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

4.4.1 Symbolschaltflächen in der Symbolleiste - Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Neue Zugriffsrechtegruppe hinzufügen

Kopieren der gewählten Zugriffsrechtegruppe in eine neue Gruppe

Umbenennen der gewählten Gruppenzugriffsrechte

Löschen der gewählten Zugriffsrechtegruppe

Zugriffsrechte der gewählten Gruppe(n) zuweisen

Zugriffsrechte der gewählten Gruppe(n) entziehen

Zugriffsrechte der gewählten Gruppe(n) ersetzen

Den gewählten Zugriffsgruppen alle Rechte entziehen

Daten vom Server aktualisieren

Anzeigen/Verbergen vordefinierter Zugriffsrechtegruppen

Anzeigen/Verbergen selbst erstellter Zugriffsrechtegruppen

Anzeigen/Verbergen der Zugriffsrechtegruppen für dynamische Applikationen

Anzeigen der Zugriffsrechte als Komponentenbaum

Anzeigen der Zugriffsrechte als Applikationsbaum

Hilfethemen anzeigen

Startseite anzeigen

Sitzung beenden

Neue Zugriffsrechtegruppe hinzufügen

Öffnet das Dialogfeld Neue Zugriffsrechtegruppe hinzufügen. Gleiche Funktion wie **Neue Gruppe hinzufügen** im Menü **Gruppe** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Kopieren der gewählten Zugriffsrechtegruppe in eine neue Gruppe

Öffnet das Dialogfeld Kopieren der ausgewählten Zugriffsrechtegruppe. Gleiche Funktion wie **Gewählte Gruppe kopieren** im Menü **Gruppe** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Umbenennen der gewählten Gruppenzugriffsrechte

Öffnet das Dialogfeld Umbenennen der ausgewählten Zugriffsrechtegruppe. Gleiche Funktion wie **Umbenennen der ausgewählten Gruppe** im Menü **Gruppe** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Löschen der gewählten Zugriffsrechtegruppe

Löscht die gewählte(n) Zugriffsrechtegruppe(n). Gleiche Funktion wie **Gewählte Gruppe(n) löschen** im Menü **Gruppe** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Zugriffsrechte der gewählten Gruppe(n) zuweisen

Die im rechten Bereich gewählten Zugriffsrechte werden allen im linken Bereich gewählten Zugriffsrechtegruppen zugewiesen. Gleiche Funktion wie **Zugriffsrechte zuweisen** im Menü **Bearbeiten** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Zugriffsrechte der gewählten Gruppe(n) entziehen

Die im linken Bereich gewählten Zugriffsrechte werden den entsprechenden Zugriffsrechtegruppen entzogen. Gleiche Funktion wie **Zugriffsrechte entziehen** im Menü **Bearbeiten** und im Kontextmenü. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Zugriffsrechte der gewählten Gruppe(n) ersetzen

Wählen Sie im linken Bereich die Menge der manuell erstellten Zugriffsrechtegruppen (funktioniert nur für MANUELL ERSTELLTE Zugriffsrechtegruppen) und im rechten Bereich die Menge der einzelnen

Zugriffsrechte oder übergeordnete Ordner. Wenn Sie im Menü **Bearbeiten** auf **Ersetzen** klicken, werden die zuvor zugewiesenen Zugriffsrechte durch die aktuell markierten Zugriffsrechte ersetzt. Die vorher zugewiesenen Zuordnungen werden überschrieben. Unterschied zu **Zuweisen**: bei **Zuweisen** werden die neuen Zugriffsrechte zu den bereits zugewiesenen hinzugefügt. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

NOTICE: Zugriffsrechte ersetzen wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.

Den gewählten Zugriffsgruppen alle Rechte entziehen

Markieren Sie im linken Bereich die Menge der manuell erstellten Zugriffsrechtegruppen (funktioniert nur für MANUELL ERSTELLTE Zugriffsrechtegruppen). Sie haben auch die Möglichkeit, die übrigen Zugriffsrechtegruppen auszublenden, um nur die manuell erstellten Zugriffsrechtegruppen anzuzeigen. Wenn Sie im Menü **Bearbeiten** auf **Alle Zugriffsrechte entziehen** klicken, werden den markierten Zugriffsrechtegruppen alle zugewiesenen Rechte entzogen. Alternativ können Sie diesen Befehl auch über das Kontextmenü oder über die Symbolleiste aufrufen.

NOTICE: Alle Zugriffsrechte entziehen wird erst nach zusätzlicher Rückfrage und Bestätigung ausgeführt.

Daten vom Server aktualisieren

Aktualisiert den Inhalt des Dialogfelds **Zugriffsrechtegruppen-Konfiguration**. Hierbei werden die aktuellen Daten vom Server neu geladen und eventuell vorgenommene Änderungen von zeitgleich laufenden Administrator-Sitzungen angezeigt. Gleiche Funktion wie **Aktualisieren** im Menü **Bearbeiten**. Siehe auch Menü Bearbeiten, Leistungsmerkmal Benutzerkennungsverwaltung.

Anzeigen/Verbergen vordefinierter Zugriffsrechtegruppen

Einblenden/Ausblenden der vordefinierten Zugriffsrechtegruppen. Gleiche Funktion wie **Vordefinierte Zugriffsrechtegruppen** im Menü Ansicht. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Anzeigen/Verbergen selbst erstellter Zugriffsrechtegruppen

Einblenden/Ausblenden der selbst erstellten Zugriffsrechtegruppen. Gleiche Funktion wie **Selbst erstellte Zugriffsrechtegruppen** im Menü Ansicht. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Anzeigen/Verbergen der Zugriffsrechtegruppen für dynamische Applikationen

Einblenden/Ausblenden der Zugriffsrechtegruppen für dynamische Applikationen. Gleiche Funktion wie **Zugriffsrechtegruppen für dynamische Applikationen** im Menü Ansicht. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Anzeigen der Zugriffsrechte als Komponentenbaum

Die Zugriffsrechte werden unterhalb der Komponenten angezeigt, zu denen sie gehören. Die entsprechenden Applikationen innerhalb der Komponenten werden ausgeblendet. Gleiche Funktion wie **Zugriffsrechte - Komponentenbaum anzeigen** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Anzeigen der Zugriffsrechte als Applikationsbaum

Die Zugriffsrechte werden unterhalb der entsprechenden Applikationen angezeigt. (Verfügbare Komponenten können aus mehr als einer Applikation bestehen, die auf der Startseite angezeigt werden.) Gleiche Funktion wie **Zugriffsrechte - Applikationsbaum anzeigen** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Hilfethemen anzeigen

Öffnet die Online-Hilfe und zeigt die Hilfethemen an. Gleiche Funktion wie **Hilfethemen** im Menü **Hilfe**. Siehe auch Menü "Hilfe", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration". Â¨

Startseite anzeigen

Öffnet ein neues Browserfenster, in dem die Startseite von OpenScape 4000 Assistant/Manager angezeigt wird. Dort sind alle Anwendungen aufgeführt, auf die der momentan angemeldete Benutzer Zugriff hat. Gleiche Funktion wie **Startseite** im Menü **Ansicht**. Siehe auch Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Sitzung beenden

Meldet den aktuellen Benutzer ab, schließt die laufende Sitzung für alle zugehörigen Browserfenster, und springt zurück zum Anmeldebildschirm.

Gleiche Funktion wie **Sitzung beenden** im Menü **Aktion**. Siehe auch Menü "Aktion", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration".

Bereiche und Vorschaufenster im Dialogfeld "Zugriffsrechtegruppen-Konfiguration"

Zugriffsrechtegruppen (linker Bereich)	Zeigt eine mehrstufige Baumstruktur mit allen verfügbaren Zugriffsrechtegruppen (obere Ebene) sowie deren zugewiesenen Zugriffsrechten (untergeordnete Ebene).
Zugriffsrechte - Komponentenbaum/ Applikationsbaum (rechter Bereich)	Zeigt alle Zugriffsrechte an, die den selbst erstellten Zugriffsrechtegruppen zugewiesen werden können. Sie können zwischen zwei Darstellungsarten wechseln: Anzeige als **Komponentenbaum** oder als **Applikationsbaum**.
Information über Zugriffsrecht (Vorschaufenster, linke und rechte Seite)	Zeigt eine genauere Beschreibung der gerade gewählten Zugriffsrechts.

Die **Vorschaufenster** am unteren Rand des Dialogfelds Zugriffsrechtegruppen-Konfiguration können durch Aktivieren bzw. Deaktivieren der Option **Information über Zugriffsrecht** im Menü "Ansicht", Leistungsmerkmal "Zugriffsrechtegruppen-Konfiguration" eingeblendet bzw. ausgeblendet werden.

4.5 Meldungen bei fehlerhafter NSL-Anmeldung und bei gesperrter NSL-Benutzerkennung

Beim Versuch, sich unter einer NSL-Kennung beim System anzumelden, werden in folgenden Fällen Fehlermeldungen angezeigt:

Keine Zugriffsberechtigung für Network Single Logon (NSL)

Passwort für NSL-Zugang nicht korrekt

NSL-Zugang gesperrt

NSL-Zugang automatisch gesperrt

Kennung am Zielserver nicht vorhanden

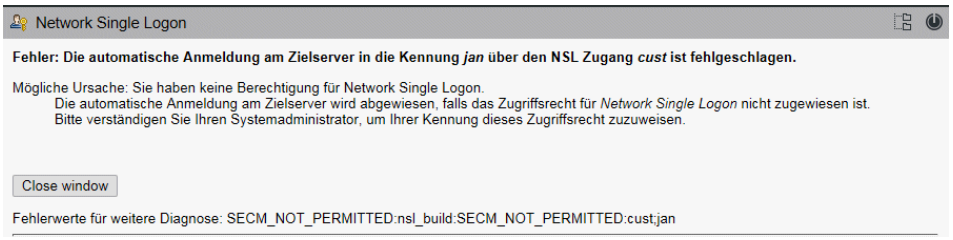
Interner Fehler während automatischer Anmeldung

Fehler bei Aufbau der Verbindung zum Zielserver

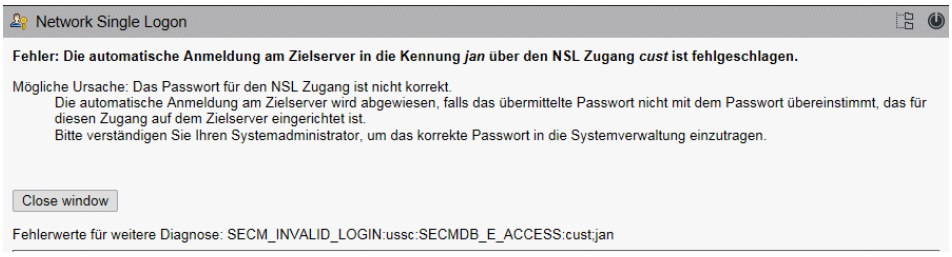
Interner Systemfehler auf Zielserver

Die Fehlermeldungen sind selbsterklärend.

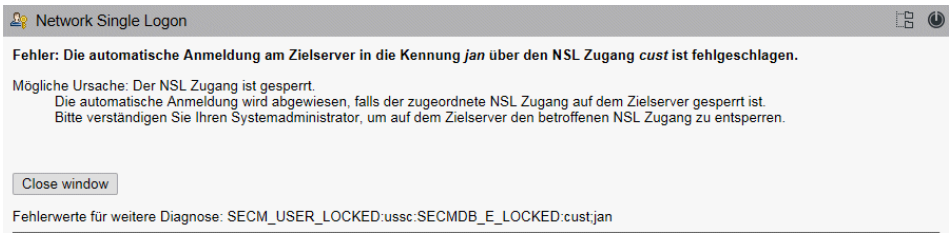
Keine Zugriffsberechtigung für Network Single Logon (NSL)



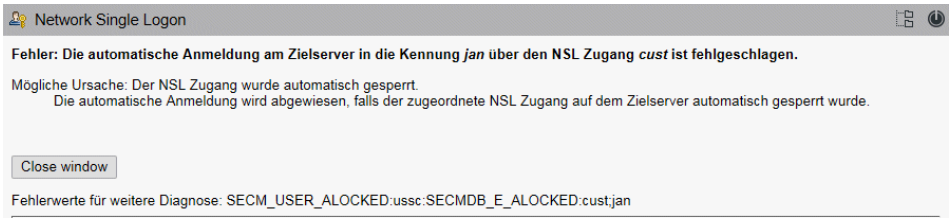
Passwort für NSL-Zugang nicht korrekt



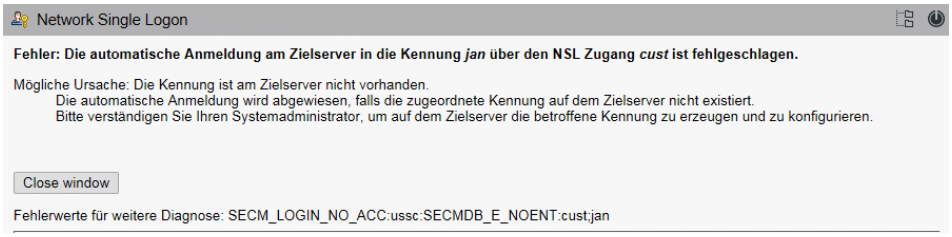
NSL-Zugang gesperrt



NSL-Zugang automatisch gesperrt



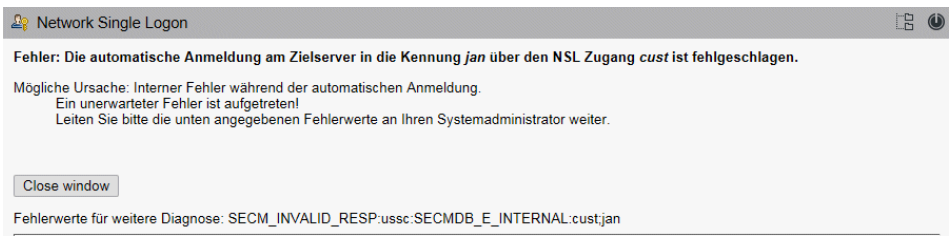
Kennung am Zielserver nicht vorhanden



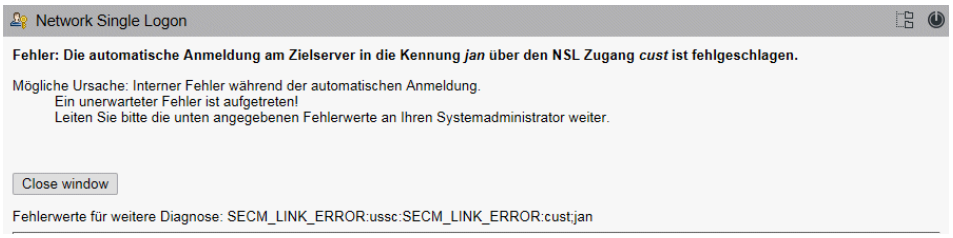
Diese Situation tritt standardmäßig nur beim Zugang von SIRA zu RSP oder Manager auf.

Es gibt jedoch die Möglichkeit, ein beliebiges System (z. B. Assistant) so zu konfigurieren, dass es nur NSL-Logons akzeptiert, wenn das entsprechende Profil (hier in Beispiel Kennung âmark") auf dem Zielsystem existiert.

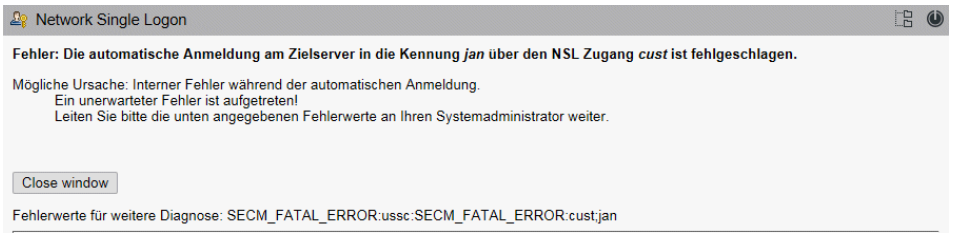
Interner Fehler während automatischer Anmeldung



Fehler bei Aufbau der Verbindung zum Zielserver



Interner Systemfehler auf Zielserver



Index

M

N

O

P

S

T

U

V

W

Z