ECOS **Appliances**

ECOS Appliances V8

Administratorhandbuch

Version: 2.12

Stand: 07/2025

IT Security Solutions

Made in Germany

ECOS TECHNOLOGY GMBH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel.: +49 6133 939-0 | Fax: +49 6133 939-333
Geschäftsführer: Paul Marx, Gerald Richter | Firmensitz: Oppenheim | Amtsgericht Mainz HRB 6889 | USt.-ID: DE 203394263

1 Installation der Appliance

1.1 Anforderung für die Installation

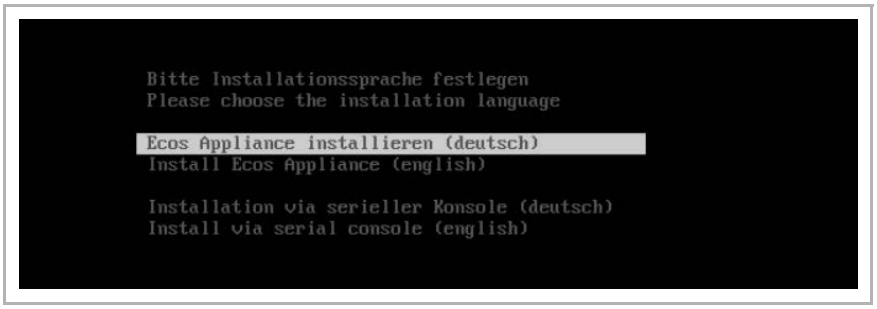
Zur Installation der Appliance ist es notwendig, eine virtuelle Maschine auf einem Hypervisor anzulegen. Die ECOS Appliance ist dabei sowohl unter VMware, Hyper-V, XenServer, KVM wie auch unter diversen anderen Hypervisoren lauffähig. An die Virtuelle Maschine (VM), auf der die Appliance installiert werde soll, bestehen folgende Mindestanforderungen:

- 4 CPU Kerne
- 8 GB RAM
- 120 GB Plattenplatz
- 1 Ethernet Interface

Je nach Ausbau, sind diese Werte zu erhöhen. Außerdem wird für die Installation eine ISO Installationsdatei von ECOS benötigt.

1.2 Einrichtung auf dem Hypervisor

Zur Installation muss die VM von der ISO Datei gebootet werden. Beim Start besteht die Möglichkeit die Installation in englischer oder deutscher Sprache auszuführen.

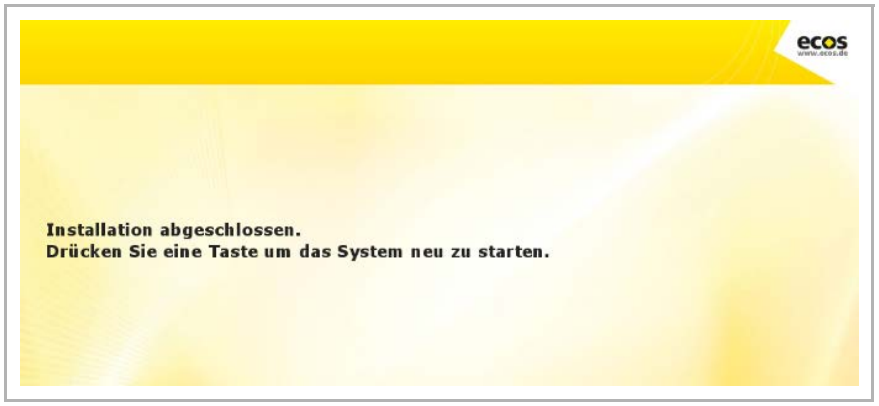


Danach ist es notwendig, die Platte auszuwählen, auf der installiert werden soll, sowie die Installation auf dieser Platte zu bestätigen.

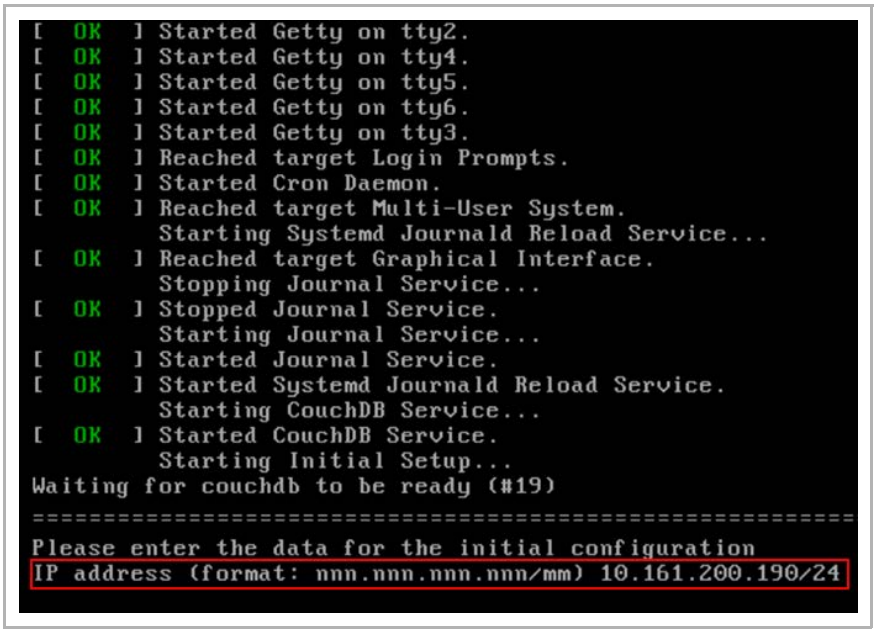
In den meisten Fällen steht nur eine Platte zur Auswahl. Zur Auswahl einer Platte wird die Ziffer der Platte eingegeben, dann die Enter-Taste gedrückt.

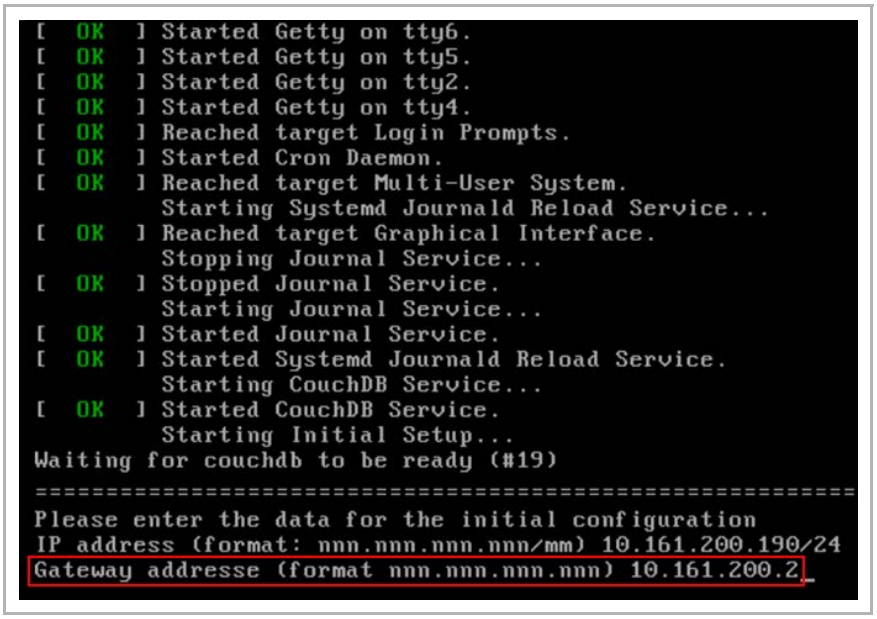
Danach muss die Installation bestätigt werden.

Die notwendigen Dateien werden auf die Festplatte kopiert, danach muss das System neu gestartet werden.



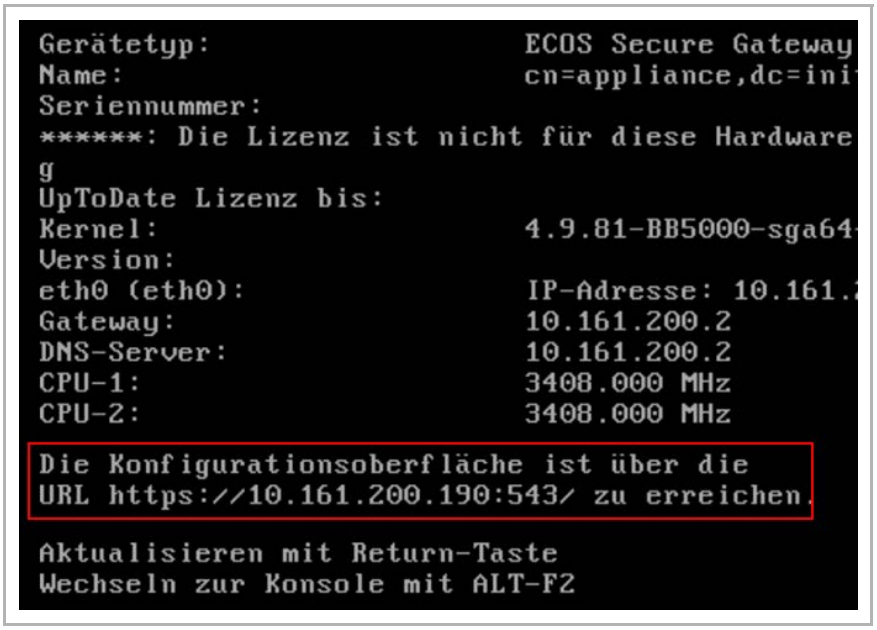
Beim ersten Boot werden die Netzwerkdaten abgefragt. Dazu muss zuerst die IP-Adresse und dann das Standard-Gateway der Appliance angegeben werden.





Nach Angabe dieser Daten bootet die Appliance vollständig und jegliche weitere Konfiguration erfolgt ausschließlich über die webbasierte Administrationsoberfläche.

Die URL für den Aufruf der Weboberfläche wird nach kurzer Zeit auf der Konsole angezeigt. Außerdem erscheint der Hinweis, dass noch keine Lizenzen vorhanden sind. Diese müssen für die vollständige Funktion der Appliance noch eingespielt werden. → *Siehe „1.4 | Lizenzen der Appliance hochladen" auf Seite 11*.

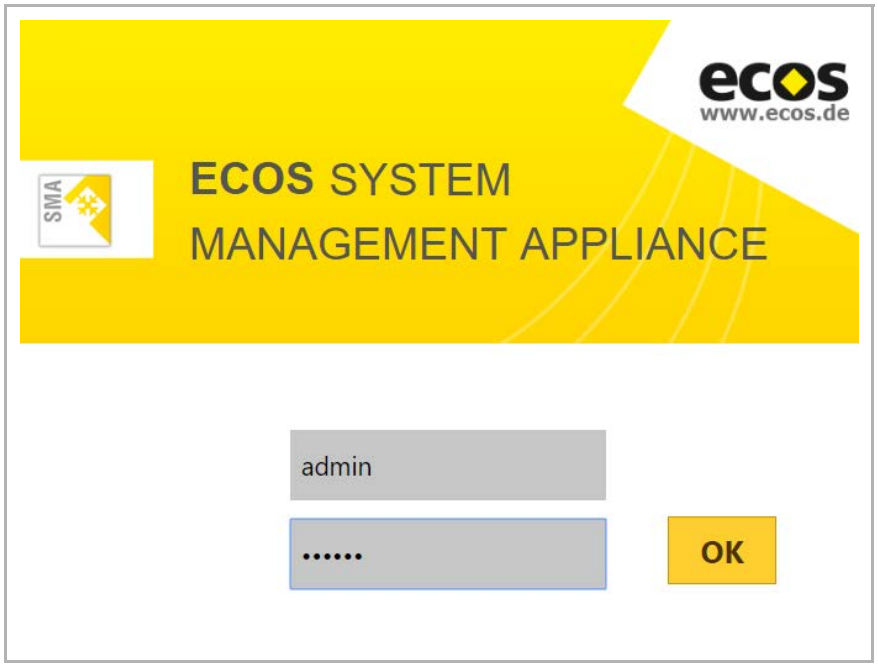


1.3 Anmeldung

Der Zugriff auf die Administrationsoberfläche erfolgt mittels Webbrowser. Der Aufruf findet via HTTPS auf Port 543 statt.

Wenn die Appliance z.B. mit der IP-Adresse 192.168.1.1 installiert worden ist, wird die Administrationsoberfläche durch Eingabe der URL https://192.168.1.1:543 aufgerufen.

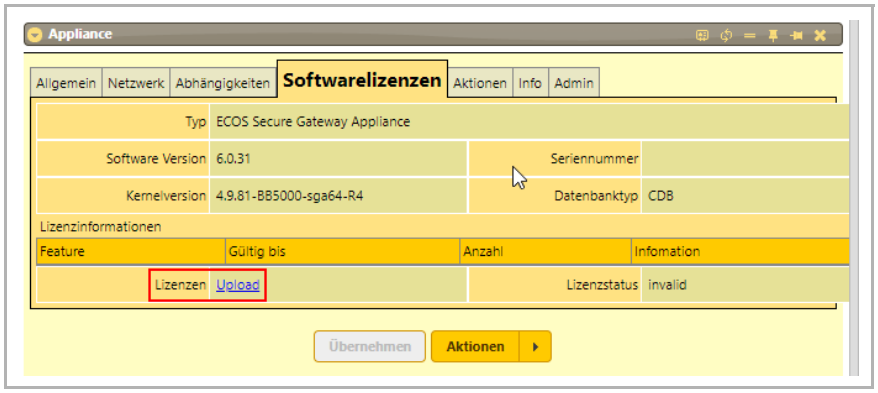
Dabei erscheint zunächst ein Anmeldefenster. Im Auslieferungszustand erfolgt die Authentifizierung als Benutzer **» admin «** mit dem Kennwort **» bb5000 «**. Bei erfolgreicher Authentifizierung öffnet sich die Administrationsoberfläche.



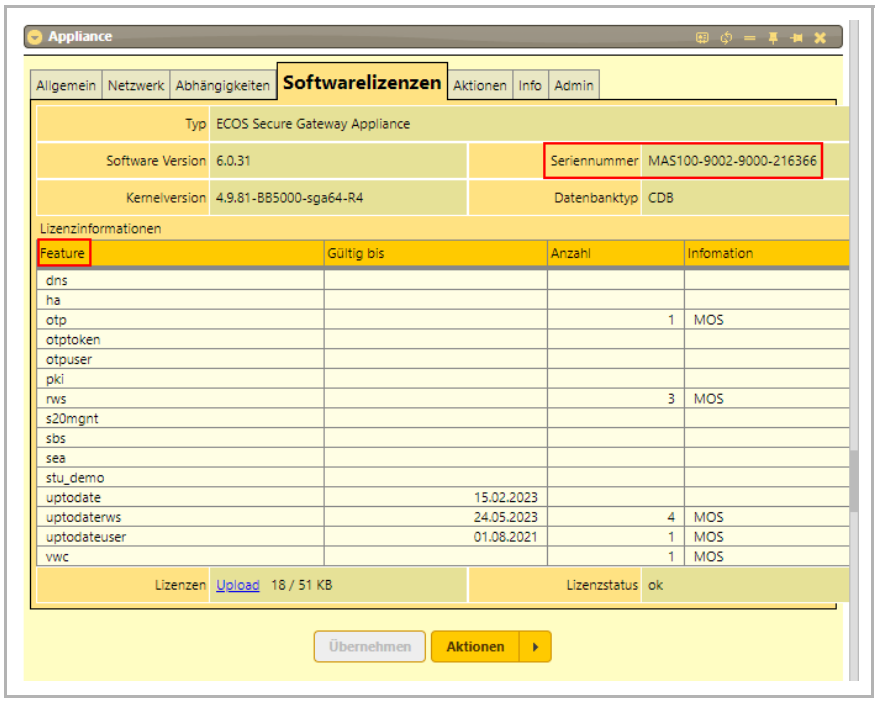
Zur vollständigen Nutzung der Appliance ist es notwendig über das Webinterface die Lizenzen im Konfigurationsobjekt der Appliance hochzuladen.

1.4 Lizenzen der Appliance hochladen

Nach der Installation und ersten Anmeldung müssen die Lizenzen in die Appliance eingespielt werden, um die Features der Appliance freizuschalten. Dazu auf der linken Seite in der Baumansicht auf **» Appliance «** klicken und danach in der Registerkarte **» Softwarelizenzen «** unter **» Lizenzen «** auf **» Upload «** klicken und die Lizenzdatei mit den initialen Lizenzen hochladen.



Nach dem Hochladen der Lizenzen werden die Seriennummer und die freigeschalteten Features angezeigt. Die initialen Lizenzen können nur hochgeladen werden, solange die Appliance noch keine Seriennummer hat.



1.5 Sicherheitsaspekte

Auf der Appliance werden für den Betrieb der ECOS Secure Boot Sticks (SBS) sensitive Informationen und Authentisierungsmerkmale sowie Konfigurationen angelegt und administriert, die für den sicheren Betrieb im Netzwerk von zentraler Bedeutung sind, um Missbrauch zu verhindern und den Schutz der mittels SBS zugreifbaren Daten zu gewährleisten.

Für den Betrieb der SMA sollten daher folgende Sicherheitsaspekte bereits mit der Installation berücksichtigt werden:

- Die SMA sollte in einem geeignet abgesicherten Netzwerk betrieben werden, um die SMA nicht als attraktives Angriffsziel in einem öffentlichen Raum zu exponieren.
- Die SMA sollte nur für autorisiertes, geschultes Personal zugänglich sein.
- Die Administration der SMA sollte von autorisiertem, geschultem Personal

durchgeführt werden, das umfängliche Kenntnisse der gegebenen Netzwerkinfrastruktur und der technischen Sicherheitseinrichtungen (Topologie, Routing, Firewalls, VPN-Gateways, AD- und/oder RADIUS-Server, etc.) besitzt.

- Sowohl für die Benutzer im mobilen Einsatz bzw. Home Office als auch für Administratoren zwecks Fernwartung ist ein sicherer Zugangsweg zur SMA via VPN erforderlich.
- Backups sind sicher und nur für autorisiertes Personal zugänglich aufzubewahren.
- Nach erfolgter Installation muss das Standardkennwort für den Zugriff auf die Konfigurationsoberfläche der SMA geändert werden.

Zur Absicherung der Verfügbarkeit kann die SMA als HA-Lösung im Cluster betrieben werden. → *Siehe „11 | Hochverfügbarkeit (High Availability)" auf Seite 147*

Bei geeigneter Installation (→ *Siehe „1.6 | Installationsvarianten" auf Seite 13*) und unter Berücksichtigung der Netzwerktopologie kann der SBS mithilfe der SMA ein sicheres, umgebendes Netzwerk mittels der Funktion Trusted Network Detection (TND) identifizieren. → *Siehe „9.4.3 | Trusted Network Detection (TND)" auf Seite 122*.

Dies ermöglicht einen durchgängigen Einsatz des SBS in unterschiedlichen Netzwerksegmenten bei gleichzeitiger Aufrechterhaltung einer sicheren Kommunikation.

Eine Voraussetzung für den Einsatz der TND-Funktion ist dabei, dass die SMA nur innerhalb des sicheren, umgebenden Netzwerks bzw. über eine VPN-Verbindung erreichbar ist.

Hinweis: Im VS-NfD-Umfeld wird es spätestens ab 2026 notwendig sein, dass nach der Installation Zugriff auf eine Smartcard oder ein HSM besteht. Grund dafür ist das Update auf einen neueren Kernel, der einen BSI-konformen Zufallszahlengenerator nicht mehr unterstützt. Daher wird ein zusätzlicher Zufallszahlengenerator aus einer zuverlässigen Quelle benötigt, z.B. einer Smartcard mit CardOS 5.4 oder höher.

1.6 Installationsvarianten

Eine SMA nimmt bei einer kompakten Installation als einzelne Instanz unterschiedliche Rollen wahr:

- Management-Server: als zentrale Autorität zum Management des Gesamtsystems
- Easy Enrollment-Server: als Anlaufstelle zur Durchführung der Personalisierung von SBS und MOS
- Software-Update-Server: zur Bereitstellung von Software-Updates
- TND-Proxy (optional): als Signalgeber zur Erkennung eines umgebenden, sicheren Netzwerks

Diese können alternativ zum Betrieb als einzelne Instanz der SMA auch auf unterschiedliche Instanzen verteilt werden. Hierbei kommt jeweils eine SMA in unterschiedlicher Konfiguration für den jeweiligen Zweck zum Einsatz. Dadurch kann die Installation flexibel auf die infolge der Netzwerktopologie gegebenen Vorbedingungen und geltenden Sicherheitsanforderungen angepasst werden.

Ebenso ist es möglich, eine Hochverfügbarkeit (HA) mit zwei oder mehr Instanzen herzustellen. Diese werden dabei als sog. **» vollsynchronisierte Slaves «** angelegt und können als passive Standby-Systeme oder als aktive SMAs im sog. **» Multi-Master «-**Betrieb eingesetzt werden. → *Siehe „11 | Hochverfügbarkeit (High Availability)" auf Seite 147*

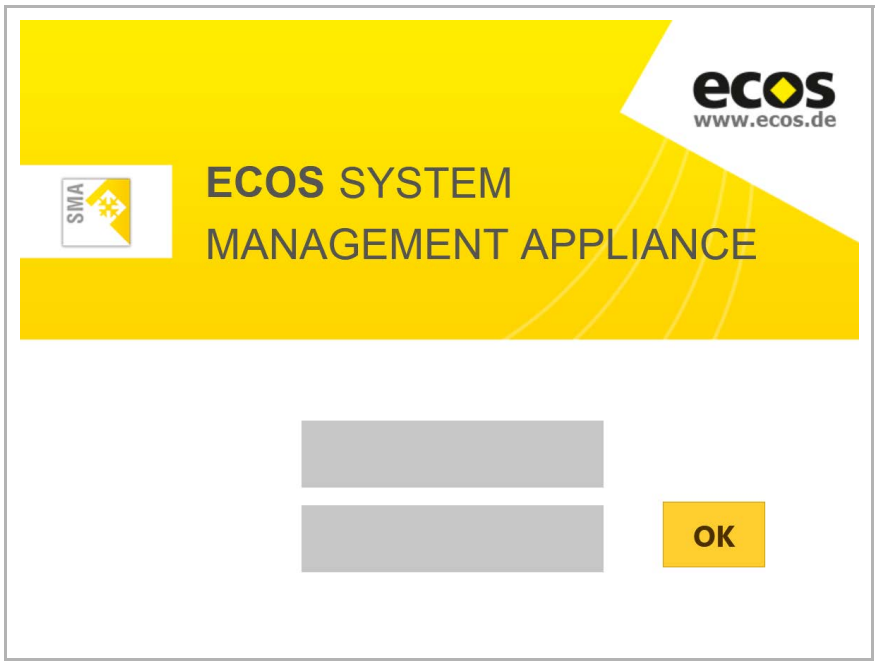
In allen Varianten spielt die Management-Verbindung eine gleichermaßen zentrale Rolle, da hierüber die erforderliche Kommunikation der SMAs untereinander abgewickelt wird. Daraus resultiert ein durchgängiges Verfahren, das sowohl zwischen den beteiligten SMAs als auch zwischen SMA und SBS eingesetzt wird. Eine sichere, gegenseitige Authentifizierung wird dabei ebenso konsistent durchgesetzt wie eine sichere Verschlüsselung der übertragenen Information in der Netzwerkkommunikation.

2 Aufbau der Administrationsoberfläche

2.1 Anmeldung

Der Zugriff auf die Administrationsoberfläche erfolgt mittels Webbrowser. Der Aufruf erfolgt über HTTPS auf Port 543.

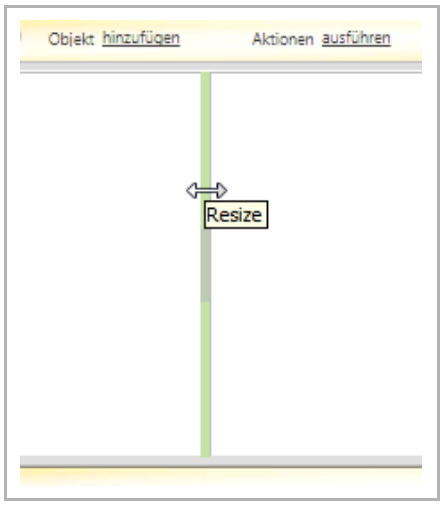
→ *Siehe „1.3 | Anmeldung" auf Seite 10*.



2.2 Bereiche der Administrationsoberfläche anpassen

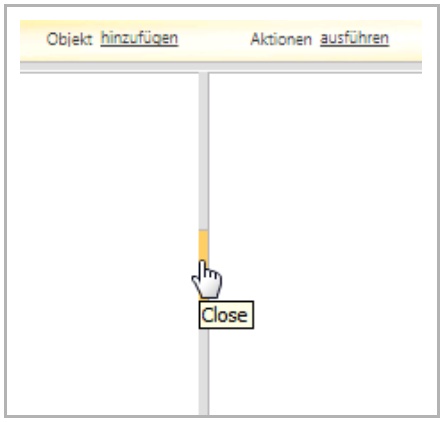
Die Administrationsoberfläche setzt sich aus drei Bereichen und jeweils einer Leiste oben und unten zusammen. Oben befindet sich die Menüleiste, links die Baumansicht, unten die Informationsleiste und in der Mitte der Bereich für die Konfigurationsobjekte. Die einzelnen Bereiche werden im Folgenden näher beschrieben.

Die einzelnen Bereiche sind durch graue Trennlinien voneinander abgegrenzt. Durch Fahren mit dem Maus-Zeiger über die Trennlinie erscheint ein Doppelpfeil.



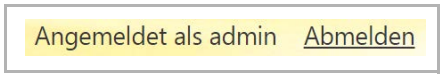
Durch Drücken der linken Maustaste und Ziehen des Mauszeigers nach links oder rechts, lässt sich die Größe der Bereiche einstellen.

Ein Klick auf den dunkleren Bereich in der Mitte der Trennlinie schließt den jeweiligen Bereich komplett. Die Trennlinie verschiebt sich dabei ganz an den Rand. Ein erneutes Klicken auf den dunkelgrauen Bereich der Trennlinie öffnet den Bereich wieder.



2.3 Informationsleiste

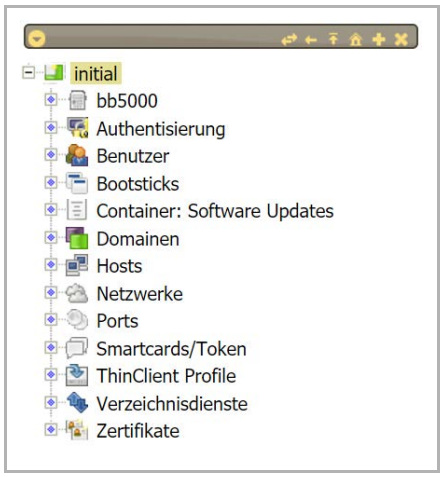
In der Leiste am unteren Rand befindet sich der Hinweis **» angemeldet als «**, der den jeweils angemeldeten Benutzer identifiziert. Ein Klick auf **» Abmelden «** meldet den Benutzer ab und lässt ihn zum Anmeldefenster zurückkehren.



Im linken Bereich befindet sich ein Baum, in dem vorhandene Konfigurationsobjekte hierarchisch angeordnet sind. Durch Klicken auf eines der Konfigurationsobjekte, öffnet sich das Formular des Konfigurationsobjekts im mittleren Bereich der Konfigurationsoberfläche. Hier kann die Einstellung des Objektes angepasst werden.

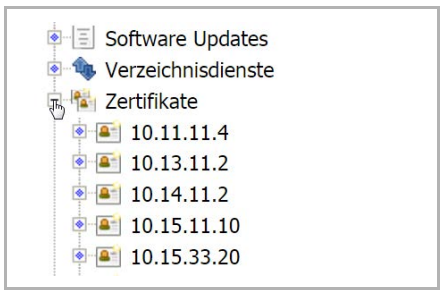
2.4 Baum / Konfigurationsobjekte

Jede Konfiguration erfolgt durch Konfigurationsobjekte, welche die eigentlichen Einstellungen enthalten und hierarchisch im Baum auf der linken Seite angeordnet sind. Ein Minimum an Konfigurationsobjekten wird bereits während der Installation angelegt. Diese Objekte können jederzeit nachträglich geändert oder, soweit sie nicht mehr benötigt werden, gelöscht werden. Ebenso können neue Objekte angelegt werden, um weitergehende Funktionen zu konfigurieren. Während manche Objekte überall im Baum angelegt werden können, gibt es für die meisten Objekte einen festen Ort/Container, wo diese hinzugefügt werden müssen.



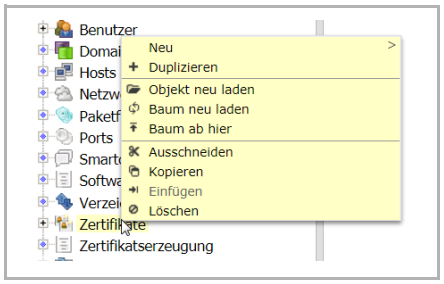
2.4.1 Untergeordnete Objekte im Baum ein- und ausblenden

Durch Klicken auf **» + «** neben den Konfigurationsobjekten werden untergeordnete Objekte angezeigt. Ein Klicken auf **» - «** schließt die Ansicht der Teilbäume wieder.



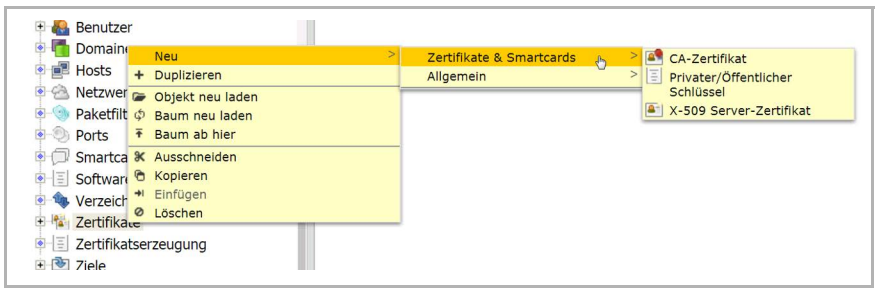
2.4.2 Kontext-Menü

Ein Rechtsklick auf ein Konfigurationsobjekt im Baum öffnet ein Kontextmenü mit folgenden Optionen: **» Neu «**, **» Duplizieren «**, **» Dokument neu laden «**, **» Baum neu laden «**, **» Baum ab hier «**, **» Ausschneiden «**, **» Kopieren «**, **» Einfügen «** und **» Löschen «**.



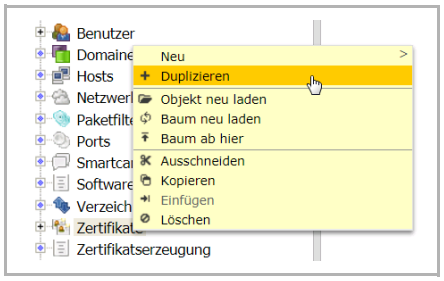
2.4.2.1 Neu

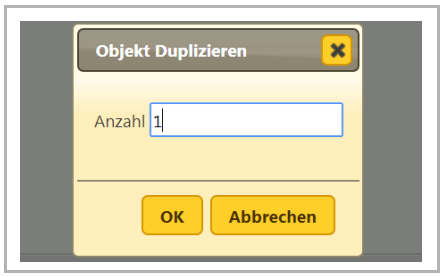
Unter dem Punkt **» Neu «** lassen sich dem ausgewählten Konfigurationsobjekt untergeordnete Konfigurationsobjekte erstellen. Es werden nur Objekte angezeigt, die an dieser Position angelegt werden können. Manche Konfigurationsobjekte können nur einmal angelegt werden. Ist ein solches bereits vorhanden, wird es nicht mehr unter **» Neu «** angezeigt. Nach Auswahl eines zu erstellenden Objektes öffnet sich das dazugehörige Formular im mittleren Bereich. Das neue Objekt wird nach Eingabe der gewünschten Parameter des Objektes durch Klicken auf die Schaltfläche **» Anlegen «** gespeichert.



2.4.2.2 Duplizieren

Durch Klicken auf **» Duplizieren «** erscheint ein Fenster, in dem angegeben werden kann, wie oft das ausgewählte Konfigurationsobjekt dupliziert werden soll. Durch Klicken auf die Schaltfläche **» OK «** werden entsprechend viele Konfigurationsobjekte angelegt. Die duplizierten Konfigurationsobjekte haben dieselben Parameter und Einstellungen wie das als Vorlage dienende Objekt. Die Duplikate werden im Namen automatisch durchnummeriert. Die Schaltfläche **» Abbrechen «** lässt die Aktion beenden, ohne das ausgewählte Objekt zu duplizieren.





2.4.2.3 Objekt neu laden

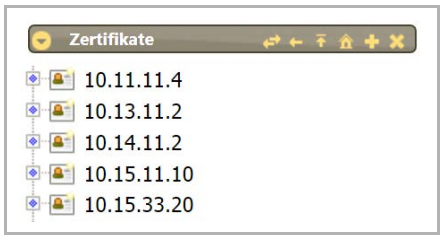
Das ausgewählte Konfigurationsobjekt wird neu geladen.

2.4.2.4 Baum neu laden

Der untergeordnete Baum wird neu geladen.

2.4.2.5 Baum ab hier

Hier wird nicht mehr der gesamte Baum, sondern lediglich der Teilbaum ab dem ausgewählten Konfigurationsobjekt angezeigt. Klicken auf das Haus-Symbol in der Menüleiste des Baumes ermöglicht den Wechsel zurück zur Gesamtansicht des Baumes.



2.4.2.6 Ausschneiden

Das ausgewählte Konfigurationsobjekt wird ausgeschnitten und kann an anderer Stelle über die Funktion **» Einfügen «** wieder eingefügt werden.

2.4.2.7 Kopieren

Das ausgewählte Konfigurationsobjekt wird kopiert und im Zwischenspeicher hinterlegt.

2.4.2.8 Einfügen

Ein zuvor ausgeschnittenes oder kopiertes Konfigurationsobjekt wird an der ausgewählten Stelle eingefügt.

2.4.2.9 Löschen

Das ausgewählte Konfigurationsobjekt wird gelöscht.

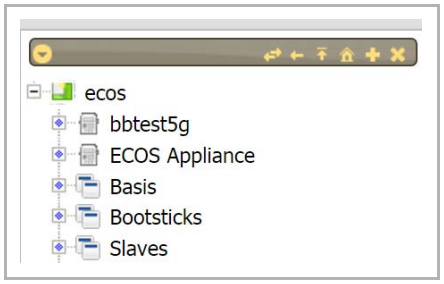
2.4.3 Verschieben und Kopieren von Objekten im Baum mit Drag-and-Drop

Klicken auf ein Konfigurationsobjekt im Baum und gleichzeitiges Gedrückthalten der linken Maustaste ermöglicht das Verschieben des ausgewählten Konfigurationsobjektes innerhalb des Baumes mittels Drag-and-Drop. Dabei wird das ausgewählte Objekt unterhalb des Konfigurationsobjektes angelegt, auf das man es zieht. Darf das ausgewählte Objekt nicht unter dem Konfigurationsobjekt, auf welches es gezogen wurde, positioniert werden, wird es automatisch am nächstgelegenen zugelassenen Ort angelegt. Ein grüner Haken erscheint, sobald man sich mit dem Maus-Zeiger an einer Stelle im Baum befindet, an die das ausgewählte Konfi-

gurationsobjekt verschoben werden darf. Hält man zusätzlich zu der linken Maustaste die Strg-Taste gedrückt, wird das ausgewählte Konfigurationsobjekt kopiert statt verschoben.

2.4.4 Menüleiste des Baums

Der Baum besitzt eine eigene Menüleiste. Durch Klicken auf den Pfeil links in der Menüleiste kann der Baum ein- und ausgeblendet werden. Außerdem befinden sich rechts in der Menüleiste die Optionen: **»Synchronisation mit Dokument ein/aus«**, **» Jetzt mit Dokument synchronisieren «**, **» Baum ab aktuellem Dokument «**, **» Gesamten Baum anzeigen «**, **» Weiteren Baum anzeigen «** und **» Baum schließen «**.



2.4.4.1 Synchronisation mit Dokument an/aus

Ist die Funktion **» Synchronisation mit Dokument an/aus «** ( ) aktiviert, wird der Pfad des aktuell geöffneten Konfigurationsobjektes im Baum automatisch angezeigt. Sind mehrere Konfigurationsobjekte geöffnet, zeigt der Baum immer den Pfad des zuletzt geöffneten bzw. aktualisierten Konfigurationsobjektes an. Das Symbol zeigt an, dass die Funktion deaktiviert ist.

2.4.4.2 Jetzt mit Dokument synchronisieren

Durch Klicken auf das Symbol öffnet sich der Pfad des aktuell geöffneten Konfigurationsobjektes im Baum.

2.4.4.3 Baum ab aktuellem Dokument

Mithilfe dieser Funktion lassen sich Teilbäume separat anzeigen. Ein Klick auf das Symbol zeigt nur noch den Teilbaum ab dem aktuell geöffneten Konfigurationsobjekt an. Klicken auf das Haus-Symbol ( ) ermöglicht den Wechsel zurück zur Gesamtansicht des Baumes.

2.4.4.4 Weiteren Baum anzeigen

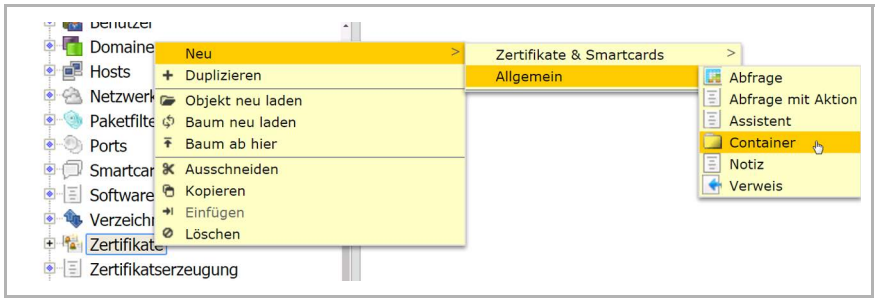
Durch Klicken auf das Plus-Symbol + wird ein weiterer Baum geöffnet. Dieser wird unter dem schon vorhandenen Baum angezeigt.

2.4.4.5 Schließen

Zusätzlich erzeugte Bäume können mithilfe des Kreuz-Symbols ✖ wieder geschlossen werden. Gibt es nur einen einzelnen Baum, kann dieser nicht geschlossen werden. Er kann lediglich mit dem Pfeil-Symbol links in der Menüleiste des Baumes oder durch Klicken auf den dunkelgrauen Bereich der Trennlinie des linken Bereiches minimiert werden.

2.4.5 Organisieren von Objekten

Zur besseren Übersicht können Konfigurationsobjekte immer auch in Containern (vergleichbar mit Ordnern im Dateisystem) organisiert werden. Container können an jeder Stelle im Baum angelegt werden und Objekte können jederzeit in oder zwischen Container verschoben werden. Dies hat keine Auswirkung auf die eigentliche Konfiguration.



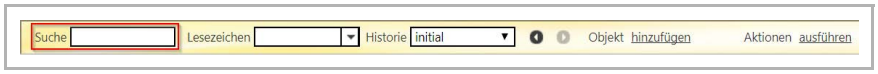
Container können aber auch dazu genutzt werden um Gruppen zu bilden. So können mehrere Konfigurationsobjekte in einem Container angelegt werden und später kann an anderer Stelle, statt der einzelnen Konfigurationsobjekte, der gesamte Container ausgewählt werden.

2.5 Menüleiste

In der Menüleiste am oberen Rand befinden sich die Schaltflächen **» Suche «**, **» Lesezeichen «**, **» Historie «**, **» Objekt hinzufügen «** und **» Aktionen ausführen «** sowie die Felder **» vor «** und **» zurück «** in Form von Pfeilen.

2.5.1 Suchen

Bei Eingabe eines Suchbegriffs in das Feld **» Suchen «**, erscheint ein Kontextmenü mit Konfigurationsobjekten, die den Suchbegriff im Namen enthalten. Es müssen mindestens drei Buchstaben in das Suchfeld eingegeben werden. Es werden nur Ergebnisse angezeigt, bei denen sich die gesuchte Buchstabenkombination an einem Wortanfang im Namen befindet. Es können auch mehrere Suchbegriffe, durch Leerzeichen getrennt, eingegeben werden. Das Leerzeichen steht für eine UND-Verknüpfung. Bei dieser Eingabe werden nur Konfigurationsobjekte angezeigt, die sämtliche Suchbegriffe im Namen enthalten. Dabei gilt die Regelung, dass sich die Buchstabenkombination am Anfang eines Wortes befinden muss, nur für den ersten Suchbegriff. Durch Klicken auf den Namen des gewünschten Konfigurationsobjektes, wird dieses im mittleren Bereich geöffnet. Außerdem öffnet sich der Pfad, unter dem das Konfigurationsobjekt liegt, im Baum im linken Bereich.



2.5.2 Lesezeichen

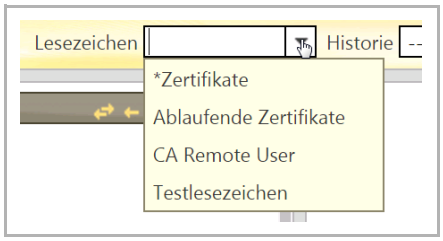
Durch Klicken auf den Pfeil rechts neben dem Feld **» Lesezeichen «** öffnet sich ein Kontextmenü mit sämtlichen angelegten Lesezeichen.

Lesezeichen können über die Menüleiste der Konfigurationsobjekte unter **» Ansicht speichern «** oder über die Schaltfläche **» Aktionen «** unter den Konfigurationsobjekten angelegt werden.

→ *Siehe „2.6.2.1 | Ansicht speichern" auf Seite 28.*

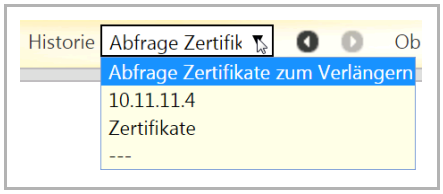
Ganze Seiten, die als Lesezeichen gespeichert wurden, sind mit einem * vor dem Namen gekennzeichnet. Namen ohne * beziehen sich auf einzelne Objekte. Durch Auswahl eines der Lesezeichen, öffnet sich das entsprechende Konfigurationsobjekt bzw. die ganze Seite mit mehreren Konfigurationsobjekten.

Anstatt das Kontextmenü durch Klicken auf den Pfeil rechts neben dem Feld zu öffnen, können Lesezeichen anhand ihres Namens durch Eingabe von Suchbegriffen in das Feld gezielt gesucht werden.



2.5.3 Historie

Klicken auf den Pfeil im Feld **» Historie «** öffnet ein Auswahl-Menü, das die zuletzt geöffneten Konfigurationsobjekte auflistet. Klicken auf eines der Konfigurationsobjekte öffnet dieses im mittleren Bereich.



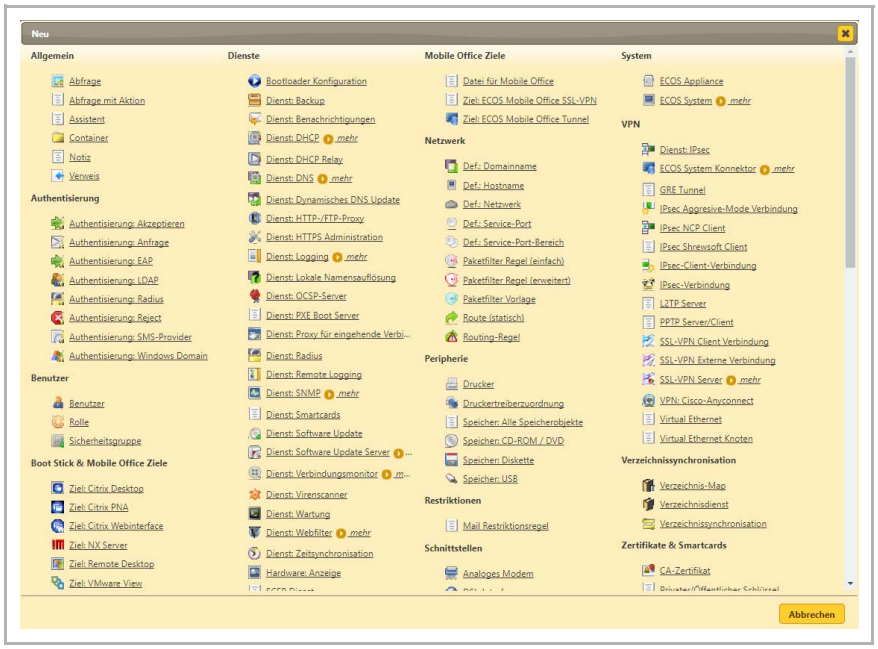
2.5.4 Vor und zurück

Rechts neben dem Feld **» Historie «** befinden sich zwei Pfeile . Ein Klick auf den Pfeil nach links wechselt zum vorher geöffneten Konfigurationsobjekt. Ein Klick auf den Pfeil nach rechts öffnet das Konfigurationsobjekt danach.

2.5.5 Objekt hinzufügen

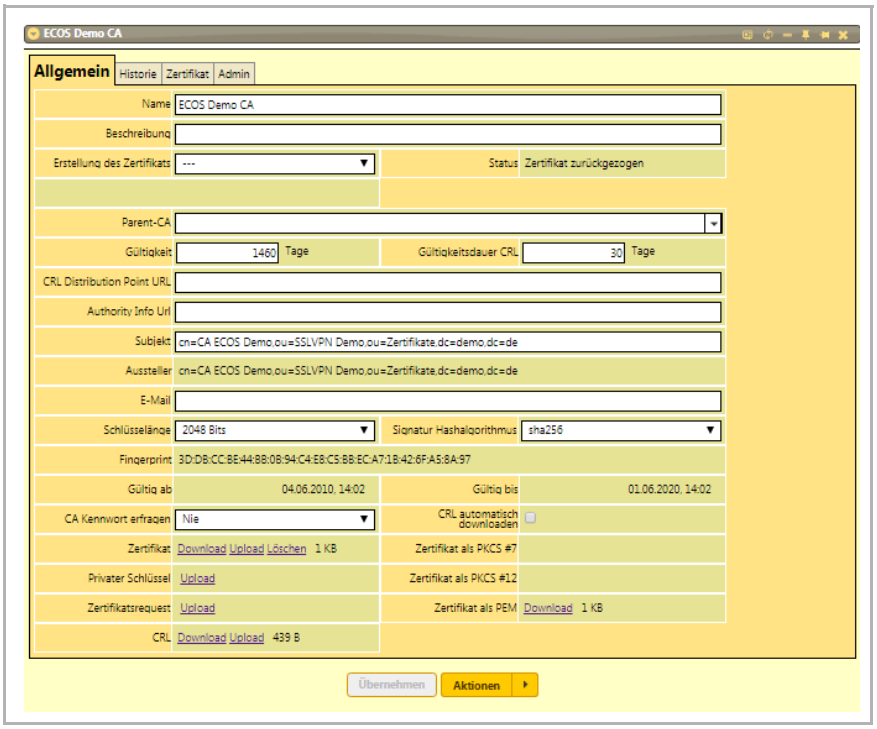
Klicken auf die Schaltfläche **» Objekt hinzufügen «** öffnet ein Dialogfenster, in dem sämtliche Konfigurationsobjekte aufgelistet sind, die angelegt werden können. Die Konfigurationsobjekte sind dabei nach Kategorien sortiert. Ein Pfeil mit dem Hinweis **» mehr «** neben einem Konfigurationsobjekt zeigt an, dass untergeordnete Objekte vorhanden sind. Klicken auf **» mehr «** zeigt diese an.

Ein Klick auf das gewünschte Konfigurationsobjekt öffnet das Formular für das entsprechende Objekt, in dem sämtliche nötigen Eingaben gemacht werden können. Anschließend wird das neue Objekt mittels **» Anlegen «** gespeichert. Dabei wird das Konfigurationsobjekt automatisch im Baum an der ersten Stelle angelegt, an der es angelegt werden darf.



2.6 Konfigurationsobjekte

Durch Klicken auf ein Konfigurationsobjekt im Baum, öffnet sich dieses im mittleren Bereich. Das Objekt besteht aus einer eigenen Menüleiste oben und dem eigentlichen Formular mit den Schaltflächen **» Übernehmen «** und **» Aktionen «**. Ein Klick auf die Schaltfläche **» Übernehmen «** speichert die im Formular des Konfigurationsobjektes getätigten oder veränderten Eingaben ab. Schließen des Konfigurationsobjektes ohne auf **» Übernehmen «** zu klicken, löst eine Warnung mit zwingender Entscheidung zur Übernahme oder dem Verwerfen der getätigten Änderung aus.



2.6.1 Aktionen

Klicken auf die Schaltfläche **» Aktionen «** öffnet ein Kontextmenü, in dem diverse Aktionen für das Konfigurationsobjekt ausgewählt werden können. Das gleiche Kontextmenü öffnet sich durch Rechtsklick auf die Menüleiste des Konfigurationsobjektes. Die Auswahl der Aktionen überschneidet sich mit der, die im Kontextmenü des Baumes zur Verfügung steht.

2.6.1.1 Gleiches Objekt erstellen

Durch Klicken auf die Aktion **» Gleiches Objekt erstellen «** öffnet sich ein Formular desselben Konfigurationsobjekttyps. Dabei sind die Felder bereits mit den Werten des aktuellen Konfigurationsobjektes gefüllt. Nach Eingabe der gewünschten Parameter des Objektes wird durch Klicken auf die Schaltfläche **» Anlegen «** ein neues Konfigurationsobjekt des gleichen Typs angelegt und gespeichert.

Erläuterungen zu **» Duplizieren «**, **» Neu «**, **» Objekt neu laden «**, **» Ausschneiden «**, **» Kopieren «**, **» Einfügen «** und **» Löschen «** → *Siehe „2.4.2 | Kontext-Menü" auf Seite 18.*

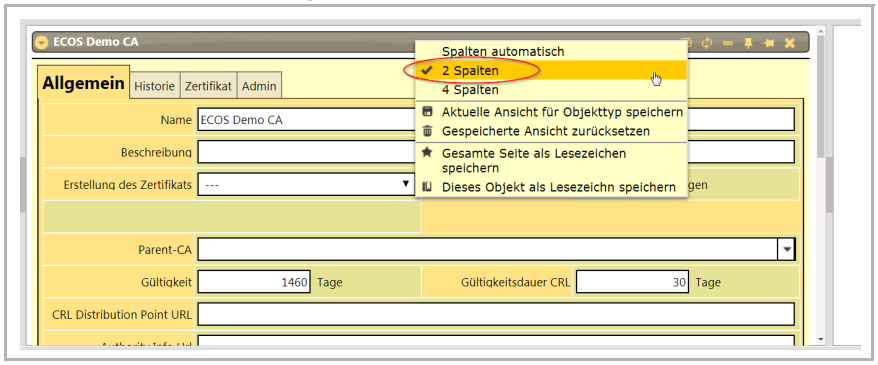
Erläuterungen zu » **Ansicht** «, » **Im Hauptfenster festpinnen** «, » **Im rechten Fenster festpinnen** «, und » **Schließen** « → *Siehe „2.6.2.4 | Im Hauptfenster festpinnen" auf Seite 30*.

2.6.2 Menüleiste Konfigurationsobjekt

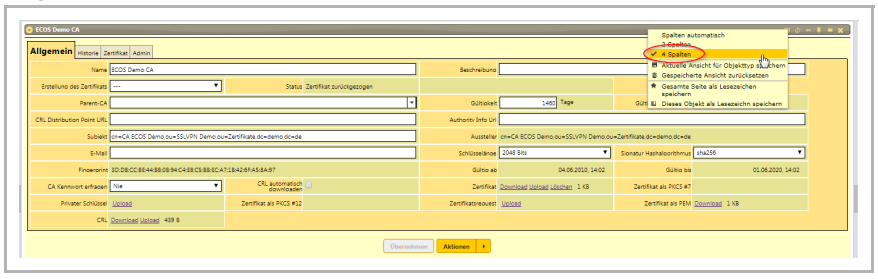
Links in der Menüleiste befindet sich ein Pfeil, über den das Formular aus- und eingeklappt werden kann. Rechts in der Menüleiste befinden sich Symbole für » **Ansicht speichern** «, » **Aktualisieren** «, » **Untereinander anzeigen** «, » **Im Hauptfenster festpinnen** «, » **Im rechten Fenster festpinnen** « und » **Schließen** «.

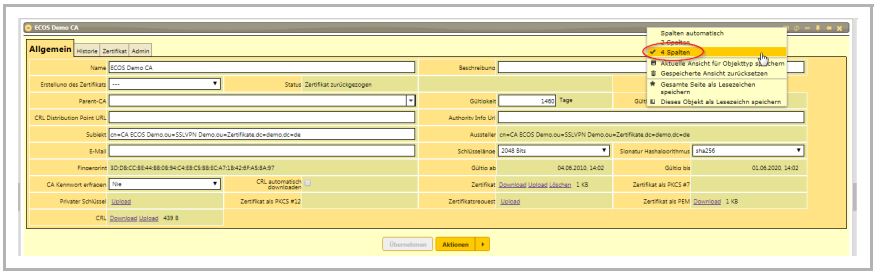
2.6.2.1 Ansicht speichern

Ein Klick auf das Symbol » **Ansicht** « öffnet ein Auswahl-Menü mit den Optionen » **Spalten automatisch** «, » **2 Spalten** «, » **4 Spalten** «, » **Aktuelle Ansicht für Objekttyp speichern** «, » **Gespeicherte Ansicht zurücksetzen** «, » **Gesamte Seite als Lesezeichen speichern** « und » **Dieses Objekt als Lesezeichen speichern** «. Als Standard ist bei der Spaltenanzahl » **2** « ausgewählt. Die Auswahl » **Spalten automatisch** « passt sich die Spaltenanzahl, in der die Felder im Formular sortiert sind, automatisch an die Bereichsgröße an.



Bei der Auswahl » **4 Spalten** «, werden die Felder im Formular in vier Spalten angezeigt.





Klicken auf **» Aktuelle Ansicht für Objekttyp speichern «** speichert die aktuellen Anzeige-Einstellungen des Objekts und zukünftig werden für jedes Konfigurationsobjekt desselben Typs diese Anzeige-Einstellungen verwendet. Zu den gespeicherten Einstellungen gehören neben der Spaltenanzahl auch sämtliche Einstellungen, die in eventuell vorhandenen Tabellen gemacht wurden, wie zum Beispiel Spaltenbreite in der Tabelle, oder Sortierungen.

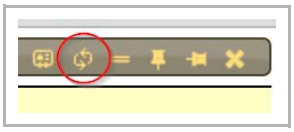
Mithilfe der Option **» Gespeicherte Ansicht zurücksetzen «** werden gespeicherte Einstellungen für die Ansicht des Objekttyps wieder gelöscht. Konfigurationsobjekte desselben Typs werden daraufhin wieder mit den Standardeinstellungen angezeigt.

Klicken auf **» Gesamte Seite als Lesezeichen speichern «** speichert sämtliche geöffneten Konfigurationsobjekte in der aktuellen Ansicht inkl. der Baumansicht. In dem sich öffnenden Fenster muss dem Lesezeichen ein Name gegeben und mittels **» OK «** bestätigt werden.

Klicken auf **» Dieses Objekt als Lesezeichen speichern «** speichert lediglich das ausgewählte Konfigurationsobjekt inklusive aller Einstellungen, welche die Ansicht betreffen, als Lesezeichen. Auch hier öffnet sich ein Fenster, in dem der Name für das Lesezeichen festgelegt wird → *Siehe „2.5.2 | Lesezeichen" auf Seite 24*.

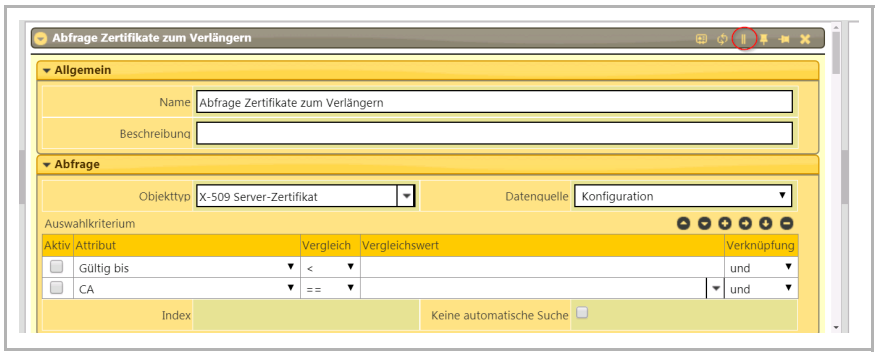
2.6.2.2 Aktualisieren

Klicken auf das Symbol mit den zwei Pfeilen lädt das Konfigurationsobjekt neu.



2.6.2.3 Untereinander anzeigen

Klicken auf das Symbol mit den zwei waagerechten Stichen = zeigt die Registerkarten des Konfigurationsobjektes untereinander an. In dieser Ansicht lässt sich die Reihenfolge der Registerkarten durch gedrückt-Halten der linken Maustaste und Verschieben verändern. Ein erneutes Klicken auf das Symbol ⏸ lässt wieder zur Registerkarten-Ansicht zurückkehren.



2.6.2.4 Im Hauptfenster festpinnen

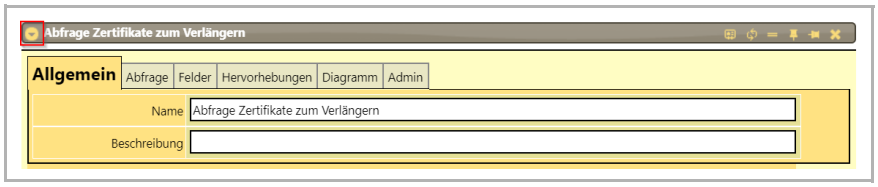
Klicken auf das Symbol mit dem senkrecht stehenden Pin 📌 pinnt das Konfigurationsobjekt im mittleren Bereich fest. Wird ein anderes Konfigurationsobjekt geöffnet, bleibt das festgepinnte Objekt weiterhin geöffnet und ist unter dem neu geöffneten Objekt platziert.

2.6.2.5 Im rechten Fenster festpinnen

Klicken auf das Symbol mit dem waagerecht stehenden Pin 📌 verschiebt das Konfigurationsobjekt in den rechten Bereich. Beim Verschieben weiterer Objekte in den rechten Bereich befindet sich das neueste Objekt immer zuoberst.

2.6.2.6 Konfigurationsobjekt ein-/ausblenden

Klicken auf den Pfeil in der jeweiligen Menüleiste der Konfigurationsobjekte klappt die Objekte ein und aus.

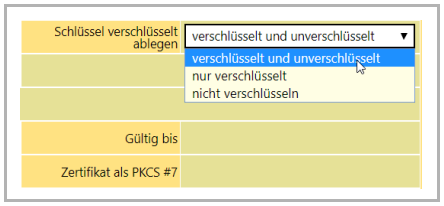


2.6.2.7 Schließen

Klicken auf das Kreuz-Symbol ✖ schließt das Konfigurationsobjekt.

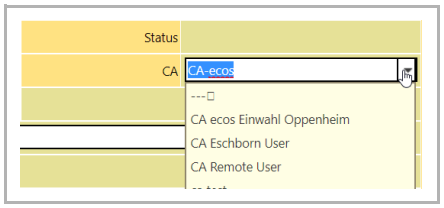
2.6.3 Auswahlboxen

Auswahlboxen können sich auf feste Größen beziehen, wie zum Beispiel bei Schlüssellänge, oder auf andere Konfigurationsobjekte, wie zum Beispiel bei CA. Im letzteren Fall ändert sich die Auswahl, je nachdem welche Konfigurationsobjekte dieses Typs angelegt wurden. Wie bei den normalen Auswahlboxen lässt sich die Auswahl durch Klicken auf den Pfeil anzeigen. Des Weiteren kann auch ein Suchbegriff in das Feld eingegeben werden → *Siehe „2.5.1 | Suchen" auf Seite 24*.

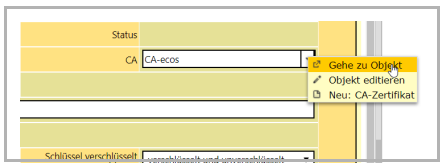


Wurde eine Auswahl getroffen, kann eine Zusammenfassung der wichtigsten Parameter des Objektes durch Fahren mit dem Maus-Zeiger über das Feld angezeigt werden. In dieser Ansicht können keine Änderungen an den Parametern vorgenommen werden. Für Änderungen muss das Konfigurationsobjekt selbst geöffnet werden.

.

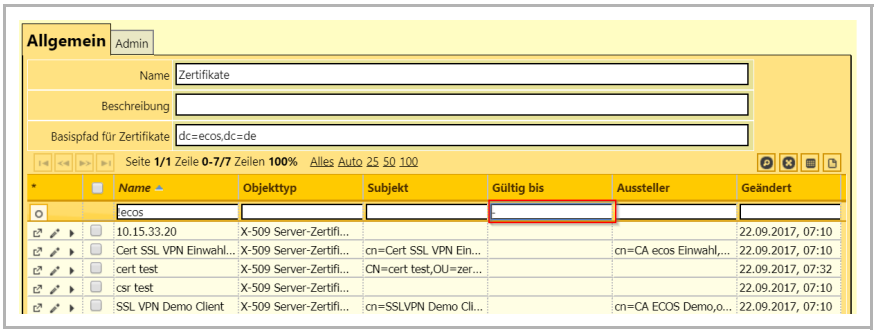


Ein Rechtsklick auf die getroffene Auswahl öffnet ein Menü mit den Optionen **» Gehe zu Objekt «**, **» Objekt editieren «** und **» Neu «** → *Siehe „2.6.4.10 | Die Aktionsspalte" auf Seite 38*.



Außerdem merkt sich die Auswahlbox die bis zu fünf zuletzt getroffenen Auswah-

len und stellt sie als Optionen im Schnellzugriff an den Anfang der Liste.



2.6.4 Tabellen

Viele übergeordnete Objekte enthalten eine Übersichtstabelle von unter ihnen angelegten Objekten. Ebenso finden sich Tabellen als Ergebnis von Abfragen.

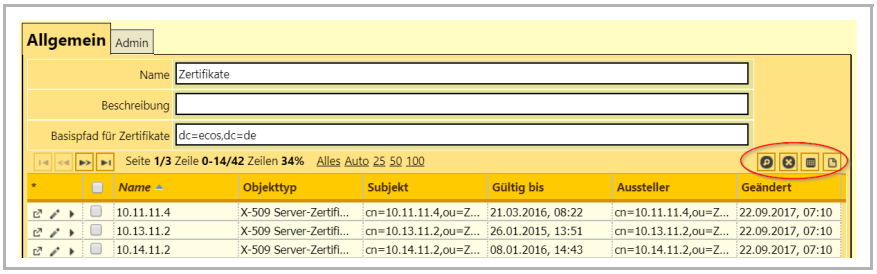
→ *Siehe „13.6 | Abfragen" auf Seite 173.*

2.6.4.1 Tabellen anpassen

Wird mit dem Maus-Zeiger im Tabellenkopf über die Trennlinien der einzelnen Spalten gefahren, erscheint ein Doppelpfeil. Durch gedrückt-Halten der Maustaste und entsprechendes Ziehen lässt sich die Spaltenbreite anpassen. Ein Klick in ein Feld des Tabellenkopfes und gleichzeitiges gedrückt-Halten der Maustaste, erlaubt das Ziehen und Versetzen der gesamten Spalte an eine andere Stelle innerhalb der Tabelle. Die Reihenfolge der Spalten kann so beliebig angepasst werden.

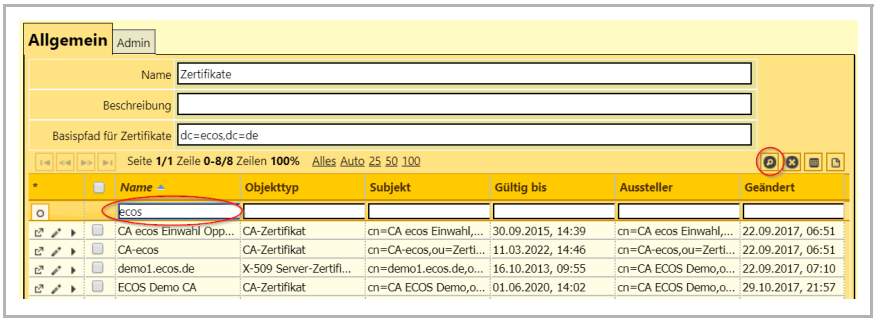
2.6.4.2 Menüleiste von Tabellen

Rechts über der Tabelle befinden sich fünf Symbole mit den Funktionen: **» Filter anzeigen «**, **» Filter entfernen «**, **» Dateiexport «** und **» Objekt hinzufügen «**.

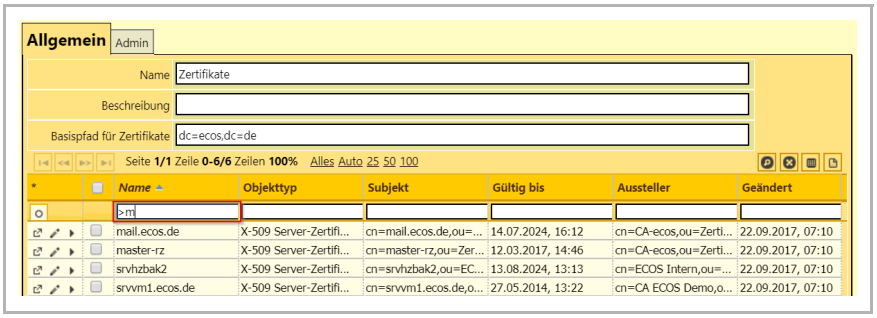


2.6.4.3 Verwendung von Filtern in Tabellen

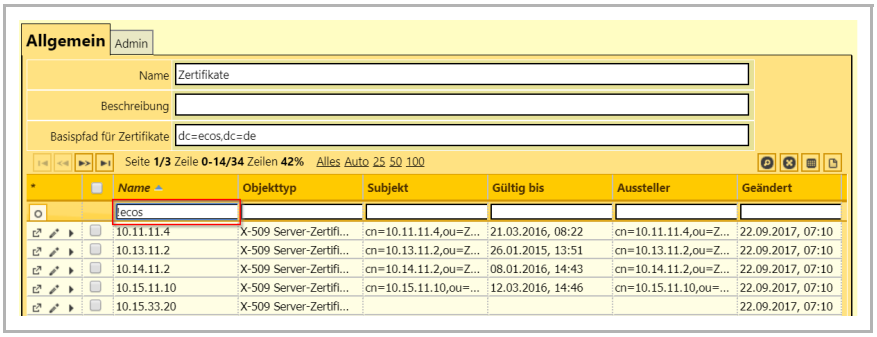
Klicken auf das Symbol lässt Suchfelder über den Spalten der Tabelle erscheinen. Durch Eingabe eines Suchbegriffs in eines der Suchfelder werden nur noch Objekte in der Tabelle angezeigt, die diesen Suchbegriff im Namen enthalten.



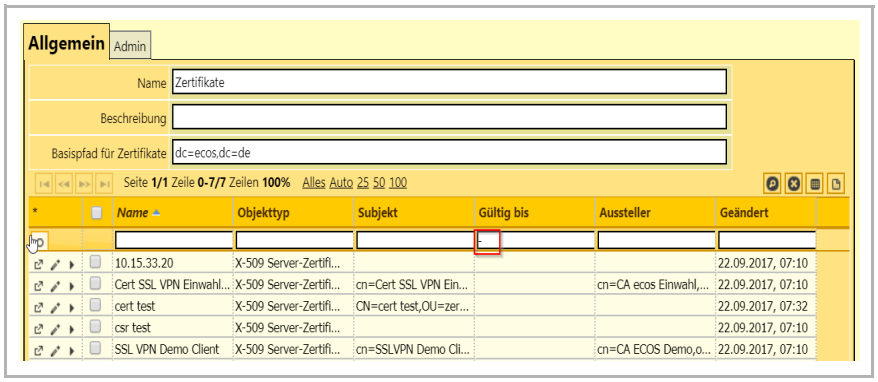
Mithilfe von **<** und **>** werden nur noch Objekte in der Tabelle angezeigt, die im jeweiligen Feld einen Wert größer bzw. kleiner als den Vergleichswert haben.



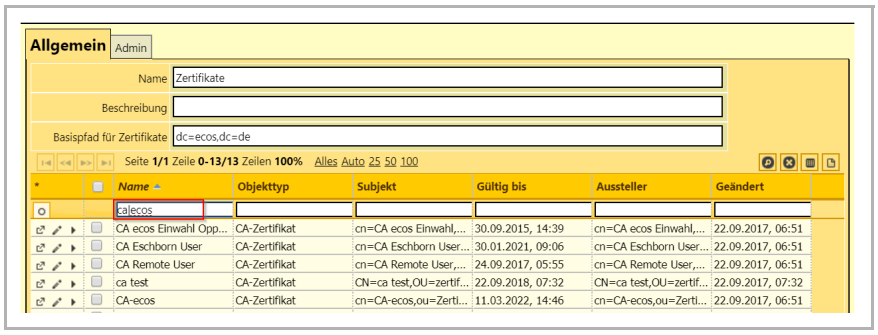
Durch Voranstellen eines Ausrufezeichens **»!«** vor den Suchbegriff, werden sämtliche Konfigurationsobjekte angezeigt, die diesen Begriff nicht im entsprechenden Feld stehen haben.



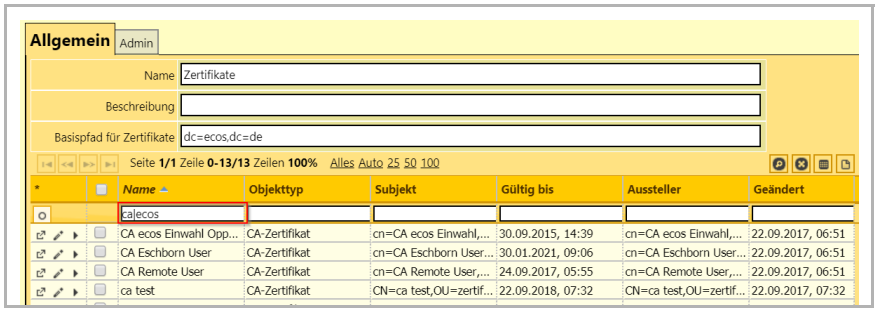
Durch Eingabe eines » * « in ein Suchfeld, werden sämtliche Objekte aufgelistet, bei denen irgendetwas im entsprechenden Feld steht. Durch Eingabe eines » - «, werden sämtliche Objekte aufgelistet, bei denen das entsprechende Feld leer ist.



Bei den Suchfeldern handelt es sich um reguläre Ausdrücke, die somit eine Vielzahl von Suchausdrücken zulassen. So lassen sich mithilfe der Eingabe » a|b « Objekte suchen, die entweder den Wert » a « oder » b « im entsprechenden Feld enthalten.



Eine weitere nützliche Eingabe im Suchfeld ist » a.*b «, die sämtliche Objekte anzeigt, die den Wert » a « gefolgt von dem Wert » b « im entsprechenden Feld enthalten, unabhängig von eventuellen Werten zwischen » a « und » b «.



Die Groß- und Kleinschreibung spielt dabei keine Rolle.

Zur Spezifizierung der Suche können Suchbegriffe in mehrere Suchfelder gleichzeitig eingegeben werden. Klicken auf das Symbol ✖ **» Filter entfernen «** setzt sämtliche Filter zurück, sodass wieder alle Konfigurationsobjekte in der Tabelle angezeigt werden. Durch erneutes Klicken auf das Symbol **» Filter anzeigen «** werden die Suchfelder ausgeblendet.

2.6.4.4 Dateiexport

Klicken auf das Symbol ▦ öffnet ein Auswahl-Menü, in dem zwischen den Dateitypen .xlsx und .csv ausgewählt werden kann. Nach Auswahl eines Dateityps wird die Tabelle entsprechend als Excel- bzw. Komma-Separierte-Datei exportiert und kann heruntergeladen werden.

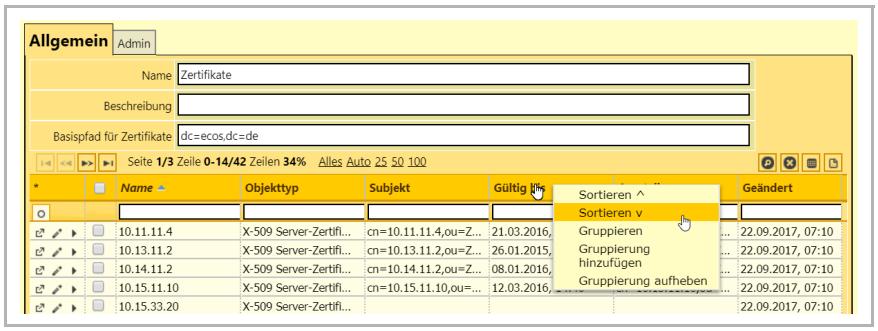
2.6.4.5 Objekt hinzufügen

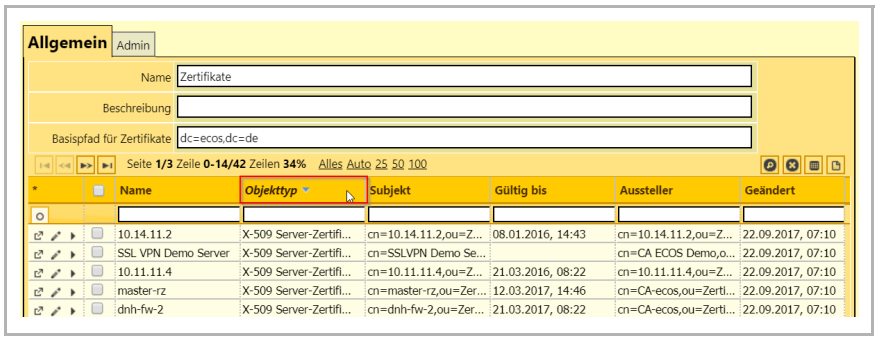
Klicken auf das Symbol 🗋 öffnet ein Auswahl-Menü, in dem sämtliche Konfigurationsobjekte aufgelistet sind, die unter dem Objekt angelegt werden können. Bei Auswahl des anzulegenden Konfigurationsobjektes öffnet sich das entsprechende Formular in einem neuen Fenster. Nach Eingabe aller gewünschten Eigenschaften wird das Objekt mittels Klick auf die **» OK «**-Schaltfläche angelegt.

2.6.4.6 Sortieren von Tabellen

Klicken auf die Überschriften im Tabellenkopf sortiert die Einträge der Tabelle nach dem entsprechenden Kriterium. Ein Pfeil neben der Überschrift zeigt an, nach welchem Kriterium die Tabelle aktuell sortiert ist und ob es sich um eine aufsteigende (Pfeil nach oben) bzw. absteigende (Pfeil nach unten) Sortierung handelt. Durch Rechtsklick auf ein Feld im Tabellenkopf erscheint ein Kontextmenü, das noch ein-

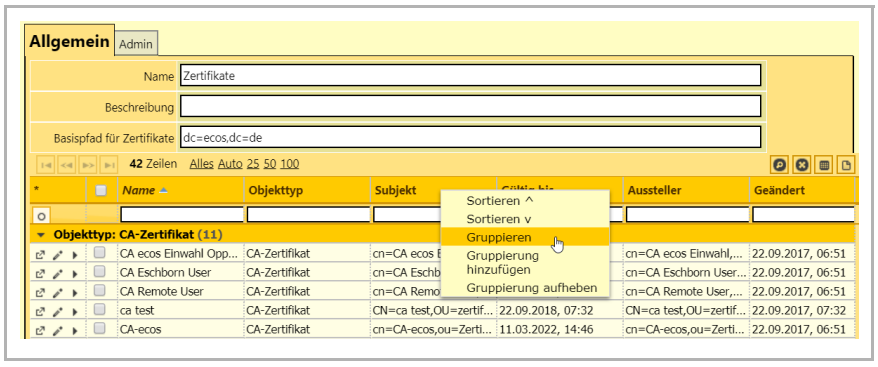
mal die Funktionen **» auf- und absteigende Sortierung «** sowie die Funktionen **» Gruppieren «**, **» Gruppierung hinzufügen «** und **» Gruppierung aufheben «** enthält.

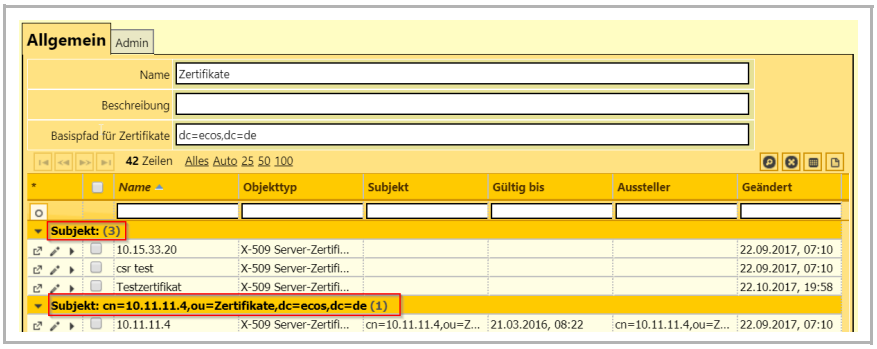




2.6.4.7 Gruppieren von Tabelleneinträgen

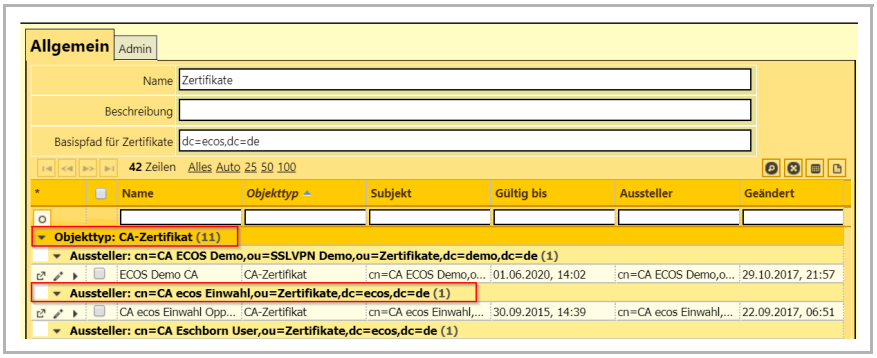
Ein Klick auf »Gruppieren« sortiert die Tabelleneinträge nach dem ausgewählten Kriterium und gruppiert sie unter der entsprechenden Überschrift. Klicken auf den Pfeil links lässt Gruppen ein- und ausblenden. Die Zahl in Klammern rechts neben der Überschrift zeigt die Anzahl der Objekte in einer Gruppe an.





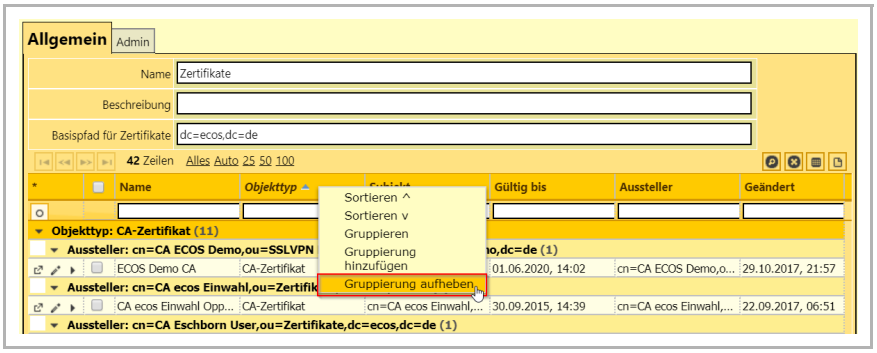
2.6.4.8 Gruppierung hinzufügen

Mithilfe dieser Funktion lassen sich bereits vorhandene Gruppen (siehe z.B. Objekttyp) in Untergruppen nach weiteren Kriterien sortieren und gruppieren (siehe z.B. Aussteller).



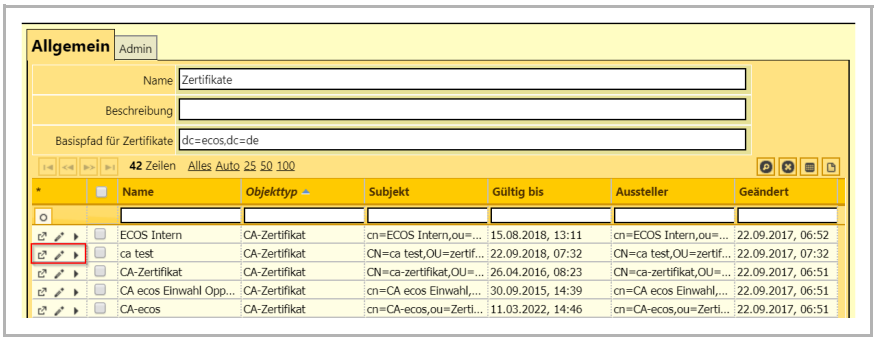
2.6.4.9 Gruppierung aufheben

Durch Auswahl von **» Gruppierung aufheben «** werden alle vorhandenen Gruppierungen aufgehoben

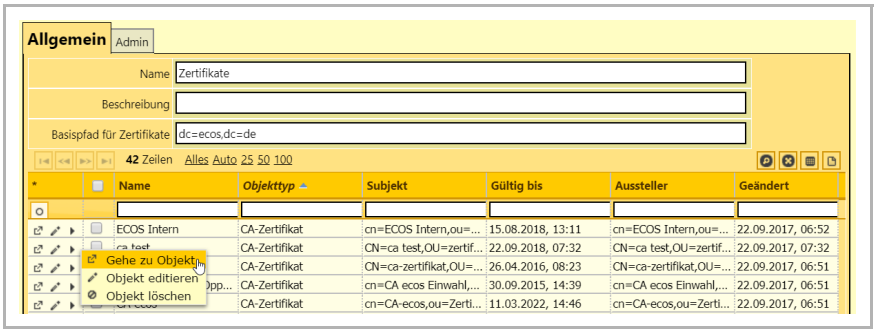


2.6.4.10 Die Aktionsspalte

Links neben jedem Objekt in der Tabelle befinden sich die Symbole » Gehe zu Objekt «, » Objekt editieren « und » Objekt einblenden «.



Alternativ erscheint bei Rechtsklick auf die Schaltfläche ein Auswahl-Menü mit den Optionen » Gehe zu Objekt «, » Objekt editieren « und » Objekt löschen «.

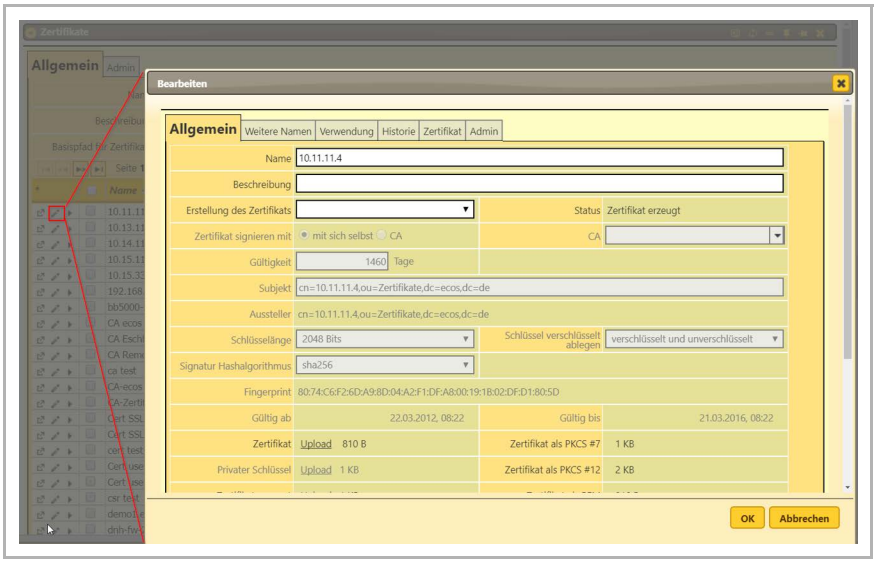


2.6.4.11 Gehe zu Objekt

Klicken auf das Symbol öffnet das entsprechende Konfigurationsobjekt im mittleren Bereich. Alternativ kann mit der mittleren Maustaste auf ein Tabellenfeld geklickt werden, um das Konfigurationsobjekt zu öffnen.

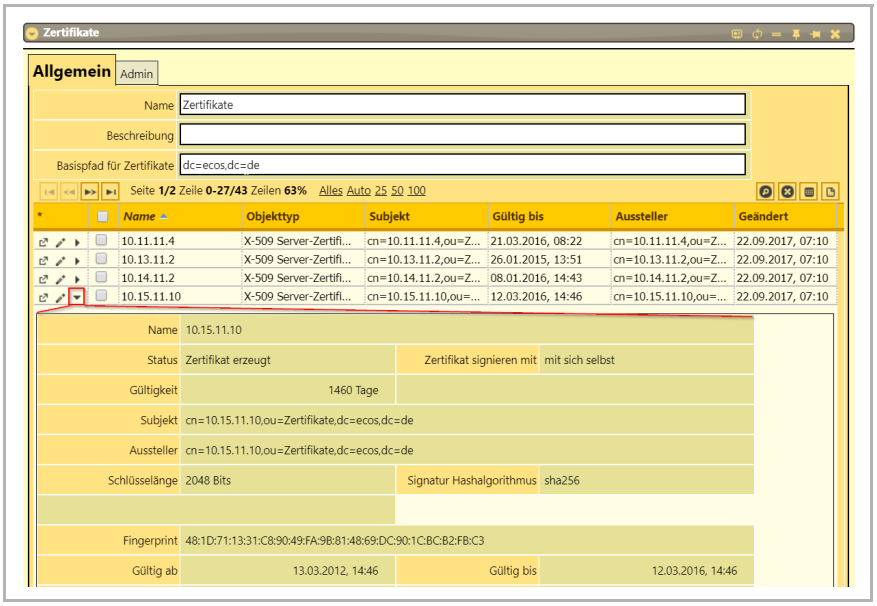
2.6.4.12 Objekt editieren

Klicken auf das Symbol öffnet das Formular des Konfigurationsobjekts in einem neuen Fenster. Alternativ kann das Formular mittels Doppelklick auf ein Tabellenfeld des Konfigurationsobjektes geöffnet werden. Hier können die Eigenschaften des Konfigurationsobjektes angepasst werden. Ein Klick auf » OK « speichert die Änderungen.



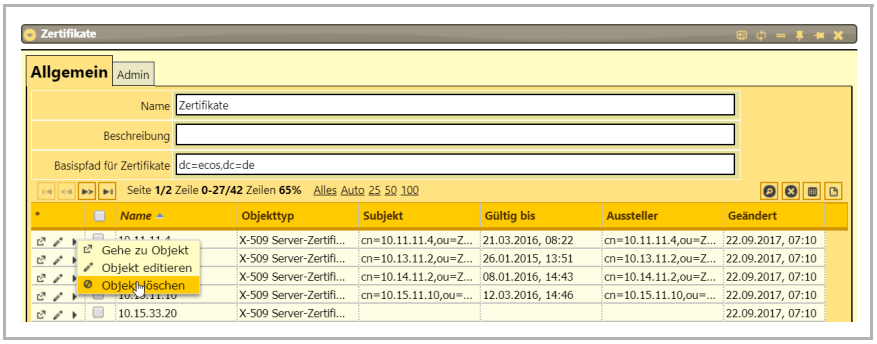
2.6.4.13 Objekt einblenden

Klicken auf das Symbol ▸ blendet eine Zusammenfassung der wichtigsten Parameter des Konfigurationsobjektes in der Tabelle ein. Ein erneutes Klicken auf das Symbol ▾ blendet sie wieder aus.



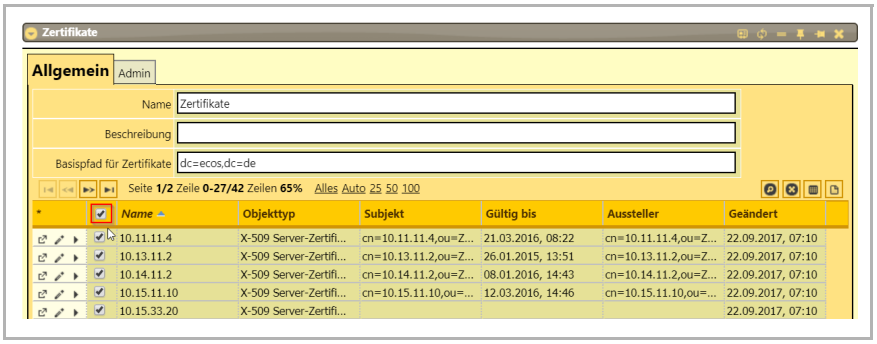
2.6.4.14 Objekt löschen

Der Befehl **»Objekt löschen«** wird das ausgewählte Objekt löschen. Sind mehrere Objekte ausgewählt, erscheint eine Warnung, bei der das Löschen sämtlicher ausgewählter Objekte bestätigt werden muss.



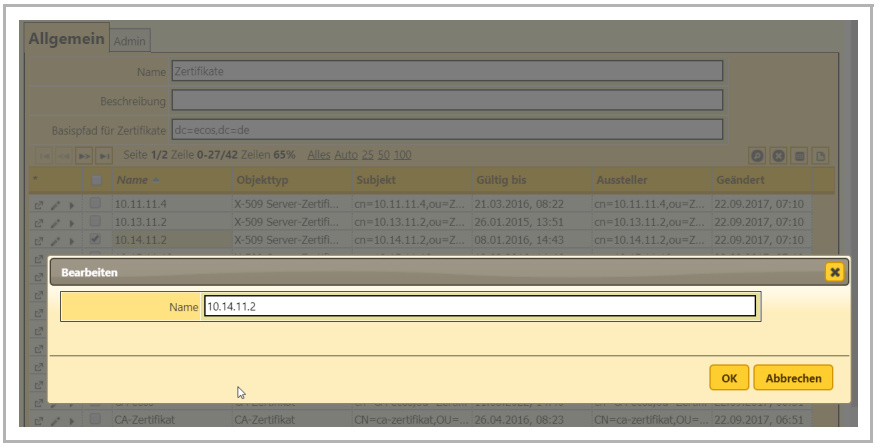
2.6.4.15 Auswählen von Objekten in Tabellen

Ein Anklicken der Auswahlbox im Tabellenkopf wählt sämtliche Konfigurationsobjekte in der Tabelle aus. Ein Anklicken der Box neben einem Konfigurationsobjekt wählt dieses aus. Auf diese Art lassen sich mehrere Objekte in der Tabelle auswählen. Alternativ kann ein Objekt in einem beliebigen Feld der Tabelle angeklickt und weitere Objekte durch Gedrückthalten markiert werden.



2.6.4.16 Tabellenfelder ändern

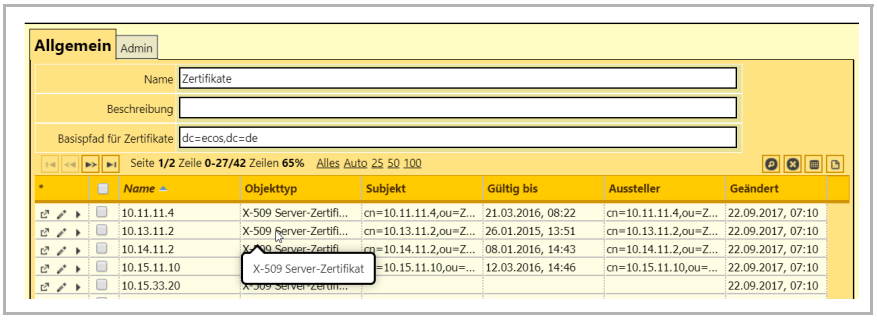
Durch Rechtsklick auf ein Tabellenfeld erscheint die Option **» Feld ändern «**. Bei Auswahl der Option öffnet sich ein neues Fenster, in dem der Inhalt des Feldes, wenn möglich, angepasst werden kann. Durch Klicken auf **» OK «** werden die Änderungen gespeichert. Sind mehrere Objekte ausgewählt, wird der Inhalt von sämtlichen Feldern entsprechend geändert.



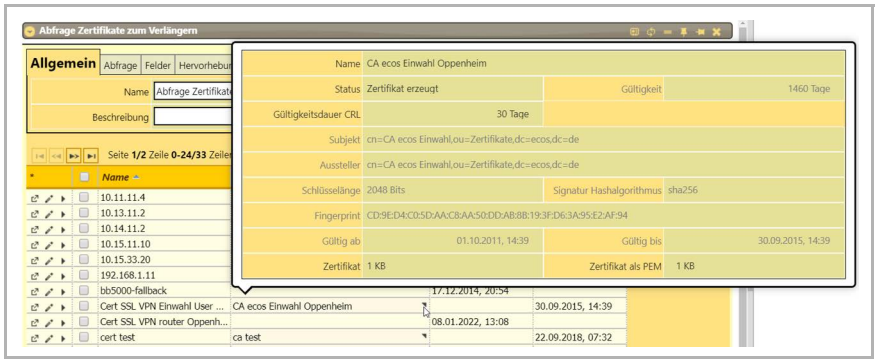
Ein schwarzes Dreieck in der rechten oberen Ecke eines Tabellenfeldes zeigt an, dass es sich bei dem Inhalt des Feldes um einen Verweis auf ein anderes Konfigurationsobjekt handelt. Bei diesen Feldern ist das Kontextmenü um die Optionen **» Gehe zu Objekt «** und **» Objekt editieren «** erweitert.

2.6.4.17 Popups

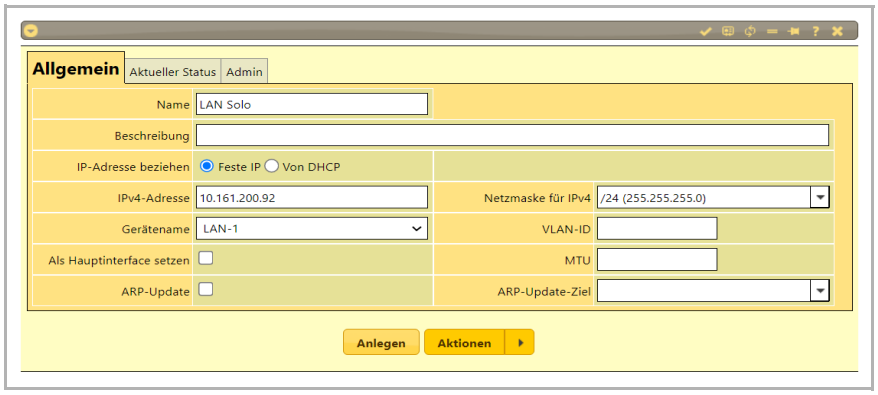
Ist eine Spalte nicht breit genug, sodass der Text nicht vollständig angezeigt wird, kann mit dem Maus-Zeiger über das Tabellenfeld gefahren werden. Dabei öffnet sich ein Popup, in dem der gesamte Text angezeigt wird.



Handelt es sich bei einem Eintrag in einem Tabellenfeld um ein anderes Konfigurationsobjekt, so erscheint durch Darüberfahren mit dem Maus-Zeiger und gleichzeitiges Drücken der Shift-Taste eine Zusammenfassung der wichtigsten Parameter des Objektes.



Im Auslieferungszustand befindet sich bereits ein angelegtes LAN-Objekt im Container **» Interfaces «**. In diesem müssen IP-Adresse und Netzmaske des gewünschten Netzwerkes konfiguriert werden. Wird mehr als ein LAN-Interface benötigt, können beliebig viele weitere Netzwerkschnittstellen angelegt und konfiguriert werden.



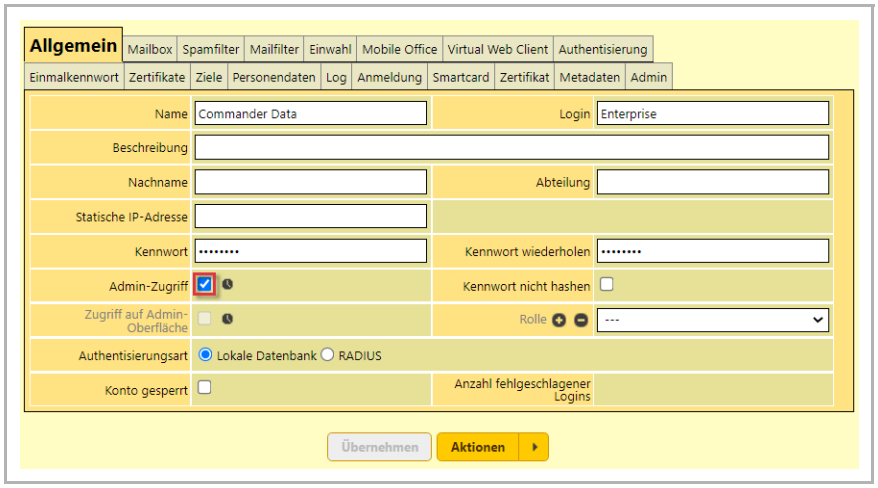
3 Appliance Grundeinrichtung

3.1 Admin-Benutzer

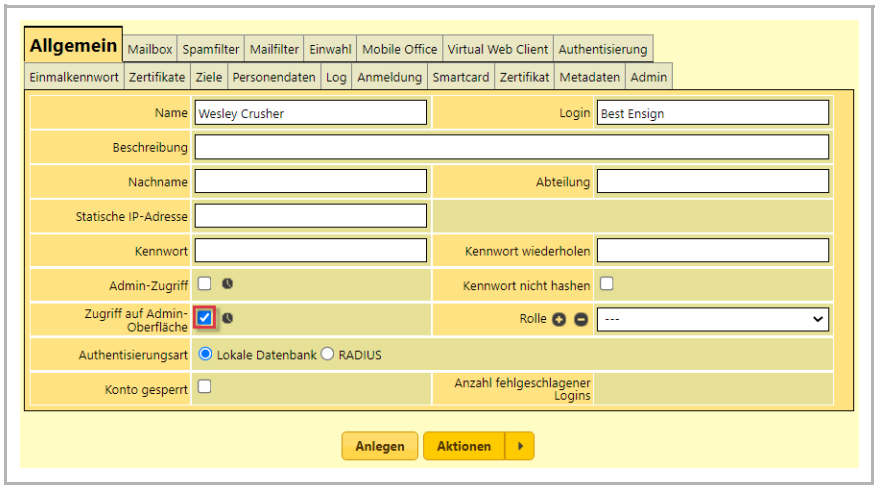
Zur Administration der ECOS Appliance muss sich der Benutzer als Admin-Benutzer anmelden.

Es können ein oder mehrere Admin-Benutzer angelegt werden. Im Auslieferungszustand ist der Benutzer **admin** vorgegeben und mit Adminrechten ausgestattet. Administratoren haben uneingeschränkten Zugriff auf alle Konfigurationsobjekte und Funktionen.

Durch Aktivieren der Checkbox unter **Benutzer → Allgemein → Admin-Zugriff** können einem Benutzer Administrationsrechte verliehen werden. Dieser Admin-Benutzer hat Zugriff auf sämtliche Funktionen des Managements.



Alternativ kann im Benutzer-Objekt die Checkbox im Feld **Zugriff auf Adminoberfläche** aktiviert werden. Dies erlaubt dem Benutzer das Aufrufen des Webinterfaces der Administrationsoberfläche.



Wurden dem Benutzer keine weiteren Rechte erteilt, bleibt das Feld leer. Durch Zuweisen einer Rolle können dem Benutzer spezifische Rechte verliehen werden.

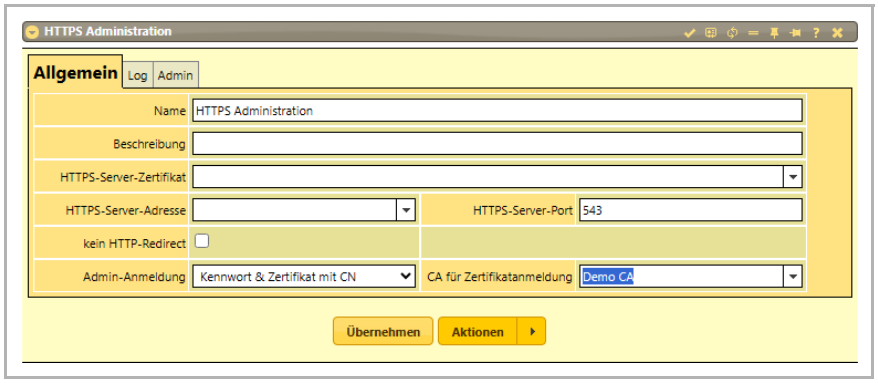
Siehe *3.4.1 | HTTPS-Administration* auf Seite 50, *6 | Benutzer* auf Seite 74 sowie *13.8.2 | Benutzern Rollen zuweisen* auf Seite 183.

3.1.1 Neuerungen für SBS und SMA mit V7.3 (VS-NfD)

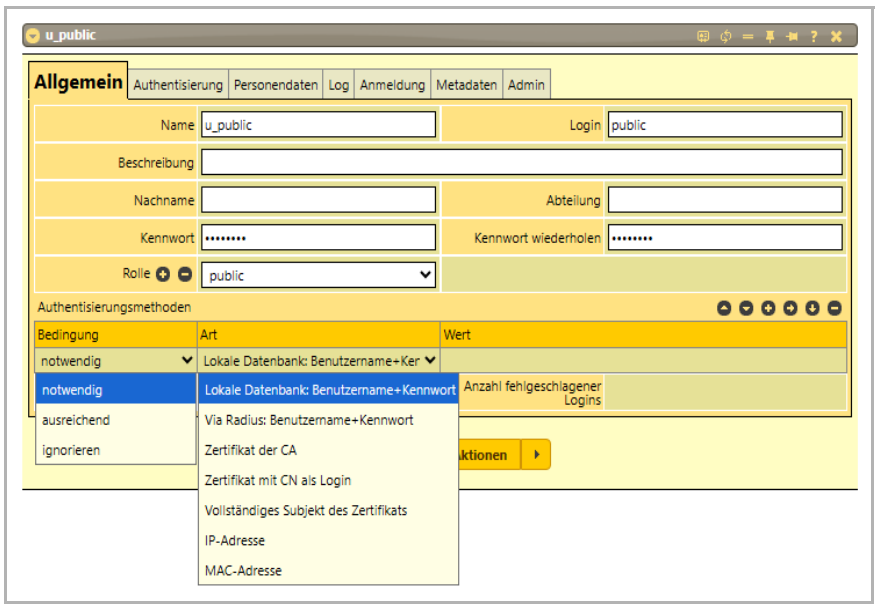
Mit der BSI-zugelassenen SBS-/SMA-Version 7.3 (VS-NfD) müssen sich Admin-Benutzer sowie Benutzer mit administrativen Teilrechten mit ihrer Smartcard an der Administrationsoberfläche der ECOS Appliance anmelden.

Dies kann einerseits global im Objekt → **HTTPS-Administration** konfiguriert werden und ist für alle Benutzer gültig. Im Feld Allgemein: Admin-Anmeldung muss die Option Kennwort & Zertifikat mit CN ausgewählt werden. Jeder Benutzer mit administrativen Zugang benötigt ein eigenes Benutzerzertifikat. Der CN des Zertifikats muss dem Namen des Benutzers entsprechen Dazu wird am einfachsten der Benutzername des Benutzerobjekts als Name des Zertifikats gesetzt. Siehe *7 | Zertifikate* auf Seite 75.

Zusätzlich muss im Feld Allgemein: CA für Zertifikatanmeldung die CA angegeben werden, mit der die Benutzerzertifikate signiert wurden. Es hat sich bewährt, eine eigene CA für das Signieren der Benutzerzertifikate anzulegen, die hier ausgewählt wird.



Gibt es Benutzerkonten, die sich nicht mit Zertifikat anmelden sollen, besteht die Möglichkeit für jeden Benutzer die Authentisierungsmethoden individuell einzustellen. Dies wird im Benutzerobjekt konfiguriert:



Im Feld Allgemein: Authentisierungsmethoden können eine oder mehrere Methoden zur Authentisierung festgelegt werden. In der Spalte Bedingung wird konfiguriert, ob die jeweilige Authentisierungsmethode für die Anmeldung notwendig bzw. ausreichend ist oder ignoriert wird. Für eine erfolgreiche Anmeldung müssen *alle* notwendigen Bedingungen erfüllt sein. Wurden ausreichende Bedingungen definiert, muss *eine* dieser Bedingungen für die Anmeldung erfüllt sein. Wurden sowohl notwendige als auch ausreichende Bedingungen definiert, müssen *alle notwendigen* und *mindestens eine ausreichende* Bedingung erfüllt sein, damit sich der Benutzer erfolgreich anmelden kann.

Neben der Anmeldung mit einfachen Zugangsdaten über die lokale Datenbank der ECOS Appliance oder einen RADIUS-Dienst stehen in der Spalte Art verschiedene Möglichkeiten zur Anmeldung mit einem Zertifikat oder aus einem bestimmten Netzwerk bzw. von einem bestimmten Gerät zur Verfügung.

- Bei der Anmeldung mit Zertifikat der CA muss das Zertifikat zur Anmeldung von der CA signiert sein, die im → **Dienst: HTTPS-Administration** ausgewählt ist.
- Für die Anmeldung mit Zertifikat mit CN als Login wird ein Zertifikat gebraucht, dessen CN dem Login des Benutzers entspricht. Das Zertifikat muss von der CA signiert sein, die im → **Dienst: HTTPS-Administration** ausgewählt ist.
- Soll ein bestimmtes Zertifikat zur Anmeldung genutzt werden, das nicht unbedingt dem Benutzerzertifikat entsprechen muss, wird als Authentisierungsmethode vollständiges Subjekt des Zertifikats gewählt. Neben dem Subjekt muss auch die CA mit dem in der Spalte Wert angegebenen Zertifikat übereinstimmen.
- Soll die Anmeldung aus einem bestimmten Netzwerk erfolgen, kann dies über die Methode IP-Adresse und den entsprechend ausgewählten Netzwerken gewährleistet werden.
- Darf der administrative Zugriff nur über ein bestimmtes Gerät erfolgen, wird die Authentisierungsmethode MAC-Adresse gewählt und die entsprechende MAC-Adresse in der Spalte Wert angegeben.

Hinweis: Sobald eine Authentisierungsmethode für die Anmeldung konfiguriert ist, ist für die Anmeldung auf der Administrationsoberfläche zwingend ein Zertifikat bzw. das entsprechende Netzwerk oder Gerät notwendig. Kann der Benutzer dies nicht vorweisen, ist eine Anmeldung nicht möglich.

3.2 Netzwerkkonfiguration

Die grundlegende Netzwerkkonfiguration erfolgt zum einen durch Anlegen der notwendigen Interfaces im Container **Interfaces**, zum anderen durch Setzen des Default-Gateways und des/der DNS-Server im **ECOS Appliance**-Objekt. Zusätzlich können im Container **Routen** statische Routen hinzugefügt werden.

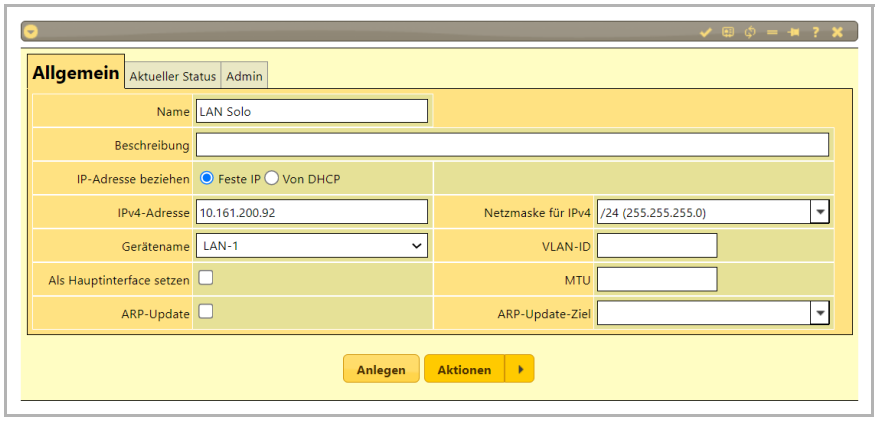
3.2.1 Interfaces

Im Container **Interfaces** des Appliance-Objekts werden die gewünschten Netz-

werkinterfaces angelegt. In Abhängigkeit vom verwendeten Gerätetyp stehen unterschiedliche Objekte zur Verfügung.

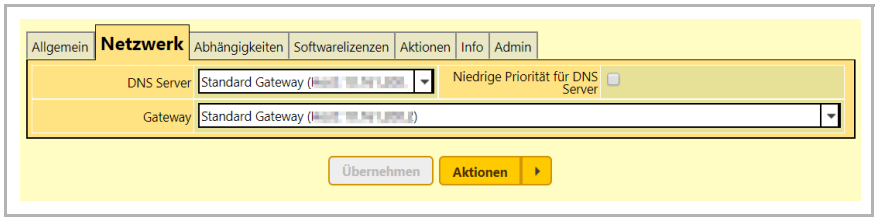
Im Auslieferungszustand befindet sich bereits ein angelegtes LAN-Objekt im Container **Interfaces**. In diesem müssen IP-Adresse und Netzmaske des gewünschten Netzwerkes konfiguriert werden.

Wird mehr als ein LAN-Interface benötigt, können beliebig viele weitere Netzwerkschnittstellen angelegt und konfiguriert werden.



3.2.2 Standard-Gateway und DNS-Server

Im Reiter **Netzwerk** des Appliance-Objekts müssen ein Standard-Gateway und ein DNS-Server konfiguriert werden. Im Container **Routen** des Appliance-Objekts können bei Bedarf weitere statische Routen angelegt werden.



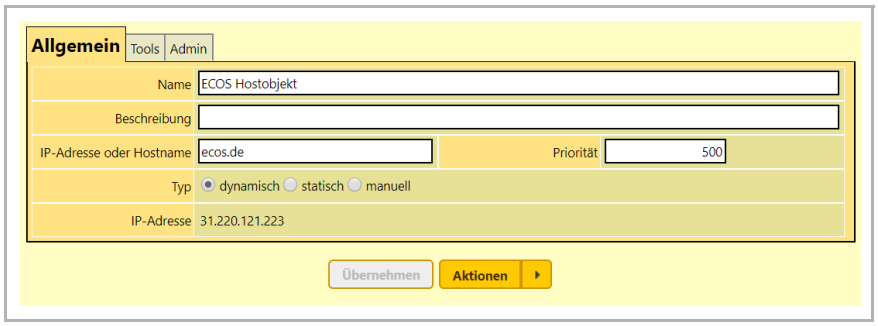
3.3 Definition von Netzwerkadressen

3.3.1 Host/Netze

Das Konfigurationsobjekt **Def.: Hostname** definiert einen Namen für einen Rechner oder eine IP-Adresse. Über diesen Namen kann der Host an verschiedenen

Stellen, an denen IP-Adressen erforderlich sind, referenziert werden. Die zentrale Definition von Host-Adressen ermöglicht eine leichte Verwaltung der Hosts, da die tatsächliche Adresse nur an einer Stelle eingegeben werden muss. Soll die IP-Adresse geändert werden, geschieht dies nur in der Host-Definition und wirkt sich direkt auf alle Stellen aus, an denen dieser Host referenziert wurde.

Der Typ eines Host-Objekts legt fest, wie die IP-Adresse des Hosts ermittelt wird. Zur Auswahl stehen **dynamisch**, **statisch** oder **manuell**.



Ist ein Host vom Typ **dynamisch** und wird ein DNS-Name eingegeben, wird aus diesem die IP-Adresse ermittelt und ständig geprüft wird, ob sich die Adresse ändert. Dies ist für dynamische DNS-Namen sinnvoll.

Wird der Typ **statisch** gewählt, wird der DNS-Name nur bei seiner Eingabe in eine IP-Adresse umgewandelt. Ändert sich die IP-Adresse von einem bereits eingegebenen DNS-Namen, ist ein erneutes Klicken auf **Übernehmen** notwendig. Dieser Typ schützt vor DNS-Spoofing, da falsche oder böswillige DNS-Einträge die IP-Adresse nachträglich nicht mehr ändern können.

Bei Auswahl des Typs **manuell** muss die IP-Adresse manuell eingegeben werden und wird nicht per DNS ermittelt. In diesem Fall wird ein Eintrag in die Hostdatei geschrieben, sodass der Name allen Programmen/Diensten auf dem System zur Verfügung steht, auch wenn keine Verbindung zu einem DNS besteht oder der Host nicht per DNS aufgelöst werden kann. Für die Typen **dynamisch** und **statisch** wird im Feld **IP-Adresse** die ermittelte IP-Adresse angezeigt. Für den Typ **manuell** muss eine IP-Adresse eingegeben werden.

Im Feld **Priorität** können Hosts unterschiedliche Prioritäten zugewiesen werden, die zur Sortierung in Listen verwendet werden. Dies findet z.B. Anwendung, wenn sich mehrere Hosts in einem Container befinden und dieser als DNS-Server angegeben wird. In diesem Fall bestimmt die Priorität, welcher DNS-Server zuerst befragt wird. Kleinere Zahlen bedeuten höhere Priorität.

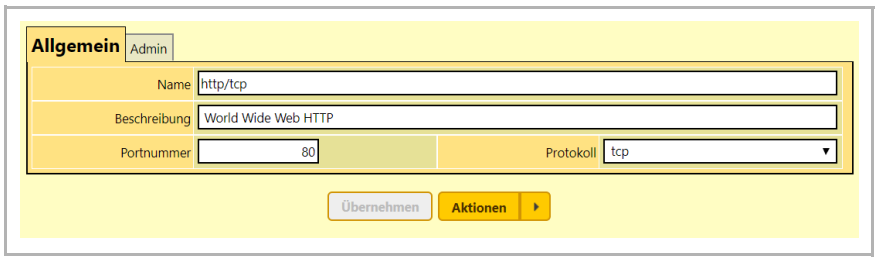
3.3.2 Netzwerke

Netzwerkadressen werden in Konfigurationsobjekten vom Typ **Def.: Netzwerk** verwaltet. Diese definieren Namen für IP-Netzwerke. Über den Namen kann das Netzwerk an verschiedenen Stellen referenziert werden, an denen Netzwerkadressen erforderlich sind. Die zentrale Definition von Netzwerkadressen ermöglicht darüber hinaus eine leichte Änderung, da die tatsächliche Adresse nur an einer zentralen Stelle eingegeben werden muss. Soll die Netzwerkadresse geändert werden, geschieht dies nur in der Netzwerkdefinition und wirkt sich direkt auf alle Stellen aus, an denen dieses Netzwerk referenziert wurde.

Im Feld **IP-Netzwerkadresse** werden die IP-Adresse und die Netzmaske des im Namensfeld definierten Netzwerkes in der Form **n.n.n.n/m** angegeben.

3.3.3 Ports

Ports werden in Konfigurationsobjekten vom Typ **Def.: Service-Port** verwaltet. Hier wird für einen bestimmten UDP- oder TCP-Port ein Name vergeben. An anderen Stellen der Konfiguration, an denen eine Portauswahl nötig ist, wird mithilfe des zugeordneten Portnamens auf den entsprechenden Port verwiesen.



3.4 Grundlegende Dienste

3.4.1 HTTPS-Administration

Der **Dienst: HTTPS-Administration** dient der Konfiguration des HTTPS-Servers, der die Administrationsoberfläche bereitstellt.

Im Feld **HTTPS-Server-Zertifikat** wird das Server-Zertifikat ausgewählt, über welches sich das ECOS System beim Aufruf der Administrationsoberfläche authentifiziert. Bei der Installation wird ein Default-Zertifikat erzeugt. Dieses kann durch ein an die aktuelle Umgebung angepasstes Zertifikat ersetzt werden, damit der Browser der Administrationsoberfläche vertraut.

Das Feld **HTTPS-Server-Port** dient der Konfiguration des Ports, über den die Administrationsoberfläche erreicht werden kann. Standardmäßig ist auf der Appliance Port 543 gesetzt, um Konflikte mit anderen Diensten zu vermeiden, die ggf. den HTTPS-Port 443 benutzen. Wird kein Port angegeben, wird der Standard-Port 443 verwendet.

Im Feld **HTTPS-Server-Adresse** kann eingestellt werden, über welche Adresse die Administrationsoberfläche erreicht werden kann. Wird das Feld leer gelassen (Standardfall) und die Appliance besitzt mehrere Adressen, kann sie über jede davon erreicht werden.

Unter **Admin-Anmeldung** kann die Art der Authentifizierung an der Administrationsoberfläche der Appliance eingestellt werden. Die Standardeinstellung ist **Nur Kennwort**. Hierbei erfolgt die Anmeldung mit dem beim Benutzer angegebenen statischem Kennwort.

*Siehe **3.1 | Admin-Benutzer** auf Seite 43.*

Bei Auswahl der Option **Kennwort & Zertifikat** ist eine Authentifizierung nur möglich, wenn der Benutzer zusätzlich im Besitz eines gültigen Zertifikats ist. Dieses muss von der für die Zertifikatanmeldung angegeben CA (Feld **CA für Zertifikatanmeldung**) ausgestellt sein. Dieses Zertifikat kann sowohl ein im Computer des Benutzers gespeichertes Softwarezertifikat sein, als auch ein Zertifikat, das auf einer Smartcard oder einem Token gespeichert ist.

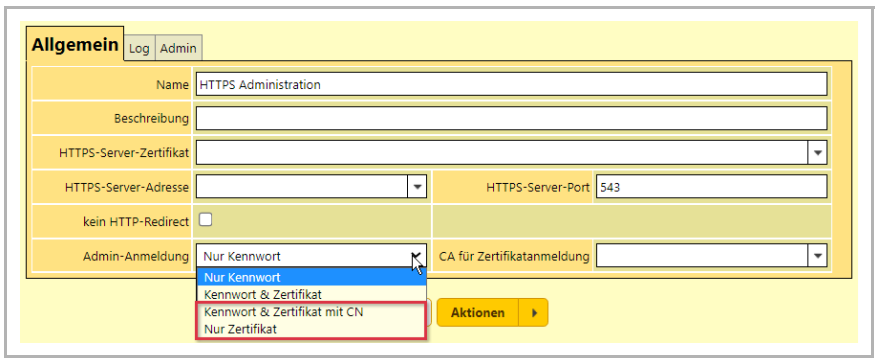
Bei Auswahl der Option **Kennwort & Zertifikat mit CN** erfolgt die Anmeldung sowohl mit dem Benutzerkennwort als auch mit einem gültigen Anmeldezertifikat. Der Common Name (CN) des Zertifikats muss dem unter **Benutzer → Allgemein → Login** angegebenen Namen entsprechen. Die übrigen Einstellungen verhalten sich identisch zu **Kennwort & Zertifikat**.

Bei Auswahl der Option **Nur Zertifikat** erfolgt die Anmeldung ausschließlich mit einem Anmeldezertifikat. Der Common Name (CN) des Zertifikats muss dem unter **Benutzer → Allgemein → Login** angegebenen Namen entsprechen. Die übrigen Einstellungen verhalten sich identisch zu **Kennwort & Zertifikat**.

Hinweis: Ab der BSI-zugelassenen SBS-/SMA-Version 7.3 (VS-NfD) müssen sich Admin-Benutzer sowie Benutzer mit administrativen Teilrechten mit ihrer Smartcard an der Administrationsoberfläche der Appliance anmelden.

Der Browser fordert bei der Anmeldung ein gültiges Zertifikat. Hierfür stehen im Feld **Admin-Anmeldung** die Optionen **Kennwort & Zertifikat mit CN** und **Nur Zertifikat** zur Verfügung.

Das Zertifikat kann ein Softwarezertifikat oder ein auf der Smartcard gespeichertes Zertifikat sein.



3.4.2 OCSP-Serverdienst

Ein **OSCP-Dienst** (Online Certificate Status Protocol) dient dazu, die Gültigkeit eines Zertifikats zum Zeitpunkt der Anfrage online zu überprüfen. Eine OCSP- Überprüfung ist somit aktueller als die Überprüfung durch die Certificate Revocation List (CRL).

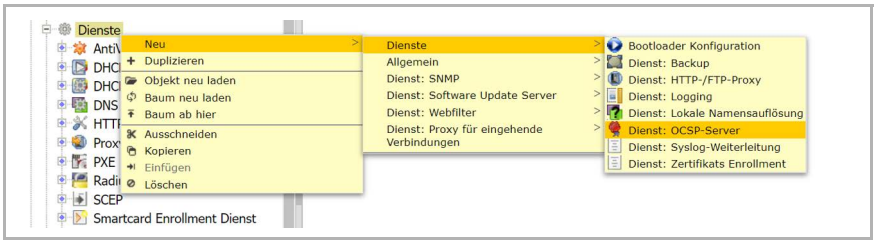
3.4.2.1 Voreinstellung

Damit die Clients wissen, unter welcher Adresse der OCSP-Server erreichbar ist, kann die URL des OCSP- Servers im CA-Objekt hinterlegt werden. Die URL wird dann in jedes von dieser CA erzeugte Zertifikat eingefügt. Hierzu wird im CA-Objekt im Feld **Authority Info Access** die Adresse hinterlegt, über die der OCSP-Server auf der Appliance erreicht werden kann (siehe ***7.4.2 | Authority Info Access*** auf Seite 86).

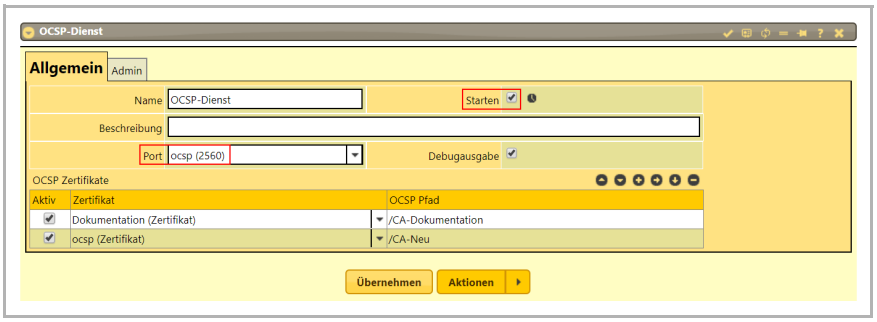
Sind diese Informationen definiert, kann der **OCSP-Dienst** konfiguriert werden.

3.4.2.2 Konfiguration des OCSP-Dienstes

Der **OSCP-Dienst** wird unter dem Appliance-Objekt im Container **Dienste** angelegt und gestartet.



Für den OCSP-Server muss zunächst ein **Port** angegeben werden, unter dem der Dienst erreichbar ist. Es sollte der Port sein, der unter **CA-Zertifikat → Erweitert →Authority Info Access** in der OCSP-URL angegeben ist.



In der Tabelle **OSCP-Zertifikate** muss angegeben werden, für Zertifikate welcher CA der OCSP-Server Überprüfungen durchführen soll. Je CA muss jeweils eine Zeile in der Tabelle eingetragen werden.

Damit die Antworten beim Client unverfälscht ankommen, signiert sie der **OSCP-Dienst** mit einem Zertifikat. Hierzu wird in der Tabelle **OSCP-Zertifikate** in der Spalte **Zertifikat** ein Zertifikat ausgewählt. Das ausgewählte Zertifikat wählt dabei gleichzeitig die CA aus, deren Zertifikate geprüft werden. Das ausgewählte Zertifikat benötigt die Schlüsselverwendung **Digital Signieren** und die Erweiterte Schlüsselverwendung **OCSP Signing** (siehe *7.2.10 | Verwendungszweck* auf Seite 82).

Über den **OCSP-Pfad** wird der Pfadanteil der OCSP-URL definiert, über den OCSP-Anfragen entgegengenommen werden. Das heißt, dass alle Anfragen für Zertifikate, die von der CA ausgestellt wurden, die über das Zertifikat in der gleichen Zeile ausgewählt wurde, müssen über diesen Pfad gestellt werden.

Beispiel: Der angegebene Port ist 2560, die Adresse der Appliance 1.2.3.4 und bei Pfad steht /CA-Neu, dann ist die OCSP-URL für diese CA http://1.2.3.4:2560/CA-Neu.

Soll der OCSP-Server-Zertifikate mehrere CAs überprüfen, so muss pro CA eine Zeile in die Tabelle eingetragen werden. Es muss für jede CA ein eigenes Zertifikat für den OCSP-Server erzeugt und eingetragen werden und die Pfade für die CAs in den einzelnen Zeilen müssen eindeutig sein.

Ist die Checkbox für die **Debugausgabe** aktiviert, wird im Log eine ausführliche Protokollierung durchgeführt, welche die Fehlersuche erleichtert.

3.4.3 RADIUS

Der RADIUS-Dienst dient der Authentisierung diverser Dienste. Er muss unter dem Appliance-Objekt im Container **Dienste** angelegt und gestartet sein.

Der RADIUS-Dienst wird für das Easy Enrollment per Aktivierungscode benötigt. Werden mit dem RADIUS-Dienst keine weiteren Dienste außer dem Easy Enrollment authentisiert, so sind keine weiteren Einstellungen notwendig. Findet das Easy Enrollment per Smartcard statt, ist der RADIUS-Dienst nicht notwendig.

3.4.4 SCEP-Dienst

SCEP (Simple Certificate Enrollment Protocol) ist ein Protokoll zum automatischen Ausrollen und Verlängern von Zertifikaten.

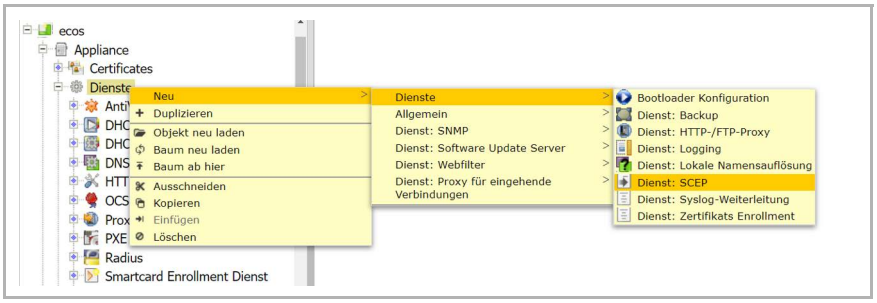
3.4.4.1 Notwendige Objekte

Damit der **SCEP-Dienst** laufen kann, muss ein Software-Update-Server angelegt und gestartet sein. Siehe *3.4.5 | Software-Update-Server* auf Seite 55

Des Weiteren muss ein Container angelegt werden, in dem neu erzeugte Zertifikate gespeichert werden.

3.4.4.2 Konfiguration des SCEP-Dienstes

Der **SCEP-Dienst** wird unter dem Appliance-Objekt im Container **Dienste** angelegt und gestartet.

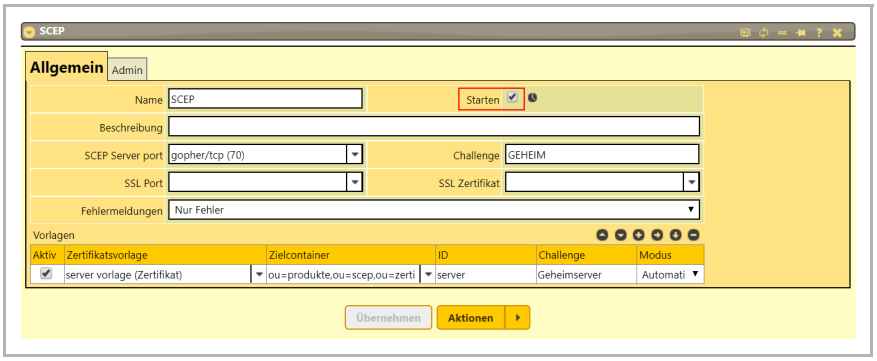


Im Konfigurationsformular des **SCEP-Dienstes** wird im Feld **SCEP-Server-Port** festgelegt, auf welchem Port der SCEP-Dienst Zertifikatanfragen annimmt. Werden ein **SSL-Port** und ein **SSL-Zertifikat** ausgewählt, werden Anfragen über diesen Port zusätzlich SSL-verschlüsselt übertragen.

Das Feld **Challenge** ist ein einfacher Authentisierungsmechanismus. Hier wird ein Passwort angegeben, das ein unberechtigtes Beantragen von Zertifikaten verhindert.

Im Feld **Fehlermeldungen** stehen die Optionen **Nur Fehler**, **Fehlersuche (wenig)**, **Fehlersuche (Mittel)** oder Fehlersuche **(Details)** zur Verfügung. Dies entscheidet darüber, wie ausführlich das Ausstellen der Zertifikate in den Logdateien protokolliert wird.

Der SCEP-Dienst wird über die Checkbox **Starten** aktiviert.



3.4.4.3 Vorlagen im SCEP-Dienst

In der Tabelle **Vorlagen** wird in der Spalte **Zertifikatvorlage** ein Zertifikat ausgewählt, das als Vorlage verwendet wird. Dieses Zertifikat wird nicht ausgeliefert, stattdessen werden die Einstellungen dieses Zertifikates in die vom **SCEP-Dienst** neu ausgestellten Zertifikate übernommen. In der Spalte **Zielcontainer** wird ausge-

wählt, in welchem Container die neu erzeugten Zertifikate abgelegt werden sollen.

Die ID ist ein Bestandteil der URL und ordnet einer Anfrage eine passende Vorlage zu. Sinnvoll ist es, die ID nach dem Zweck zu vergeben, für den diese Zertifikate erstellt werden sollen.

Beispiel:

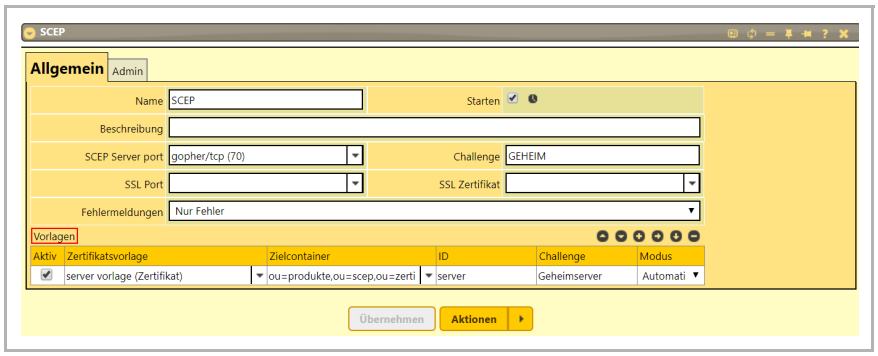
id = telefon, port = 1234, server dns = www.ecos.de

→ http://www.ecos.de:1234/telefon/pkiclient.exe

Wird die Spalte **Challenge** leer gelassen, wird der Wert aus dem Eingabefeld **Challenge** des Formulars verwendet. Ist diese Spalte gefüllt, hat der Wert Vorrang.

Wird der Modus **Automatisch** ausgewählt, wird durch alle Anfragen automatisch ein neues Zertifikat erzeugt und ausgeliefert. Wird **Manuell** ausgewählt, müssen alle Anfragen vom Administrator überprüft und genehmigt werden. Erst dann wird auf die nächste Anfrage des Clients ein Zertifikat ausgeliefert. Vorherige Anfragen werden mit **Bitte warten** beantwortet. Dazu muss der Administrator im Zielcontainer nachsehen, welche Zertifikatanfragen dort eingegangen sind und diese dann von Hand erstellen oder löschen.

Ist die Checkbox **Aktiv** aktiviert, wird die Vorlage freigeschaltet.

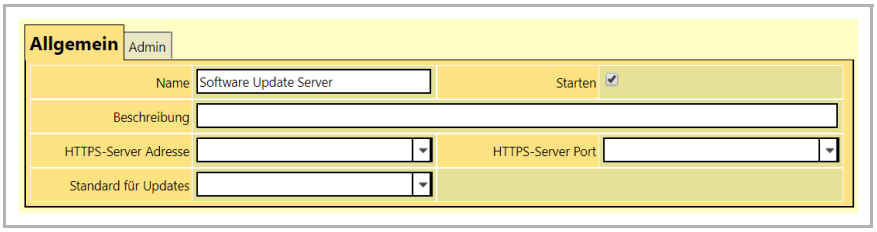


3.4.5 Software-Update-Server

Der Software-Update-Server wird sowohl für das Easy Enrollment als auch für die Anbindung von Secure Boot Sticks benötigt. Außerdem kann er Software-Updates an Secure Boot Sticks oder weitere Appliances verteilen.

*Siehe **13.3 | Dienst: Software-Update-Server einrichten** auf Seite 165.*

Um Secure Boot Sticks anzubinden, muss der Software-Update-Server lediglich angelegt und gestartet sein.



3.4.6 Software-Update

Das Software-Update-Objekt dient dazu, Einstellungen für das Software-Update vorzunehmen. Updates können entweder manuell oder automatisch ausgeführt werden. Außerdem können Updates entweder über die Master-Appliance oder über den ECOS Update-Server (hz.update.ecos.de) erfolgen.

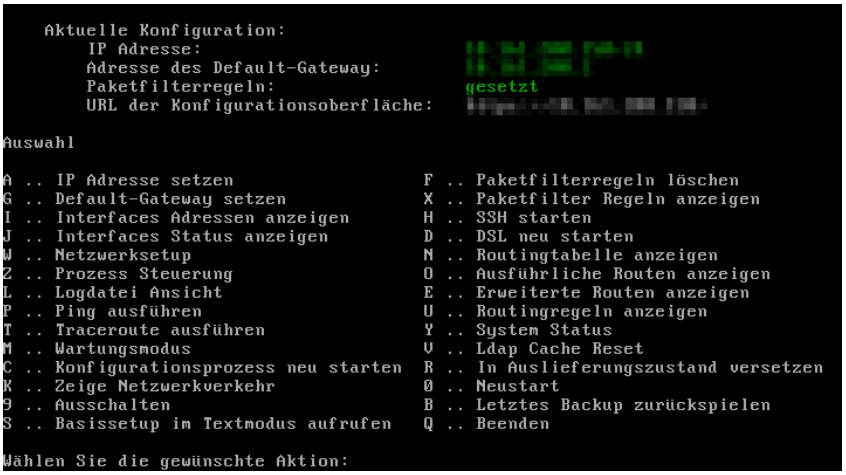
*Siehe **13.4 | Dienst: Software-Update einrichten** auf Seite 166.*

3.4.7 Wartung

Im **Dienst: Wartung** werden Wartungszugänge konfiguriert.

Im Reiter **Lokale Wartung** werden die Einstellungen für den lokalen Wartungszugang konfiguriert. Die Checkbox **Kennwort für Konsole aktivieren** aktiviert das benutzerdefinierte Kennwort für die Anmeldung an der Konsole. Die Anmeldung erfolgt mit dem Benutzernamen **setup**. Ist kein Kennwort gesetzt, greift das Standardkennwort **bb5000**. In diesem Fall ist über die Konsole kein Shell- oder Root-Zugang möglich, sondern nur zu einem Menü, das grundlegende Wartungsaufgaben wie das Setzen der IP-Adresse oder das Senden eines Ping erlaubt.

Soll ein Secure Boot Stick SX/FX oder GX/ZX gewartet werden, muss nach Eingabe des Kennworts zusätzlich die PIN am Pinpad des SBS eingegeben und mit der ECOS-Taste bestätigt werden.



Die Checkbox im Feld **Fernwartung → Starten** aktiviert die SSH-Fernwartung. Im Feld **Port** kann der Port angegeben werden, auf den der SSH-Dienst reagieren soll. Wird das Feld leer gelassen, wird der Standard-SSH-Port 22 verwendet.

Durch Aktivieren der Checkbox im Feld **Zugriff für Benutzer 'remotesetup' erlauben** wird für den Benutzer **remotesetup** die Anmeldung mit einem benutzerdefiniertem Kennwort via SSH zugelassen, mit der er zum selben Menü wie bei der direkten Konsolenanmeldung gelangt. Im Feld **Kennwort Fernwartung** muss hierzu ein entsprechendes Kennwort vergeben werden. Zusätzlich können für eine SSH-Portweiterleitung **Erlaubte weitergeleitete Ports** für diesen Benutzer ausgewählt werden.

Durch Aktivieren der Checkbox im Feld **Zugriff für Benutzer 'remotebackup' erlauben** wird für den Benutzer **remotebackup** der SFTP-Zugriff auf die internen Konfigurationsbackups erlaubt. Dieser Benutzer hat nur Zugriff auf das Backupverzeichnis (/backup) der Appliance. So können Backupdateien per SFTP abgeholt werden, wenn sie z.B. zu groß sind, um über das Appliance-Objekt der Administrationsoberfläche heruntergeladen zu werden. Die Anmeldung über das SFTP-Protokoll ist nur durch Authentifizierung mit einem SSH-Schlüssel möglich. Der öffentliche Schlüssel wird im Feld **SSH Public Key für Benutzer 'remotebackup'** hinterlegt. Der Zugriff auf die Backupdateien kann mit einem beliebigen Tool per SFTP erfolgen (z.B. WinSCP).

3.4.8 Zeitsynchronisation

Der Dienst **Zeitsynchronisation** stellt die lokale Uhrzeit mittels NTP-Protokoll automatisch korrekt ein. Dazu ist es nötig, einen oder mehrere NTP-Server anzugeben.

3.5 Lizenzen und Features

Je nach gekaufter Lizenz stehen dem Benutzer verschiedene Features zur Verfügung. Diese lassen sich im Appliance-Objekt im Reiter **Software-Lizenzen** in der Tabelle **Lizenzinformationen** einsehen.

Wird der ECOS Update-Server zur Update-Verwaltung verwendet, werden die neu freigeschalteten Lizenzen automatisch vom Updateserver an die Appliance bzw. die Secure Boot Sticks während des Updates verteilt.

*Siehe **13.2 | Updates** auf Seite 164.*

Die Management Appliance lädt jedoch nur ihre eigenen Lizenzen vom Update-Server. Sollen Lizenzen an angeschlossene Secure Boot Sticks verteilt werden, müssen diese als ZIP-Datei eingespielt werden.

Wird ein lokaler Update-Server zur Update-Verwaltung verwendet, müssen der Appliance neue Lizenzen per ZIP-Datei zur Verfügung gestellt werden. Die ZIP-Datei enthält die notwendigen Lizenzen für die Management Appliance sowie für alle verknüpften Secure Boot Sticks.

Unter **Aktion ausführen** in der Menüleiste am oberen Bildschirmrand befindet sich die Option **Lizenzen hochladen**. Über diesen Menüpunkt werden lizenzbasierte Funktionen freigeschaltet, indem Lizenzen in Form von ZIP-Dateien hochgeladen werden.

Nach Klicken auf **Lizenz hochladen** öffnet sich ein neues Fenster, in dem die Lizenzdatei ausgewählt und durch Klicken auf **Weiter** hochgeladen werden kann.

Alternativ können einzelne Lizenzen für eine spezifische Appliance oder einen spezifischen Secure Boot Stick im Appliance- bzw. SBS-Objekt im Reiter **Software-Lizenzen** hochgeladen werden.

4 Werkzeuge des Systems

4.1 Registerkarte Aktionen

Unter der Registerkarte **»Aktionen«** sind folgende Funktionen verfügbar: **»Netzwerktools«**, **»Update«**, **»Konfigurationsexport«**, **»Restart System/Dienste«**, **»Uhrzeit einstellen«** und **»Backup«**.

Die Aktionen werden jeweils auf dem System ausgeführt, auf dessen Konfigurationsobjekt man sich befindet. Ist dies nicht das lokale System, so muss eine Master-Slave Verbindung mit dem System bestehen, damit die Management-Appliance die Aktionen auf dem entsprechenden Zielsystem bzw. Host ausführen kann. Besteht keine Management-Verbindung, so wird die Fehlermeldung **»Host ist nicht online«** ausgegeben.

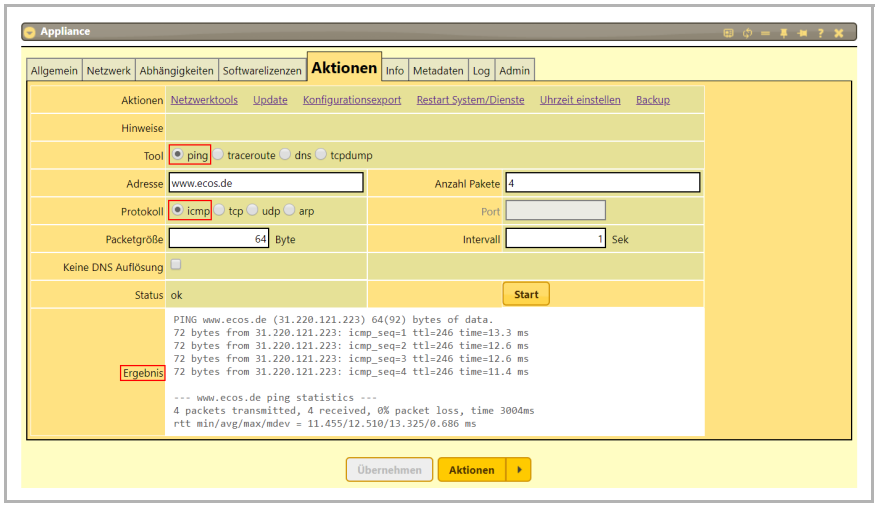
Zu welchen Systemen aktuell eine Verbindung besteht, kann im **»ECOS System Connector«** auf dem Reiter **»Verbindung«** eingesehen werden.

4.1.1 Netzwerktools

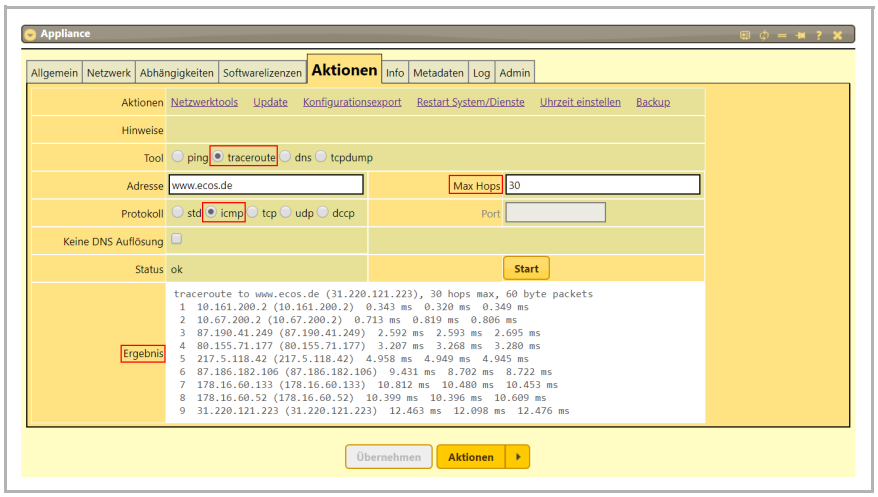
Netzwerktools enthalten Werkzeuge, die bei Verbindungs- bzw. Kommunikationsproblemen zwischen den beteiligten Systemen eine schnelle Fehleranalyse unterstützen. Zur Auswahl stehen **»ping«, »traceroute«**, **»dns«** und **»tcpdump«** zur Verfügung.

Die Erreichbarkeit, RTD (Round Trip Delay) sowie Packet Loss zu einem Zielsystem im Netzwerk kann mit dem Tool **»ping«** geprüft werden. Dazu kann die standardmäßige Ping-Implementierung (via ICMP) eingesetzt werden. Paketgröße (Standard 64 Byte), Anzahl der Pakete (Standard 4) sowie das Intervall (Standard 1 Sekunde) können über die gleichnamigen Felder eingestellt werden.

Ein Erreichbarkeitstest auf Basis **»tcp«**, **»udp«** oder **»arp«** wird mit dem Tool NPING realisiert.



Zur Überprüfung des Routings zu einem Zielsystem resp. zur näheren Analyse von Erreichbarkeitsproblemen steht das Tool **»traceroute«** zur Verfügung. Als Protokoll kann **»std«**, **»icmp«**, **»tcp«**, »udp« oder **»dccp«** verwendet werden. Die maximale Anzahl der Zwischenstationen auf der Route kann mit **»Max. Hops«** (Standard 30) begrenzt werden.



Mit dem Netzwerktool **»dns«** wird die Namensauflösung und Umsetzung in IP-Adressen aus Sicht des Hosts überprüft. Über das Feld **»Record Typ«** werden die verschiedenen Einträge aus dem Domain Name Service abgefragt (**»A«** -Adress Record, **»NS«** - Name Server Record, **»MX«** - Mail eXchange Record,**»SOA«** - Start Of Authority, **»TXT"** - TeXt Record oder **»PTR«** - PoinTeR Record).

Statt des im System (Resolv-Konfiguration) standardmäßig eingestellten DNS-

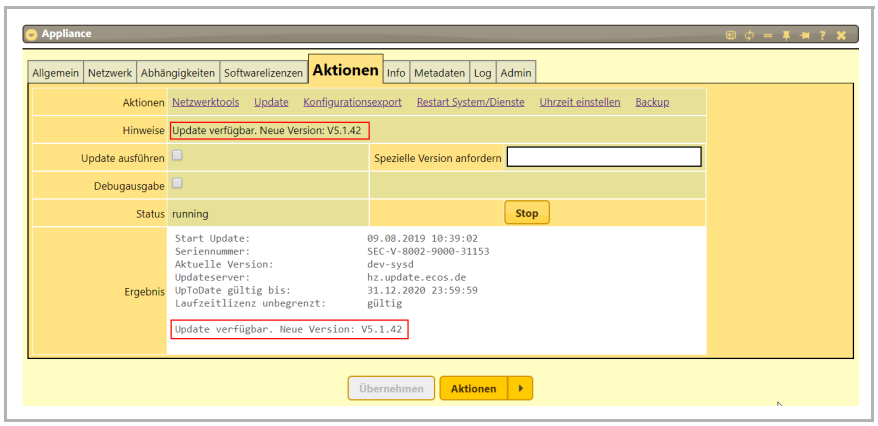
Servers können andere DNS-Server via **»DNS-Server«** zum Test der Namensauflösung verwendet werden.

Mittels **»tcpdump«** kann die Kommunikation über die Netzwerkschnittstellen auf Paketebene analysiert werden. Hierzu wird bei **»Netzwerkkarte«** eine bestimmte Netzwerkkarte oder alle Netzwerkkarten **»any«** ausgewählt. Bei **»Max. Aufnahmezeit«** wird die Zeit in Sekunden, in der die Aufzeichnung laufen soll, eingetragen. Nach dieser Zeit wird die Aufzeichnung gestoppt.

Der aufgezeichnete Netzwerkverkehr kann mittels Filterkriterien auf bestimmte Protokolltypen (z.B. icmp) oder Portnummern (z.B. 22 für SSH) eingegrenzt werden. Mehrere Filterkriterien können dabei durch **»and«** sowie **»or«** verknüpft werden.

4.1.2 Update

Über den Link **»Update«** kann das System aktualisiert werden. Das Update des Systems wird durch Klicken auf die Schaltfläche **»Start«** ausgelöst. Hierzu fragt das System bei dem konfigurierten Software Update Server → *Siehe „3.4.5 | Software-Update-Server" auf Seite 55*, ob eine aktuelle Version zur Verfügung steht. Über **»Hinweise«** und **»Ergebnis«** wird dies mitgeteilt. Dabei wird auch die verfügbare Version Nummer angezeigt.

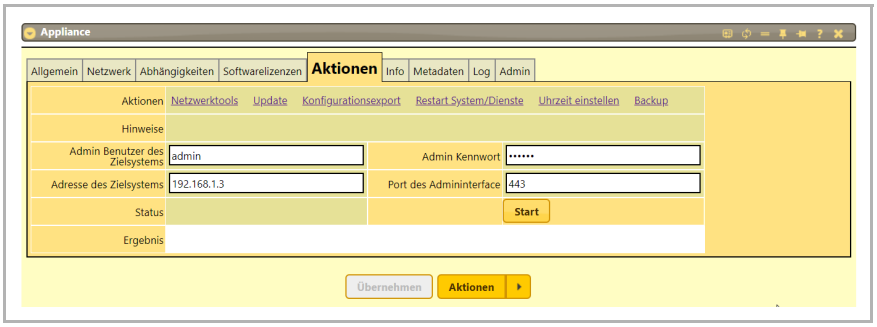


Ist ein Haken bei **»Update ausführen«** gesetzt, wird die neueste Version des Systems, die der Update Server anbietet, durch Klicken auf die Schaltfläche **»Start«** heruntergeladen und installiert.

Über **»Spezielle Version anfordern«** wird die gewünschte Version des Systems eingetragen. Das System prüft deren Verfügbarkeit und bezieht diese, wenn möglich. Die Version muss im Format Vn.n.n z.B. V6.0.53 angegeben werden.

4.1.3 Konfigurationsexport

Über den Link **»Konfigurationsexport«** kann die Konfiguration für einen Bootstick oder eine Appliance an das gewünschte System übertragen werden. Hierzu müssen die entsprechende Felder des Formulars ausgefüllt werden.



Bei »**Admin Benutzer des Zielsystems**« und **»Admin Kennwort«** werden der Benutzername und das Kennwort für den administrativen Zugang des Zielsystems (z.B. Bootstick) eingetragen. → *Siehe „3.1 | Admin-Benutzer" auf Seite 43*.

Bei **»Adresse des Zielsystems«** wird die IP-Adresse des Bootsticks oder gegebenenfalls einer anderen Appliance eingegeben. Bei **»Port des Admininterface«** wird der erreichbare Port eingetragen. Der Standard Port für einen Bootstick ist 443, für eine Appliance 543.

Wird auf **»Start«** gedrückt, wird die Konfiguration an das Zielsystem übertragen.

Das Zielsystem muss (über die angegebene Adresse und den angegebenen Port) von der Appliance aus erreicht werden können. Außerdem muss vor dem Übertragen die Master-Slave Verbindung korrekt konfiguriert werden → *Siehe „9.2.2 | ECOS System Connector für SBS einrichten" auf Seite 104*. Ebenfalls muss es für das Zielsystem möglich sein, die Master-Slave Verbindung aufzubauen. Hierfür muss eine entsprechende Netzwerkverbindung vom Zielsystem zur Appliance möglich sein.

Standardmäßig erfolgt diese Verbindung auf Port 909. Der Port kann aber im **»ECOS System Connector«** geändert werden.

4.1.4 Restart System/Dienste

Wird ein Neustart des Systems oder einzelner Dienste gewünscht, erfolgt dies über **»Restart System/Dienste«**.

Bei **»Verwaltungsdienste neu starten«** werden nur die Verwaltungsdienste neu gestartet. Dies führt zu keinerlei Unterbrechung des laufenden Betriebs.

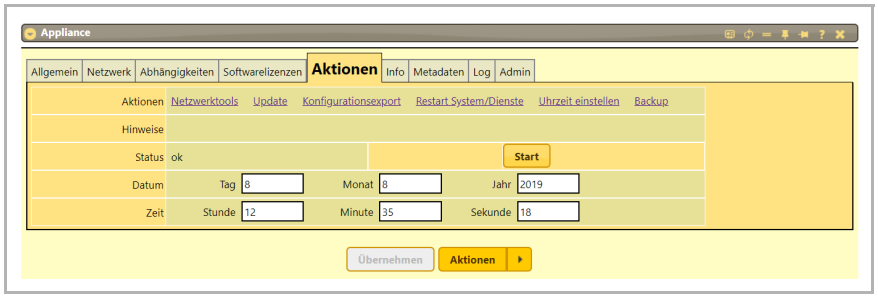
Bei **»Konfiguration neu erzeugen«** wird geprüft, ob die vom System erzeugte Konfiguration den aktuellen Einstellungen entspricht. Bei Differenzen wird die Konfiguration des Systems aktualisiert. Einstellungen werden dadurch nicht geändert.

Bei **»System neu starten«** wird das System neu gestartet.

Das System kann mittels **»System ausschalten«** heruntergefahren werden.

4.1.5 Uhrzeit einstellen

Über **»Uhrzeit einstellen«** werden das Datum und die Zeit des Systems konfiguriert. Die aktuelle Zeit wird durch einen Klick auf die Schaltfläche **»Start«** in den entsprechenden Feldern angezeigt. Wird in den Datum- und Zeitfelder eine Zeit eingegeben. Wird auf die Schaltfläche **»Start«** gedrückt, wird die Uhrzeit des Systems aktualisiert.



4.1.6 Backup

Es besteht die Möglichkeit ein Backup der Konfiguration manuell zu starten. Einmal pro Tag startet das System auch automatisch ein Backup der Konfiguration und speichert es auf der lokalen Platte.

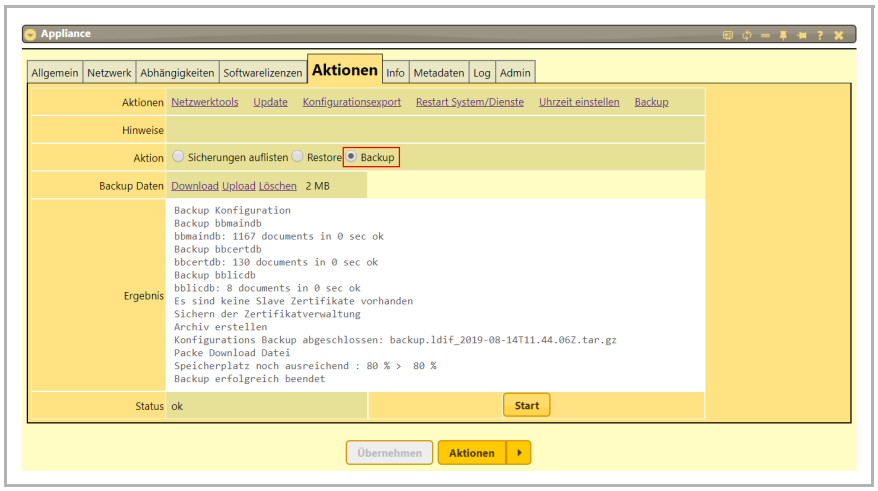
Mittels der Auswahl **»Sicherungen auflisten«** und dem Klick auf die Schaltfläche **»Start« ,** kann eine Liste aller auf der lokalen Platte gespeicherten Backups, angezeigt werden.

»Restore« dient dazu ein Backup wiederherzustellen. Wurden vorher die Backupdateien aufgelistet, so kann bei **»Datei für Restore«** das gewünschte Backup ausgewählt werden. Möglich ist auch, über **»Backup Daten«** bei dem Link **»Upload«** eine Datei mit einem Backup hochzuladen.

Durch Drücken auf die Schaltfläche **»Start«** wird das Zurückspielen der Konfiguration gestartet. Zum Abschluss des Restorevorgangs, werden die Verwaltungsdienste neu gestartet, um die zurückgespielte Konfiguration zu aktivieren. In dieser Zeit ist die Administrationsoberfläche des Systems nicht erreichbar.

Zu beachten ist, dass durch das Zurückspielen der Konfiguration, auch eine ggf. geänderte Netzwerkkonfiguration aktiv wird.

Wird **»Backup«** ausgewählt und anschließend die Schaltfläche **»Start«** gedrückt, wird ein Backup erstellt. Bei **»Backup Daten«** kann das Backup über den Link **»Download«** heruntergeladen werden. Das Backup wird immer auch auf der lokalen Platte gespeichert. Wenn nicht mehr ausreichend Speicherplatz zur Verfügung steht, so wird die älteste Backup-Datei gelöscht.



4.2 Registerkarte Info

Unter der Registerkarte **»Info«** werden Informationen über das System angezeigt. Die Informationen werden jeweils auf dem System ermittelt, auf dessen Konfigurationsobjekt man sich befindet. Ist dies nicht das lokale System, so muss eine

Master-Slave Verbindung mit dem System bestehen, damit die Management-Appliance die Informationen vom entsprechenden Slave abrufen kann. Besteht keine Management-Verbindung, so wird die Fehlermeldung **»Host ist nicht online«** ausgegeben.

Zu welchen Systemen aktuell eine Verbindung besteht, kann im **»ECOS System Connector«** auf dem Reiter **»Verbindung«** angezeigt werden.

4.2.1 Plattenplatz

Über **»Plattenplatz«** wird über die Größe und Füllstand der Platte sowie deren Partitionen angezeigt.

4.2.2 Prozesse

Bei **»Prozesse«** werden alle aktuelle laufende Prozesse auf dem System angezeigt.

4.2.3 Speichernutzung

Über die **»Speichernutzung«** wird der Arbeitsspeicher des Systems dargestellt. Dies zeigt wie der Speicher der Maschine ausgelastet ist.

4.2.4 CPU Nutzung

Die **»CPU Nutzung«** zeigt die aktuelle Auslastung des Prozessors auf dem System.

4.2.5 Routen

Über **»Routen«** werden alle aktiven Routen angezeigt.

4.2.6 ARP Tabelle

Über die **»ARP Tabelle«** wird die ARP-Tabelle ausgegeben, diese zeigt die dem System bekannten IP-Adresse anderer Systeme und die dazugehörigen MAC-Adressen an.

4.2.7 PCI Geräte

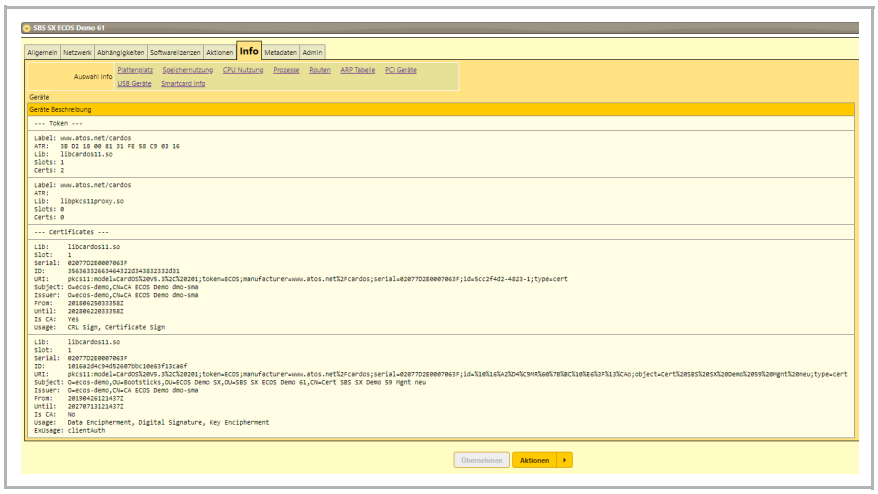
Über **»PCI Geräte«** werden alle PCI-Geräte des Rechners angezeigt.

4.2.8 USB Geräte

Über **»USB Geräte«** werden alle am System angeschlossenen USB-Geräte angezeigt. Die angezeigten Vendor- und Product-ID, sowie die Seriennummer, können verwendet werden, um den Zugriff auf Massenspeicher auf dem Bootstick einzuschränken.

→ *Siehe „9.5.2 | Massenspeicher" auf Seite 124.*

Über **»Smartcard Info«** werden, falls vorhanden, Informationen über die Smartcard und die darauf befindlichen Zertifikate eines Bootsticks angezeigt.

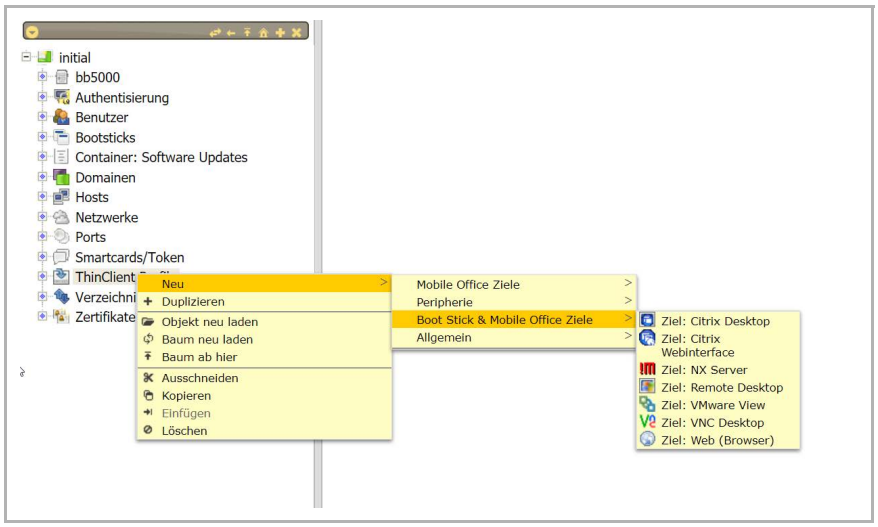


5 Ziele

5.1 Allgemeines zum Ziel-Objekt

Um über einen Bootstick den Remotezugriff auf einen Terminalserver oder ein anderes Zielsystem zu ermöglichen, müssen Verbindungsprofile, sog. Ziele, angelegt werden. Ziele sind die Systeme, auf die der eigentliche Zugriff des Benutzers erfolgen soll. In den dazu gehörigen Konfigurationsobjekten werden die nötigen Informationen zum Verbindungsaufbau hinterlegt.

Sämtliche Ziele werden unterhalb des Konfigurationsobjekts vom Typ **» Container: Ziele «** angelegt. Der Container trägt standardmäßig den Namen **» Ziele «**. Der Container **» Ziele «** enthält eine Übersicht aller angelegten Ziele. Unterhalb des Containers befinden sich die bereits vorhandenen Ziel-Objekte. Hier können neue Ziel-Objekte angelegt und konfiguriert werden. Unterstützte Zielsysteme beinhalten
u. a. Microsoft Terminalserver, Citrix, VMware Horizon und Webserver.

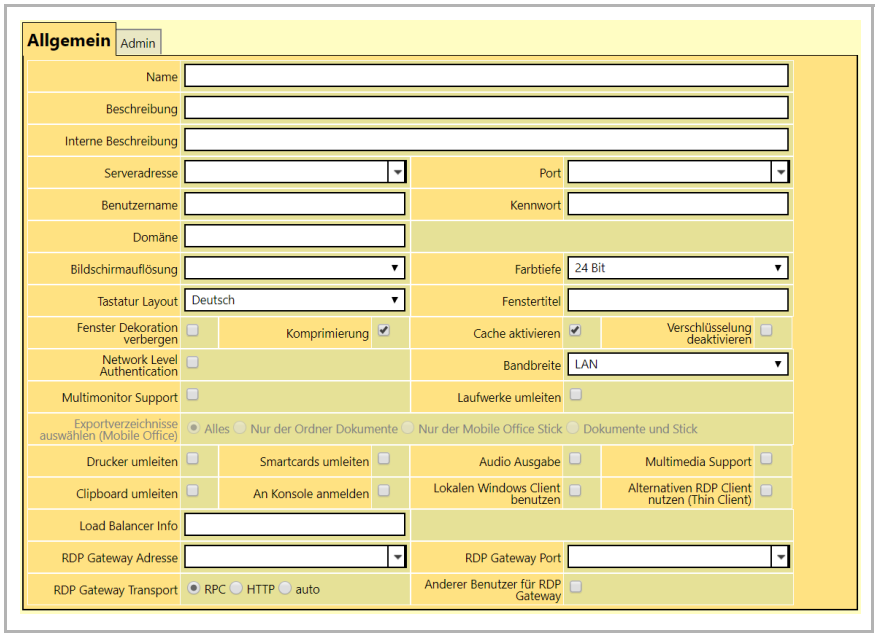


5.2 RDP

Mithilfe des Remote Desktop Protocols (RDP) kann über den ECOS Bootstick auf einen Terminalserver zugegriffen werden. Hierzu wird ein neues Konfigurationsobjekt **» Ziel: Remote Desktop «** unter dem Container **» Ziele «** angelegt.

Jedes RDP-Zielobjekt benötigt einen Namen, unter dem es gespeichert ist und der

dem Benutzer später im Zielauswahl-Fenster angezeigt wird. Optional können eine Beschreibung und eine interne Beschreibung des RDP-Objektes ergänzt werden. Die Beschreibung wird ebenfalls dem Benutzer des ECOS Secure Boot Stick angezeigt.



Im Feld **» Serveradresse «** wird die Hostadresse des Terminalservers angegeben, auf den der Remotezugriff erfolgen soll. Im Feld **» Port «** kann ein alternativer Port spezifiziert werden, falls nicht der Standard-RDP-Port genutzt werden soll.

Optional können Benutzername und Kennwort zur Authentifizierung am Terminalserver hinterlegt werden. Bei korrekter Vorbelegung erfolgt die Anmeldung am Terminalserver bei Aufbau der RDP-Verbindung automatisch und muss nicht vom Benutzer manuell durchgeführt werden. Wird lediglich der Benutzername angegeben, wird dieser im Anmeldefenster vorgegeben, sodass der Benutzer nur noch das Kennwort eintragen muss.

Ebenso kann ein RDP-Gateway angegeben werden, über das der RDP-Server erreicht werden kann. Hierzu werden im Formular des RDP-Konfigurationsobjektes die Felder **» RDP Gateway Adresse «**, **» RDP Gateway Port «** und **» RDP Gateway Transport «** ausgefüllt. Des Weiteren kann ein separater Benutzer zur Authentifizierung am RDP-Gateway verwendet werden. Durch Setzen des Hakens bei **» Anderer Benutzer für RDP Gateway «** erscheint ein Untermenü, in dem dieser konfiguriert werden kann.

Im Formular des RDP-Zielobjektes werden auch gewünschte Anzeigeeinstellun-

gen vorgenommen. Hier lassen sich Bildschirmauflösung, Farbtiefe und Fenstertitel festlegen. Erweiterte Optionen können im Formular durch das Setzen des Hakens in den entsprechenden Feldern konfiguriert werden.

5.3 Citrix

Zu den unterstützten Zielsystemen gehört u. a. Citrix (XenApp, XenDesktop). Neue Citrix-Zielobjekte lassen sich im Container **» Ziele «** erstellen. Zur Auswahl stehen die Ziele **» Citrix Desktop «** und **» Citrix Web «**. Das Citrix Desktop-Objekt lässt sich sowohl als Server, als auch als freigegebene Anwendung sowie für den Zugriff auf Storefront konfigurieren.

5.3.1 Citrix Desktop

Um sich direkt zu einem Citrix Desktop und ohne den Umweg über Anmeldung am Webinterface zu verbinden, muss das Objekt **» Ziel: Citrix Desktop «** angelegt werden.

Als Typ entweder **» Freigegebene Anwendung «** oder **» Storefront «** auswählen. **» Freigegebene Anwendung «** verwendet die **» Program Neighbourhood «** und funktioniert nur in XenApp bis Version 7.5. **» Storefront «** wiederum funktioniert nur bei neueren XenApp-Versionen. Der dritte Typ **» Server «** kommt nur in Spezialfällen zum Einsatz. Hier wird keine Verbindung zur Citrix Farm, sondern direkt zu einem bestimmten Citrix-Server aufgebaut. Es findet also kein Load Balancing innerhalb der Farm statt.

In der Konfiguration **» Freigegebene Anwendung «** verbindet sich der Bootstick über die im Feld **» Serveradresse «** angegebene IP-Adresse (oder Gruppe von IP-Adressen) mit einer Serverfarm und bekommt dort einen freien Server zugewiesen. Hierbei muss der Anwendungs- bzw. Desktopname der Anwendung bzw. des Desktops, zu der bzw. zu dem eine Verbindung aufgebaut werden soll, im Feld **» Anwendungsname «** angegeben werden. Der Name muss mit dem im Citrix-Ser-

ver konfigurierten Namen übereinstimmen.

Im Reiter **» Allgemein «** muss das für die Citrix-Verbindung gewünschte Protokoll spezifiziert werden. Zur Auswahl stehen **» TCP/IP «**, **» TCP/IP + HTTPS «** und **» SSL/TSL + HTTPS «**. Optional lässt sich hier auch der Port eintragen, über den die Verbindung hergestellt werden soll. Andernfalls wird der Standard-Port verwendet.

In den Reitern **» Optionen «**, **» Proxy «**, **» Fenster «**, **» Benutzerdaten «**, **» Automatische Verbindung «** und **» Erweiterungen «** lassen sich tiefer gehende Einstellungen vornehmen. Diese gelten allerdings nur für die Einstellung **» freigegebene Anwendung «**.

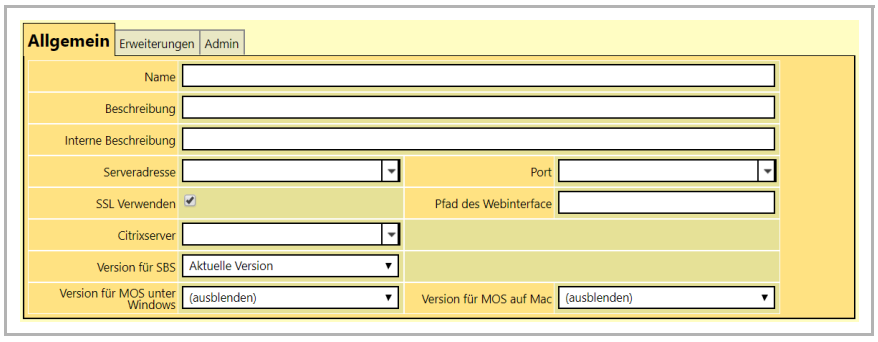
Um eine direkte Verbindung zu einem Desktop oder eine Anwendung über einen Storefront Store aufzubauen, die Option **» Storefront «** als Typ im Reiter **» Allgemein «** des Formulars auswählen. Des Weiteren muss ein Anwendungs- oder Desktopname, so wie er im Citrix-Server konfiguriert ist, angegeben werden. Ist der Store unter einem speziellen Pfad zu erreichen, kann dieser im Feld **» Pfad des Stores «** angegeben werden. Durch Entfernen des Hakens bei **» SSL verwenden «** kann die Verbindung zum Store auch per **» http «** aufgebaut werden.

Erfolgt die Verbindung SSL-Verschlüsselt, so ist es zusätzlich notwendig die CA's die das Server-Zertifikat signiert haben, dem Bootstick bekannt zu machen, damit der Citrix-Client, das Server-Zertifikat prüfen kann. Dies erfolgt durch anlegen von CA Objekten und hochladen der entsprechenden Zertifikate. → *Siehe „7 | Zertifikate" auf Seite 75*.

Erweiterte Einstellungen werden im Reiter **» Erweiterungen «** vorgenommen.

5.3.2 Citrix Web

Um die Verbindung zur Citrix Farm über das Citrix-Webinterface oder einen NetScaler herzustellen, das Objekt **» Ziel: Citrix Webinterface «** anlegen.



Hierfür muss im Reiter **» Allgemein «** die Serveradresse des gewünschten Webservers angegeben werden. Des Weiteren lassen sich der Port, über den die Verbindung hergestellt wird, der Pfad des Webinterfaces und eine mögliche SSL-Verschlüsselung konfigurieren.

Erfolgt die Verbindung nicht über einen NetScaler, muss der Citrix-Client auf dem Bootstick direkt mit dem Server der Citrix Farm kommunizieren können. Dazu muss in dem Feld **» Adresse der Citrix-Server «** das Netz, in dem die Citrix-Server stehen oder eine Liste von Citrix Hosts angegeben werden, damit die Firewall auf dem Bootstick entsprechend freigeschaltet werden kann.

Erfolgt die Verbindung SSL-verschlüsselt, so ist es zusätzlich notwendig, die CA's, die das Server-Zertifikat signiert haben, dem Bootstick zuzuordnen, damit der Citrix-Client das Server-Zertifikat prüfen kann. Dies erfolgt durch Anlegen von CA-Objekten und Hochladen der entsprechenden Zertifikate.
→ *Siehe „7 | Zertifikate" auf Seite 75*.

Erweiterte Einstellungen werden im Reiter **» Erweiterungen «** vorgenommen.

5.4 VMware

Um eine Verbindung zu VMware Horizon aufzubauen, das Objekt **» Ziel: VMware View «** anlegen. Im Feld **» Serveradresse «** wird die IP-Adresse des gewünschten Terminalservers angegeben und im Feld „Name des Desktops die Bezeichnung des Desktops, zu dem eine Verbindung hergestellt werden soll.

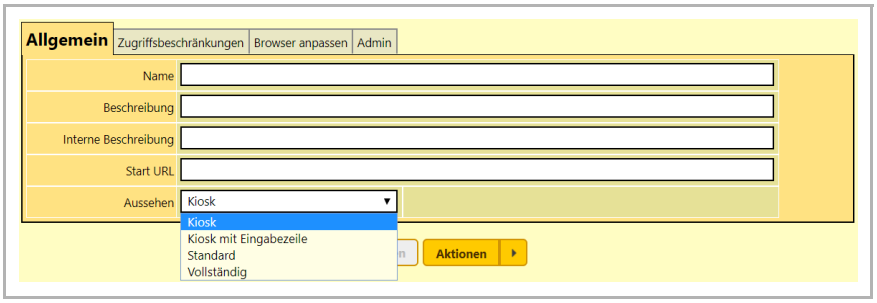
Es kann zwischen verschiedenen Verbindungsprotokollen gewählt werden. Zur Auswahl stehen **» RDP «**, **» PCoIP «** und **» BLAST «**

Optional können Benutzername und Kennwort zur Authentifizierung am Terminalserver hinterlegt werden. Bei korrekter Vorbelegung erfolgt die Anmeldung am Terminalserver bei Aufbau der Verbindung automatisch und muss nicht vom Benutzer manuell durchgeführt werden. Wird lediglich der Benutzername angegeben, wird dieser im Anmeldefenster vorgegeben, sodass der Benutzer nur noch das Kennwort eintragen muss.

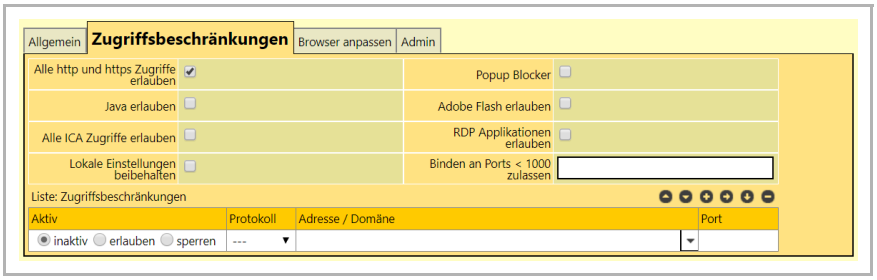
5.5 Browser

Um auf einen Web-Server zuzugreifen, das Objekt **» Ziel: Web (Browser) «** anlegen.

Über das Dropdown-Menü **» Aussehen «** lassen sich unterschiedliche Varianten des Browsers auswählen. Im Kiosk-Modus erhält der User lediglich Zugriff auf die Website, die im Feld **» Start-URL «** definiert ist. Der Modus **» Kiosk mit Eingabezeile «** erlaubt dem User zusätzlich den Zugriff auf die Eingabezeile im Browser und dadurch die Möglichkeit, andere Webseiten neben der Start-URL aufzurufen. Im Modus **» Standard «** steht dem Benutzer ein nahezu vollständiger Browser, aber ohne Zugriff auf das Dateisystem zur Verfügung. Die Option **» Vollständig «** erlaubt dem Benutzer das Zugreifen auf den Browser mit vollem Funktionsumfang.



Mithilfe des Reiters **» Zugriffsbeschränkungen «** kann gezielt eingestellt werden, welche Webseiten der Benutzer aufrufen darf. Ist die Option **» Alle http und https Zugriffe erlauben «** aktiviert, darf der Benutzer jede beliebige Webseite aufrufen. Dies kann über die Liste **» Zugriffsbeschränkungen «** eingeschränkt werden. Hier kann der Zugriff auf einzelne IP-Adressen und Domänen verboten werden. Umgekehrt kann man auch über die Liste den Zugriff auf einzelne IP-Adressen erlauben, wenn der allgemeine Zugriff durch die deaktivierte Option **» Alle http und https Zugriffe erlauben «** verboten wurde.



Des Weiteren können im Reiter **» Zugriffsbeschränkungen «** Plug-Ins wie RDP oder Java erlaubt bzw. verboten werden. Bei Aktivierung des Java Plug-Ins müssen zusätzlich im Untermenü **» Für Java freigegebene URLs «** die Webseiten spezifiziert werden, denen man das Ausführen von Java-Applikationen gestatten möchte.

Über den Reiter **» Browser anpassen «** können erweiterte Einstellungen vorgenommen werden, wie z. B. der Import von Firefox-Einstellungen im Feld **» Preferences «**.

5.6 Hotspot

Um einen Internetzugang über einen Hotspot zu ermöglichen, muss ein Web-Browser im Kiosk-Modus als Ziel konfiguriert und eine Start-URL vergeben werden (z. B. die Firmenwebsite). Nach Starten des Bootsticks kann über die Netzwerkeinstellungen eine Verbindung zum WLAN hergestellt und dann der Browser aufgerufen und die Anmeldung am Hotspot durchgeführt werden. Öffnet sich die Webseite, die als Start-URL angegeben wurde, war die Anmeldung am Hotspot erfolgreich.

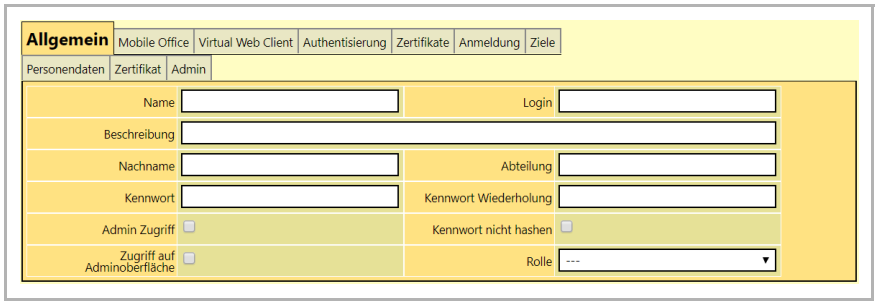
6 Benutzer

Benutzer befinden sich unterhalb des Container-Objekts **» Benutzer «**. Benutzer dienen zur Steuerung des Zugriffs an verschiedenen Stellen. Zum einen kann damit der Zugriff auf die Administrationsoberfläche erlaubt oder teilweise erlaubt werden, zum anderen wird im Benutzerobjekt definiert, auf welche Ziele (Terminalserver etc.) von einem Bootstick aus zugegriffen werden darf.

Im Auslieferungszustand ist der Benutzer **» admin «** vorgegeben und mit Admin-Rechten ausgestattet. Administratoren haben uneingeschränkten Zugriff auf sämtliche Konfigurationsobjekte und weitere Funktionen.

Um einen neuen Benutzer anzulegen, mit der rechten Maustaste auf den Container **» Benutzer «** klicken, unter **» Neu «** das Konfigurationsobjekt **» Benutzer «** auswählen.

Im Reiter **» Allgemein «** wird dem neuen Benutzer ein Name zugewiesen. Durch Setzen eines Hakens bei **» Admin-Zugriff «** oder **» Zugriff auf «** können dem Benutzer Administrationsrechte verliehen werden.



Für eine genauere Beschreibung der möglichen Vergabe von Berechtigungen.
→ *Siehe „13.8.2 | Benutzern Rollen zuweisen" auf Seite 183*.

Außerdem muss ein Kennwort vergeben werden, welches später zur Authentifizierung des Benutzers an der Administrationsoberfläche dient.

7 Zertifikate

7.1 Allgemeines zur Zertifikatsverwaltung

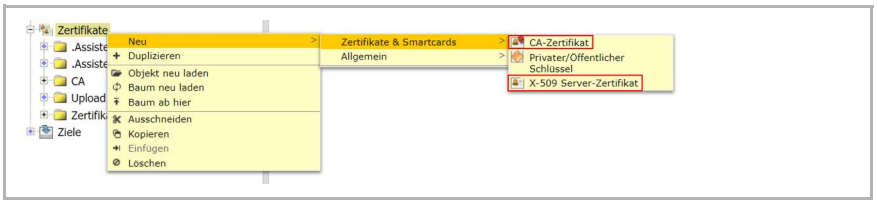
Zur Verwaltung von Zertifikaten können über die Administrationsoberfläche sowohl CA-Zertifikat als auch normale X.509 Zertifikate erstellt werden. Neben dem Objekttyp **»CA-Zertifikat«** gibt es Server- und Benutzerzertifikate. Letztere beiden stellen **»X.509 Zertifikate«** aus, der einzige Unterschied ist, dass das Benutzerzertifikat direkt im bzw. unterhalb eines Benutzers angelegt wird und somit direkt eine Beziehung zu einem bestimmten Benutzer besteht. Grundsätzlich können aber auch mit dem Objekttyp **»X.509 Zertifikat«**, Zertifikate für Benutzer ausgestellt werden.

Es können sowohl Root-CA's wie auch Sub-CA's verwaltet werden und es besteht keine Limitierung bezüglich Anzahl oder Tiefe der Zertifikate bzw. der Hierarchie.

Eine CA oder ein Zertifikat kann dabei grundsätzlich vollständig auf der Appliance erzeugt, von extern importiert oder nur signiert werden.

Je nachdem gehören zu einem Zertifikat ein öffentlicher und/oder ein privater Schlüssel und es können Metainformationen zum Zertifikat verwaltet werden.

Ein Zertifikatsobjekt wird im Baum durch Rechtsklick auf den Container **»Zertifikate> Neu> Zertifikate & Smartcards> CA-Zertifikat«** oder **»Zertifikate> Neu> Zertifikate & Smartcards> X-509 Server-Zertifikat«** angelegt.

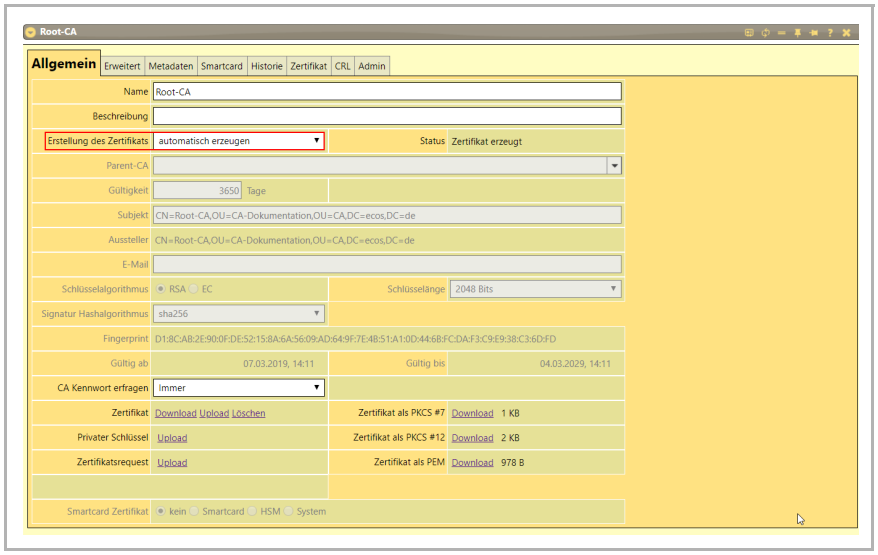


Grundsätzlich wird ein Zertifikat (egal, ob CA oder normales Zertifikat) in zwei Schritten generiert. Zunächst wird das Zertifikatsobjekt in der Konfiguration angelegt und dort werden alle notwendigen Parameter eingestellt. In einem zweiten Schritt wird das eigentliche Zertifikat erzeugt bzw. hochgeladen. Der zweite Schritt, das eigentliche Erzeugen des Zertifikats, wird dabei durch das Feld **»Erstellung des Zertifikats«** bestimmt. Alle Parameter, die Teil eines Zertifikates sind, können nach dessen Erzeugung nicht mehr geändert werden und sind deshalb ausgegraut.

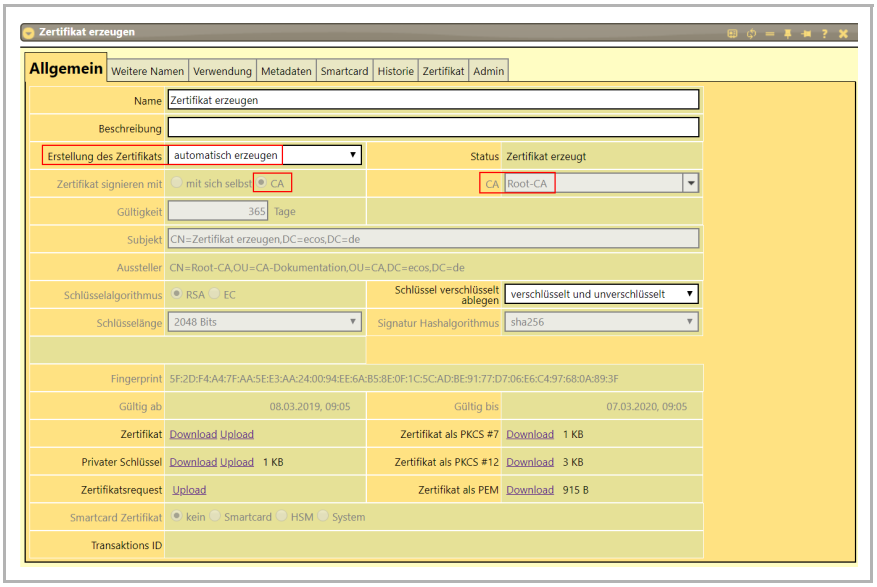
7.1.1 Erstellen einer eigenen Zertifikatshierarchie

Um eine Zertifikatshierarchie zu erstellen, muss zunächst eine Root-CA erzeugt werden. Dazu muss ein CA-Objekt angelegt werden und die gewünschten Parameter, wie **»Gültigkeit«**, **»Subjekt«**, **»Schlüsselalgorithmus«**, **»Schlüssellänge«** (oder EC-Name) müssen ausgefüllt werden. Anschließend wird im Feld **»Erstellung des Zertifikats«** die Auswahl **»automatisch erzeugen«** selektiert. Wird das Feld **»Subjekt«** leer gelassen, wird es automatisch entsprechend dem vergebenen Namen gefüllt.

→ *Siehe „7.2.3 | Subjekt" auf Seite 79*.



Nun können Zertifikate erzeugt werden, die von dieser CA signiert werden, indem ein neues Zertifikatsobjekt angelegt wird. In diesem neuen Zertifikatsobjekt wird die zuvor erzeugte CA ausgewählt, sowie die übrigen Parameter befüllt. Auch hier wird im Feld **»Erstellung des Zertifikats« »automatisch erzeugen«** ausgewählt. Nach dem Anlegen ist ein neues **»X.509- Zertifikat«** erstellt, dessen einzelne Werte wie Fingerprint und Gültigkeit in den entsprechenden Feldern angezeigt werden.



Der vollständige Inhalt des Zertifikats wird im Reiter **»Zertifikat«** angezeigt.

Das Zertifikat und die dazugehörigen Schlüssel können über die Downloadlinks am unteren Ende des Formulars heruntergeladen werden.

→ *Siehe „7.3 | Dateien hoch- und herunterladen" auf Seite 84*.

Beim Erstellen einer CA bzw. eines Zertifikats müssen je nach Einstellung ggf. Kennwörter für den CA-Schlüssel bzw. den Schlüssel des Zertifikats vorgegeben bzw. eingegeben werden.

Um eine mehrstufige CA-Hierarchie anzulegen, erzeugt man, bevor die Zertifikate erstellt werden, eine oder mehrere Sub-CAs, genauso wie die Root-CA selbst, nur mit dem Unterschied, dass die Root-CA als Parent-CA ausgewählt wird → *Siehe „7.2.1 | CA/Parent-CA" auf Seite 78*. Danach können diese Sub-CAs zum Erstellen von Zertifikaten verwendet werden.

7.2 Die Zertifikatsparameter im Einzelnen

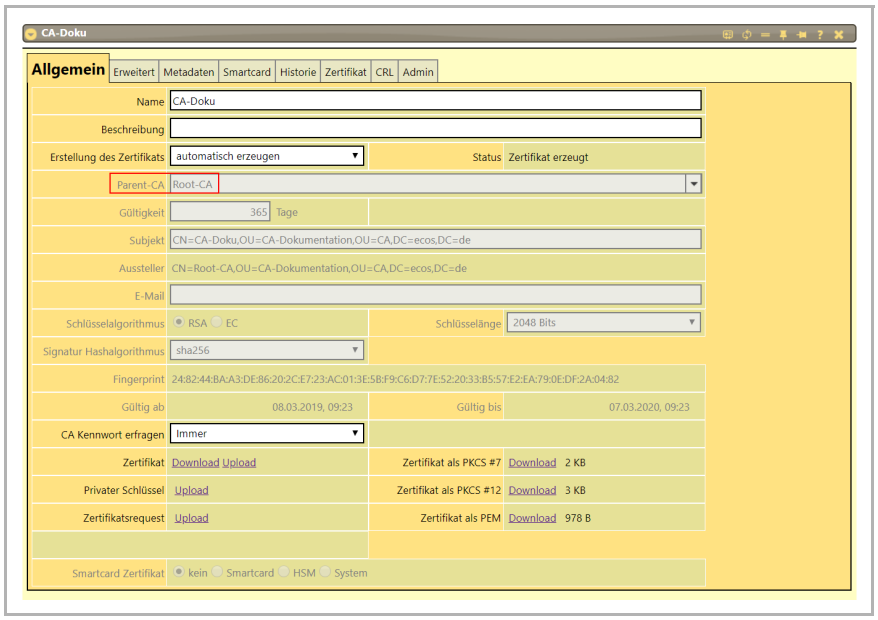
Bei einem Zertifikatsobjekt können, bevor ein Zertifikat erzeugt wird, verschiedene Parameter definiert werden. Die Felder **»Gültigkeit«**, **»Schlüsselalgorithmus«**, **»Schlüssellänge«** und **»Signatur Hashalgorithmus«** werden mit den Standardeinstellungen vorbelegt falls keine Auswahl getroffen wird.

7.2.1 CA/Parent-CA

Die Certificate Authority (CA) oder auch Zertifizierungsstelle signiert Zertifikate, damit man mittels deren öffentlichen Schlüsseln, die Gültigkeit eines Zertifikats prüfen bzw. feststellen kann, ob ein Zertifikat tatsächlich von einer bestimmten CA ausgestellt wurde.

Dementsprechend ist bei jedem Zertifikat anzugeben, mit welcher CA es signiert werden soll. Die CA muss dazu zuvor angelegt und erzeugt oder hochgeladen worden sein.

Im CA-Objekt selbst, kann über das Feld **»Parent-CA«** eine übergeordnete CA ausgewählt werden, mit der wiederum das zu erstellende CA-Zertifikat signiert wird. Die Parent-CA muss dazu zuvor angelegt und erzeugt oder hochgeladen worden sein.



7.2.2 Gültigkeit

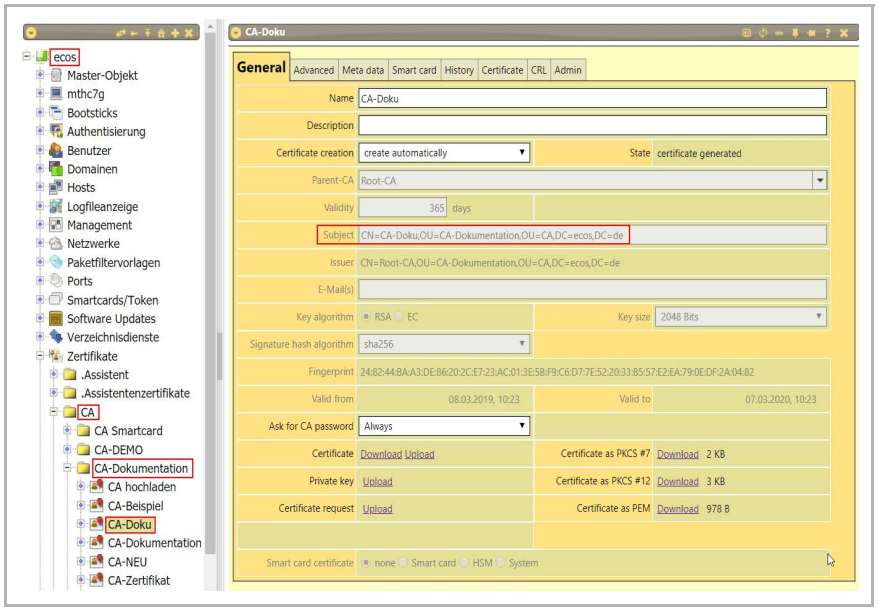
Zertifikate sind nur für eine bestimmte Zeitspanne gültig. Über das Feld **»Gültigkeit«** wird die Gültigkeitsdauer des Zertifikats in **»Tagen«** angegeben. Nach deren Ablauf wird das Zertifikat ungültig. Die Standardeinstellung ist für CAs 3650 Tage und für Zertifikate 365 Tage. Die Gültigkeit eines Zertifikats darf nicht länger sein als die Gültigkeit der CA, die es signiert.

→ *Siehe „7.5.1 | Zertifikate verlängern" auf Seite 88.*

7.2.3 Subjekt

Das Subjekt gibt an, für wen oder was (z.B. Benutzer oder Server) das Zertifikat ausgestellt werden soll. Es ist quasi dessen Name. Es wird in der Form eines Distinguished Name (DN) angegeben. Der DN besteht dabei aus mehreren Attributen, die durch Komma getrennt sind. Mögliche Attribute sind z.B. CN, O, OU, L, S; C, DC, usw.

Falls das Feld nicht ausgefüllt ist, wird das Subjekt automatisch erstellt. Dabei wird der Name des Zertifikatobjektes als CN verwendet, die Container, in der sich das Zertifikat befindet, als OU und das im Top-Level-Zertifikate-Container angegebe Zertifikatssuffix als Suffix angehängt.



7.2.4 Schlüsselalgorithmus

Der zur Generierung der Schlüssel verwendete Algorithmus, wird über **»Schlüsselalgorithmus«** eingestellt. Dabei stehen RSA (Rivest Shamir-Adleman System) oder EC (Elliptic-Curve-Cryptography) zur Verfügung. Die Standardeinstellung ist RSA.

7.2.4.1 Schlüssellänge

Wird der Schlüsselalgorithmus **»RSA«** selektiert, muss über das Feld **»Schlüssellänge«** die Anzahl der Bits für die Schlüsselgenerierung ausgewählt werden. Die

Standardeinstellung ist **»3072 Bits«**. Zur Verwendung für VS-NfD muss die Schlüssellänge mindestens **»3072 Bits«** betragen.

Wird der Schlüssel auf einer Smartcard oder einem Token erzeugt, so ist es wichtig, dass die Hardware die Schlüssellänge unterstützt.

7.2.4.2 Elliptische Kurve

Wird der Schlüsselalgorithmus **»EC«** selektiert, muss über das Feld **»Elliptische Kurve«** die gewünschte elliptische Kurve ausgewählt werden. Die Standardeinstellung ist **»prime256v1«**. Bei elliptischen Kurven sind die Errechnung des Schlüssels, sowie die Kryptooperationen mit dem Schlüssel, schneller und kürzer als bei RSA.

Wird der Schlüssel auf einer Smartcard oder einem Token erzeugt, so ist es wichtig, dass die Hardware die elliptische Kurve unterstützt.

7.2.5 Signatur Hashalgorithmus

Über den **»Signatur Hashalgorithmus«** werden die kryptografischen Hashfunktionen ausgewählt. Diese dienen zur Berechnung der Prüfsumme und zur Erstellung der digitalen Signatur. Die Standardeinstellung ist **»SHA256«**.

7.2.6 Schlüssel verschlüsselt ablegen (nur X.509 Zertifikat)

Bei der Erstellung eines X.509 Zertifikats wird über das Feld **»Schlüssel verschlüsselt ablegen«** eingestellt, ob der private Schlüssel **»verschlüsselt und unverschlüsselt«**, **»nur verschlüsselt«** oder **»nicht verschlüsselt«** angelegt werden soll. Bei **»verschlüsselt und unverschlüsselt«** ist der private Schlüssel in der Datenbank unverschlüsselt abgelegt und wird beim Download mit dem angegebenen Passwort verschlüsselt. Bei **»nur verschlüsselt«** ist der private Schlüssel mit dem Passwort geschützt und in der Datenbank abgelegt. Bei **»nicht verschlüsseln«** ist der private Schlüssel unverschlüsselt in der Datenbank abgelegt. In jedem Fall wird der Schlüssel durch die normalen Sicherungsmechanismen geschützt und der Zugriff unterliegt den eingestellten Zugriffsrechten.

Wird der Schlüssel **»nur verschlüsselt«** oder **»verschlüsselt und unverschlüsselt«** abgelegt, so ist beim Erzeugen des Schlüssels die Eingabe eines Kennwortes notwendig. Dies ist eine zusätzliche Sicherheit für die Schlüssel. Sollen Zertifikate automatisch angelegt werden (z.B. per Verzeichnissynchronisation), ist es aber nicht möglich ein zusätzliches Kennwort einzugeben. In diesem Fall sollte der Schlüssel nur unverschlüsselt abgelegt wer-den.

Dient das Zertifikat z.B. beim SBS zum Verbindungsaufbau bei VPN, so wird, wenn der Schlüssel nur verschlüsselt abgelegt ist, bei jedem Verbindungsaufbau nach dem entsprechenden Kennwort gefragt. Liegt auch eine unverschlüsselte Variante vor, so kann das VPN ohne explizite Eingabe eines Kennwortes gestartet werden.

7.2.7 CA-Kennwort erfragen (nur CA)

Wird ein CA-Zertifikat erstellt, lässt sich über das Auswahl-Menü **»CA-Kennwort erfragen«** festlegen, für welche Aktionen das Kennwort benötigt wird. Zur Auswahl stehen: **»Immer«**, **»Beim Erstellen«**, **»Nie«** und **»Nicht für CRL«**. Bei der Auswahl **»Beim Erstellen«** muss das Kennwort lediglich beim Erstellen neuer Zertifikate angegeben werden. Bei **»Nicht für CRL«** ist die Eingabe des Kennwortes beim Erzeugen der CRL nicht erforderlich. Bei nachträglicher Änderung dieser Einstellung muss das Kennwort eingegeben werden.

7.2.8 Subject Alternative Name (SAN) (nur X.509 Zertifikat)

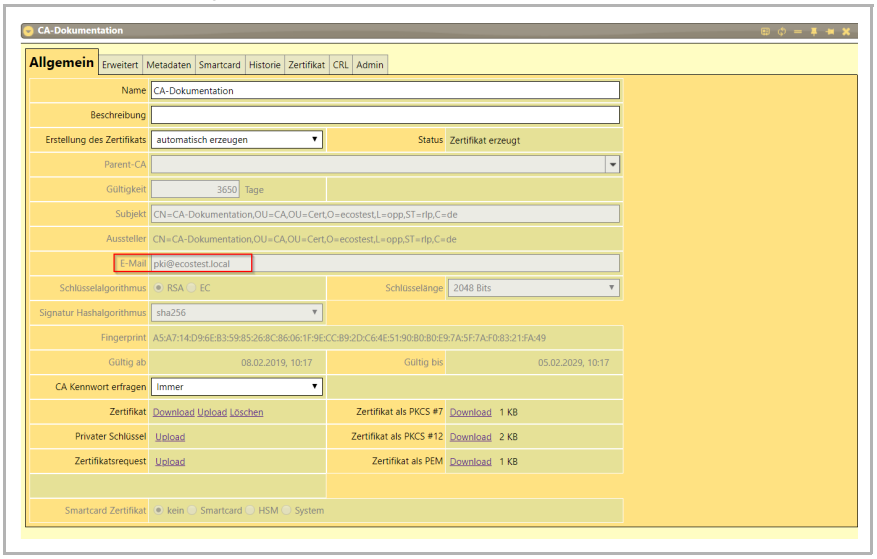
In der Registerkarte **»Weitere Namen«** eines X.509 Zertifikats können zusätzliche Informationen im Zertifikat eingebettet werden. Diese sind alternative Namen zu dem Subjekt, auch SAN genannt und können zusätzliche Elemente wie Emailadresse(n), DNS-Namen, IPv4- oder IPv6-Adresse(n), URI(s) und Other Name beinhalten.

Diese dienen dazu alternative Namen eines Zertifikats anzugeben (z.B. wenn ein Server mehrere Hostnamen hat).

Das Feld **»Other Name«** wird wesentlich für Zertifikate verwendet, die auf einer Smartcard benutzt werden, um sich im Windows-System oder an einem Rechner anzumelden.

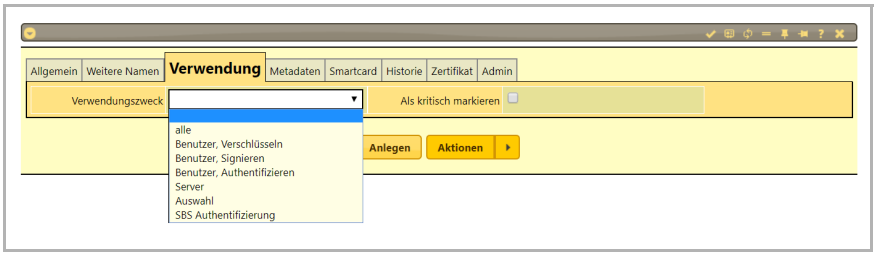
7.2.9 E-Mail (nur CA)

Beim CA-Zertifikat kann zusätzlich eine E-Mail-Adresse eingegeben werden, die Bestandteil des Subjekts wird.

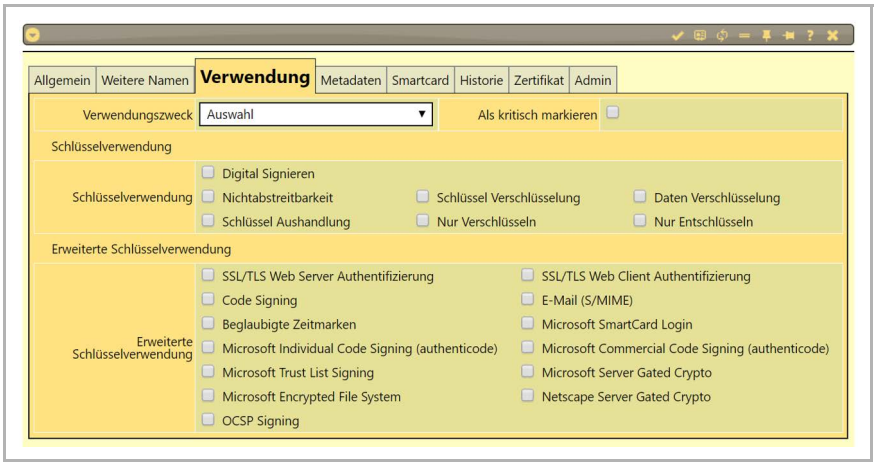


7.2.10 Verwendungszweck

Im Reiter **»Verwendung«** kann der Verwendungszweck des Zertifikats genauer bestimmt werden. Über das Feld **»Verwendungszweck«** werden die Schlüsselverwendung und die erweiterte Schlüsselverwendung selektiert. Es gibt hierzu Vorauswahlen: **»alle«**, **»Benutzer, Verschlüsseln«**, **»Benutzer, Signieren«**, **»Benutzer, Authentifizieren«**, **»Server«**, **»Auswahl«** und **»SBS Authentifizierung«**.



Bei **»alle«** werden alle Schlüsselverwendungen und alle erweitertete Schlüsselverwendungen verwendet. Bei **»Auswahl«** kann der Verwendungszweck genau definiert werden.



Die Schlüsselverwendung und erweitere Schlüsselverwendung der anderen vorgenannten Vorauswahlen sind hier in der unteren Tabelle dargestellt.

	Benutzer, Verschlüsseln	Benutzer, Signieren	Benutzer, Auth.	Server	SBS Auth.
Schlüsselverwendung					
Digitale Signatur		X	X	X	X
Nichtabstreitbarkeit	X	X	X	X	
Schlüssel-verschlüsselung	X	X	X	X	X
Daten-verschlüsselung	X		X	X	X
Erweiterte Schlüsselverwendung					
E-Mail Verschlüsselung	X	X	X		
Microsoft Encrypted File System	X				
TLS Web Client Authentification			X	X	X
Mircrosoft Smartcard Login			X		

Tabelle 7-1 Schlüsselverwendung

7.3 Dateien hoch- und herunterladen

Über das Zertifikat-Formular werden verschiedene Dateien zum Hoch- und Herunterladen angeboten.

7.3.1 Zertifikat

Über das Feld **»Zertifikat«** besteht die Möglichkeit, das Zertifikat mit einem Klick auf den Link **»Download«** binär codiert herunterzuladen oder es mit einem Klick auf den Link **»Upload«** hochzuladen → *Siehe „7.7.2 | Direkter Upload im Zertifikatsobjekt" auf Seite 95*. Ein vorhergehender Upload kann mit einem Klick auf dem Link **»Löschen«** entfernt werden. Beim Hochladen werden diverse Formate akzeptiert (Binär, Base64, PKCS#7, PKCS#12).

7.3.2 Privater Schlüssel

Wurde das Zertifikat auf der Appliance erstellt, so kann hier der private Schlüssel mit einem Klick auf den Link **»Download«** heruntergeladen werden. Wenn das Zertifikat von einer externen CA erstellt wurde, kann der private Schlüssel des Zertifikats mit einem Klick auf den Link **»Upload«** hochgeladen werden → *Siehe „7.6.2 | SUB-CA einer externen CA erzeugen" auf Seite 92*. Grundsätzlich werden sowohl binär codierte wie auch base64 codierte Schlüssel akzeptiert.

7.3.3 Zertifikatsrequest

Der Zertifikatsrequest (CSR- Certificate Signing Request) kann über **»Zertifikatsrequest«** mit einem Klick auf den Link **»Download«** heruntergeladen werden → *Siehe „7.6 | Mit CSRs arbeiten" auf Seite 91*. Dieser Download-Link wird z.B. verwendet, wenn der CSR an eine externe CA gesendet wird, um signiert zu werden.

7.3.4 PKCS7

PKCS#7 ist ein Standard, um verschlüsselte und signierte Daten zusammen mit den nötigen Zusatzinformationen des Zertifikats in einer Datei zu speichern. Der Link **»Download«** bietet die Möglichkeit das Zertifikat selbst, sowie das zugehörige CA-Zertifikat in einer Datei herunterzuladen. Handelt es sich bei dem Zertifikat um ein Root-Zertifikat, ist nur das Zertifikat der CA enthalten.

7.3.5 PKCS12

PKCS#12 ist ein Dateiformat, das dazu benutzt wird, den privaten Schlüssel mit dem zugehörigen Zertifikat passwortgeschützt zu speichern.

Der Link **»Download«** bietet die Möglichkeit, das Zertifikat selbst, sowie den privaten Schlüssel (Kennwort-geschützt) und alle Aussteller des Zertifikats in einer Datei herunterzuladen. Diese ist mit dem Passwort, welches beim Erstellen des Zertifikats angegeben wurde, verschlüsselt.

7.3.6 PEM

Über **»Zertifikat als PEM«** wird das Zertifikat bei einem Klick auf den Link **»Download«** Base64 codiert heruntergeladen.

7.4 Spezielle Einstellungen im CA-Zertifikat

Über die Registerkarte **»Erweitert«** des CA-Zertifikat-Formulars können weitere Einstellungen angegeben werden, um Informationen im Zusammenhang mit der CA zu veröffentlichen.

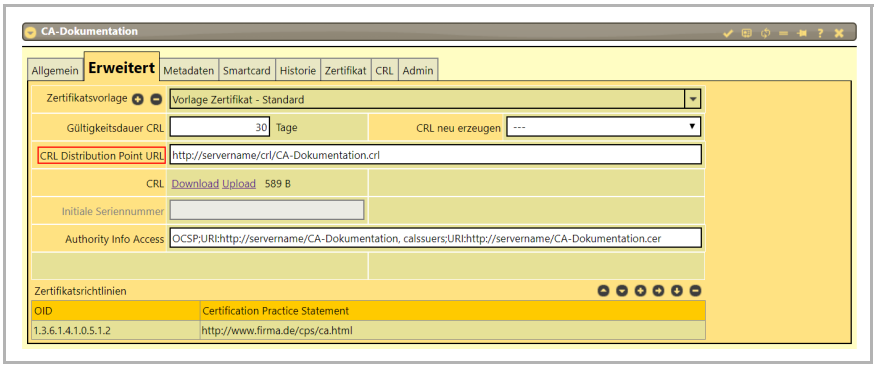
7.4.1 Die Zertifikatssperrliste

Die Authentizität und die Gültigkeit von Zertifikaten müssen überprüfbar sein. Um zu prüfen, ob ein Zertifikat zurückgezogen wurde, kommt eine Zertifikatssperrliste (CRL) zum Einsatz. Alternativ kann ein OCSP Server verwendet werden.

Eine CRL ist eine, von einem CA-Zertifikat, signierte Liste mit den Seriennummern von widerrufenen Zertifikaten. Um anderen Applikationen die Zertifikatssperrliste zur Verfügung zu stellen, wird diese von der Appliance generiert und zum Download bereitgestellt. Über die Sperrlistenverteilungspunkte, auch CRL Distribution Point genannt, kann in den Informationsteil des Zertifikates eine/mehrere URLs geschrieben werden, über die die CRL heruntergeladen werden kann. Dies kann ein öffentlicher Server sein oder auch die Appliance selbst.

Ist ein **»CRL Distribution Point«** eingetragen, so wird der Dateiname, der im CRL Distribution Point angegeben ist, verwendet, um die CRL auf der Appliance selbst zu veröffentlichen. Die Appliance stellt die CRL dann unter folgender URL zur Verfügung:

http://<Servername>/crl/<Name der CA>.crl
https://<Servername>/crl/<Name der CA>.crl



Sind mehrere CRL Distribution Point URLs angegeben, so wird der Name aus der ersten URL für die Publizierung herangezogen.

7.4.1.1 Gültigkeit der CRL

In der Registerkarte **»Erweitert«** des Zertifikat-Objektes wird über das Feld **»Gültigkeitsdauer CRL«** eingegeben, wie lange die CRL für das erzeugte CA-Zertifikat gültig ist.

Damit die CRL auch automatisch neu erzeugt werden kann, bevor dieser Zeitraum abgelaufen ist, ist es notwendig bei **»CA-Kennwort erfragen«** nicht **»Immer«** anzugeben, da ansonsten für die Generierung der CRL die Eingabe des CA-Kennwortes notwendig ist und die CRL dann nur manuell erzeugt werden kann.

Die CRL wird immer beim Zurückziehen eines Zertifikates neu erzeugt.

Um die CRL auch dann neu zu erzeugen, wenn bis zum Ablauf der CRL kein Zertifikat zurückgezogen wurde, kann man eine **»Abfrage mit Aktion«**, die in regelmäßigen Abständen die CRL neu erzeugt, anlegen.

→ *Siehe „7.5.1.1 | Zertifikate und CRL automatisch verlängern" auf Seite 88*.

7.4.2 Authority Info Access

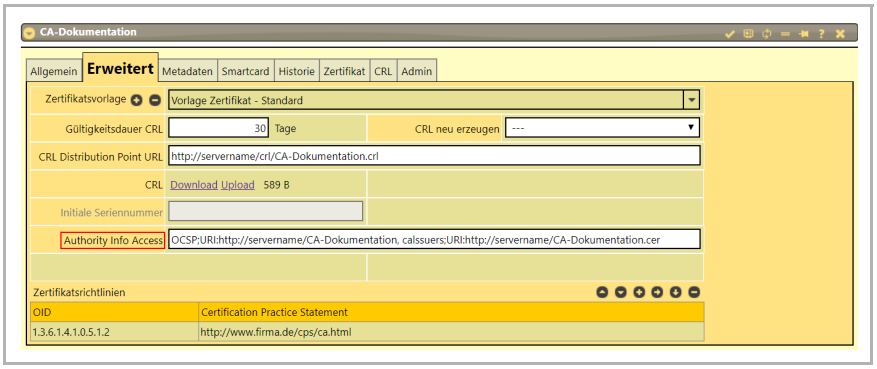
Über das Feld **»Authority Info Access«** (AIA) kann die URL eines OCSP Servers angegeben werden. Dieser erlaubt es Zertifikate online und in Echtzeit zu überprüfen. Damit stellt der OCSP-Server eine Alternative zur Prüfung via CRL da.

Des Weiteren kann die URL angegeben werden, unter der das CA-Zertifikat zum Download bereitgestellt wird. Diese URL wird dann, genauso wie die OCSP URL, in jedes von dieser CA signierte Zertifikat eingebettet.

Hierzu werden die gleichen Veröffentlichungsprotokolle unterstützt wie bei den Sperrlistenverteilungspunkten.

Die OCSP URL muss dabei mit dem Präfix OCSP;URI: angegeben werden und die CA URL mit dem Präfix calssuers;URI: z.B.:

OCSP;URI:http://servername/NameCA, calssuers;URI:http://servername/Name-CA.cer



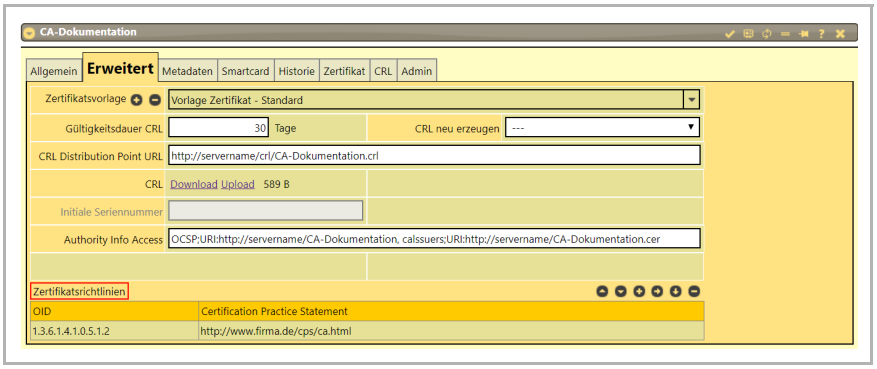
7.4.3 Initiale Seriennummer

Zertifikate besitzen eine Seriennummer, die von der CA vergeben wird. Über das Feld **»Initiale Seriennummer«** wird der Startwert festgelegt. Es handelt sich um einen hexadezimalen Wert und dieser wird bei der Erstellung eines Zertifikates automatisch hoch gezählt.

7.4.4 Zertifikatsrichtlinien

Über die **»Zertifikatsrichtlinien«** können weitere Informationen über die CA veröffentlicht werden, die für den Benutzer eines CA-Zertifikats relevant sind. Die Zertifikatsrichtlinien beinhalten eine Liste von Bestimmungen, die in Zusammenhang mit der Ausstellung, der Nutzung, der Verlängerung oder dem Widerruf eines Zertifikats stehen.

Diese sind über **»Certification Practice Statement«** mittels einer URL abrufbar. Die bei Zertifikatsrichtlinien eingetragenen URLs werden in jedem Zertifikat, das mittels dieser CA signiert wird, hinterlegt.



7.5 Zertifikatslebenszyklus

Zertifikate haben eine zeitliche Gültigkeit und müssen deshalb, wenn sie weiterverwendet werden sollen, verlängert werden. Ebenso ist es möglich Zertifikate durch Zurückziehen vorzeitig für ungültig zu erklären oder temporär auf ungültig zu setzen.

7.5.1 Zertifikate verlängern

Die Gültigkeit eines Zertifikats kann verlängert werden. Hierzu muss das Zertifikat erneut signiert werden. Im Zertifikat-Objekt wird über das Feld **»Erstellung des Zertifikats« »verlängern«** ausgewählt. Nach Klick auf **»Übernehmen«** wird das Zertifikat verlängert. Je nach Einstellung bei Zertifikat und CA wird nach dem Kennwort des bestehenden privaten Schlüssels und einem CA-Kennwort gefragt. Die Felder **»Gültig ab«** und **»Gültig bis«** spiegeln anschließend die neue Gültigkeit wider.

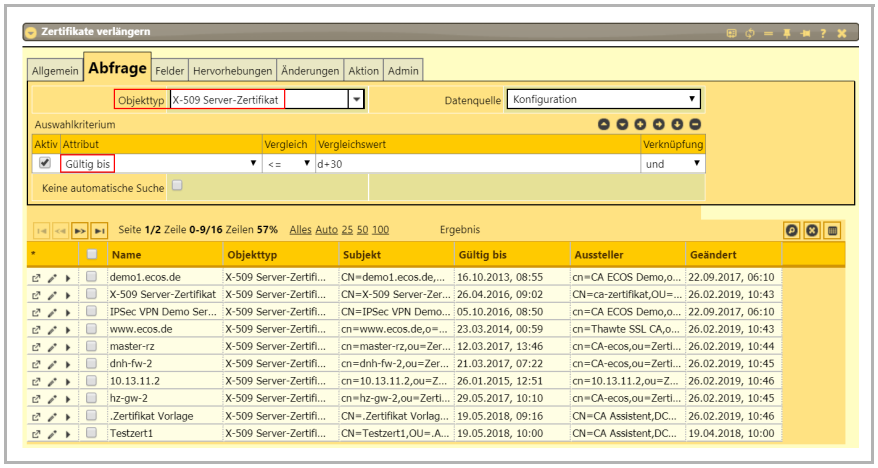
7.5.1.1 Zertifikate und CRL automatisch verlängern

Zertifikate, genauso wie CRL, können mittels des Objektes **»Abfrage mit Aktion«**, automatisch verlängert werden, bevor sie ablaufen. Dieses wird durch Rechtsklick im Baum **»Neu> Allgemein> Abfrage mit Aktion«** angelegt.

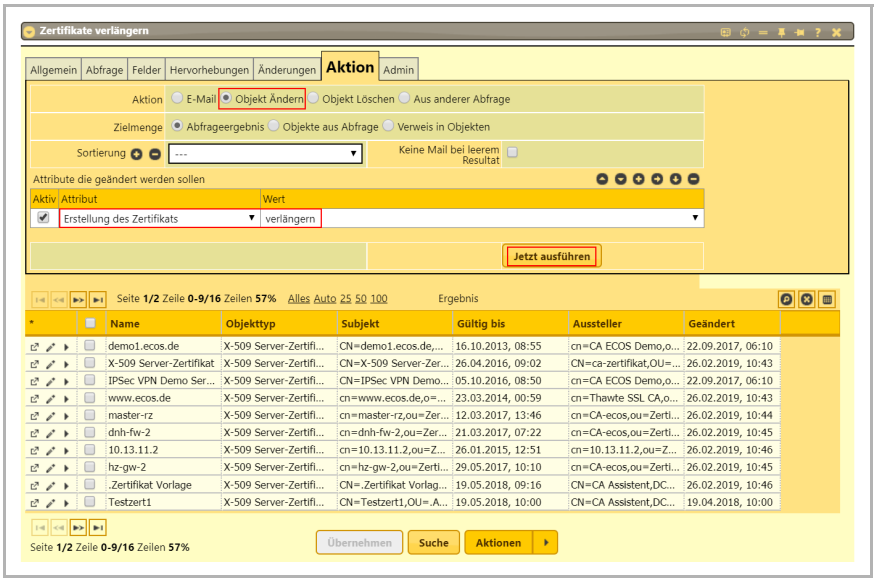
Es wird zunächst eine Abfrage erstellt, die alle Zertifikate, die automatisch verlängert werden sollen, umfasst. Dazu auf der Registerkarte **»Abfrage«** bei **»Objekttyp«** den passenden Zertifikat-Objekttyp (z.B. X.509 Zertifikat oder CA-Zertifikat) auswählen.

Danach in der Tabelle Auswahlkriterium, in der Spalte **»Attribut« »Gültig bis«** und bei **»Vergleich« »<=«** auswählen. Dann den Vergleichswert so setzen, dass Zertifikate aus dem gewünschten Zeitraum angezeigt werden, z.B. führt **»d+60«** dazu, dass alle Zertifikate, die in den nächsten 60 Tagen ablaufen, ausgewählt werden. Zu einer genaueren Erklärung der Auswahlkriterien → *Siehe „13.6 | Abfragen" auf Seite 173*.

Im folgenden Beispiel werden nur X-509 Server-Zertifikate aufgelistet, deren Gültigkeit weniger oder in genau als 30 Tage auslaufen.



Auf der Registerkarte **»Aktion«** wird die Verlängerung ausgeführt, in dem das Attribut **»Erstellung des Zertifikats«** und der Wert **»verlängern«** eingestellt sind. Bei dem Feld **»Aktion«** muss **»Objekt ändern«** ausgewählt werden. Um die **»Aktion«** manuell auszuführen, kann auf die Schaltfläche **»Jetzt ausführen«** geklickt werden.



Um die Verlängerung automatisch zu einem bestimmten Zeitpunkt auszuführen, wird über die Registerkarte **»Änderungen« »Zeitgesteuert«** ausgewählt. Bei **»Ausführungszeit«** wird die Zeit im Crontab-Format eingegeben.

Um die CRL zu verlängern, ist der Vorgang ähnlich wie beim Zertifikate verlängern. Bei der Registerkarte **»Abfrage«** wird **»CA-Zertifikat«** ausgewählt, da die CA die CRL signiert. Bei Auswahlkriterium kann eingeschränkt werden für welche CAs die CRL automatisch verlängert wird. Auf der Registerkarte **»Aktion«** wird das Attribut **»CRL neu erzeugen«** und der Wert **»CRL neu signieren«** ausgewählt. Damit die CRL auch automatisch neu erzeugt werden kann, bevor dieser Zeitraum abgelaufen ist, ist es notwendig im Zertifikat-Objekt bei **»CA-Kennwort erfragen«** nicht **»Immer«** anzugeben, da ansonsten für die Generierung der CRL die Eingabe des CA-Kennwortes notwendig ist und diese dann nur manuell erzeugt werden kann.

7.5.2 Zertifikate zurückziehen

Wenn man die Gültigkeit eines Zertifikats vorzeitig beenden möchte, kann man es zurückziehen. Dies kann z.B. dann notwendig werden, wenn der private Schlüssel öffentlich geworden ist oder der Benutzer, dem das Zertifikat zugeordnet ist, das Unternehmen verlässt. Um das Zertifikat zurückzuziehen, muss bei **»Erstellung des Zertifikats« »zurückziehen«** ausgewählt werden. Falls bei der CA, **»CA-Kennwort erfragen«** nicht auf **»Nie«** steht, so ist dazu die Eingabe des CA-Kennworts notwendig. Nach der Eingabe ändert sich der **»Status«** auf **»Zertifikat zurückgezogen«**. Das Zertifikat ist dann ungültig und wird in die CRL aufgenommen. Ein zurückgezogenes Zertifikat kann nicht wieder gültig werden. Es kann lediglich neu

ausgestellt werden und erhält dabei einen neuen privaten Schlüssel. Das bisherige Zertifikat bleibt dann weiterhin ungültig.

7.5.3 Zertifikate temporär zurückziehen

Nicht immer möchte man das Zertifikat endgültig zurückziehen. Wird bei **»Erstellung des Zertifikats«** über das Auswahlmenü **»vorübergehend ungültig setzen«** ausgewählt, wird das Zertifikat temporär zurückgezogen. Es wird dann ebenfalls in die CRL aufgenommen.

Um das Zertifikat zu einem späteren Zeitpunkt gültig zu setzen, wird bei **»Erstellung des Zertifikats« »wieder gültig setzen«** ausgewählt. Es wird dann wieder aus der CRL entfernt.

7.5.4 Zertifikate im Status vorübergehend ungültig erzeugen

Soll ein Zertifikat erzeugt werden, das aber erst zu einem späteren Zeitpunkt benötigt wird, kann man dieses direkt im Status **»vorübergehend ungültig«** erstellen. Wahlweise kann man erst ein Zertifikat erzeugen und dann auf **»vorübergehend ungültig setzen«**. Dadurch kann das Zertifikat vor dem Zeitpunkt, an dem es freigegeben wird, nicht benutzt werden. Dazu muss bei **»Erstellung des Zertifikats«** über das Auswahlmenü **»als ungültig erzeugen«** selektiert werden. Der **»Status«** ist dann **»vorübergehend ungültig setzen«**. Um das Zertifikat zu einem späteren Zeitpunkt gültig zu setzen, wird bei **»Erstellung des Zertifikats« »wieder gültig setzen«** ausgewählt.

7.6 Mit CSRs arbeiten

Eine Zertifikatssignierungsanforderung (CSR - Certificate Signing Request) ist ein digitaler Antrag, der Informationen beinhaltet, welche die CA zum Erstellen eines Zertifikats verwendet. Dies beinhaltet z.B.

- Informationen über den Antragsteller (CN, O, OU, L, S und C),
- die E-Mail-Adresse,
- der öffentliche Schlüssel, der nach CA-Authentisierung in das Zertifikat eingefügt wird,
- den Schlüsselalgorithmus,
- die Schlüssellänge.

Zu einem CSR gehört auch immer ein Schlüsselpaar. Zur Absicherung gegen Manipulation wird der CSR vom privaten Schlüssel unterschrieben. Der CSR enthält den öffentlichen Schlüssel, der später in das Zertifikat eingefügt wird. Mittels dessen kann die Gültigkeit des CSR geprüft werden.

7.6.1 CSR zum Signieren durch eine externe CA erzeugen

Ein CSR wird benötigt, um ein Zertifikat bei einer Zertifizierungsstelle zu beantragen. Wird über das Feld **»Erstellung des Zertifikats« »Nur CSR erzeugen«** ausgewählt, wird, sobald man auf **»Übernehmen«** klickt, ein Schlüsselpaar und ein CSR erzeugt.

Ist eingestellt, dass der Schlüssel verschlüsselt abgespeichert werden soll, so muss man beim Erzeugen ein Kennwort für den privaten Schlüssel eingeben. Nach erfolgreicher Ausführung zeigt das Feld **»Status« »CSR erzeugt«** an. Der CSR kann nun mittels des Links im unteren Teil des Formulars heruntergeladen und durch die externe CA signiert werden → *Siehe „7.3 | Dateien hoch- und herunterladen" auf Seite 84*. Das Zertifikat, welches nach dem Signieren durch die externe CA entstanden ist, sollte dann mittels des Upload-Links bei **»Zertifikat«** wieder hochgeladen werden. Damit steht ein von einer externen CA signiertes Zertifikat zur Verfügung.

7.6.2 SUB-CA einer externen CA erzeugen

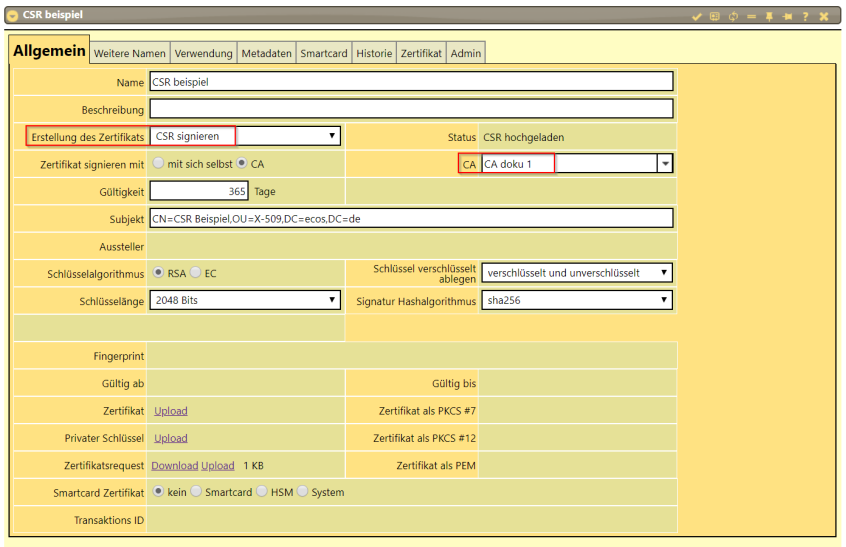
Möchte man eine Sub-CA einer externen CA erstellen und diese dann innerhalb der Appliance für das Ausstellen von Zertifikaten nutzen, ist grundsätzlich genauso vorzugehen wie im letzten Abschnitt beschrieben. Es wird im CA-Objekt ein CSR erzeugt, dieser heruntergeladen und durch die externe Parent-CA signiert. Das neue SUB-CA Zertifikat, kann anschließend hochgeladen werden. Mit dieser SUB-CA können neue Zertifikate auf der Appliance ausgestellt werden.

7.6.3 Zertifikat mittels Signieren eines externen CSR erzeugen

Soll der private Schlüssel nicht auf der Appliance, sondern auf dem System, auf dem das Zertifikat eingesetzt werden soll, erzeugt werden, so muss dieses System einen CSR erzeugen.

Auf der Appliance muss zuerst ein Zertifikat-Objekt (CA-Zertifikat oder X.509 Zertifikat, je nachdem ob ein neues Zertifikat oder eine Sub-CA erstellt werden soll) angelegt werden. Dann wird der Zertifikatsantrag bei **»Zertifikatsrequest»** mit einem Klick auf den Link **»Upload»** hochgeladen. Sollte der CSR mit einem Kennwort versehen sein, so ist dieses beim Upload einzugeben.

Um aus dem CSR das Zertifikat zu erstellen, muss eine CA zugewiesen werden und bei **»Erstellung des Zertifikats« »CSR Signieren«** eingestellt werden.



Nach Klick auf **»Übernehmen«** wird, falls die Eingabe erforderlich ist, nach dem CA-Kennwort gefragt. Ist der Vorgang erfolgreich, wird im Feld **»Status« »Zertifikat erzeugt«** angezeigt und das Zertifikat steht in den verschiedenen Formaten zum Download bereit.

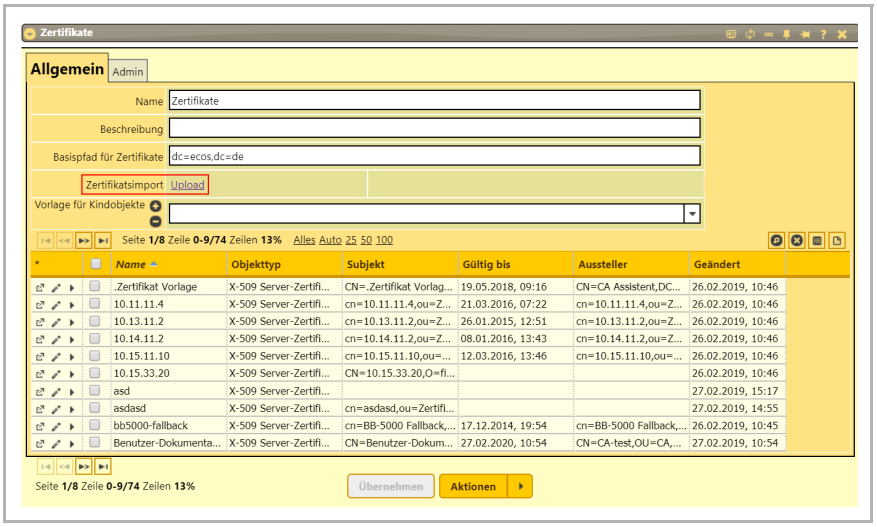
.→ *Siehe „7.3 | Dateien hoch- und herunterladen" auf Seite 84*.

7.7 Import von Zertifikaten

Die Appliance kann auch Zertifikate verwalten, die von einer anderen CA/PKI erstellt wurden. Dazu müssen die Zertifikate importiert werden. Dies ist auf zwei Arten möglich: per allgemeinem Upload oder per direktem Upload im Zertifikatsobjekt.

7.7.1 Allgemeiner Upload

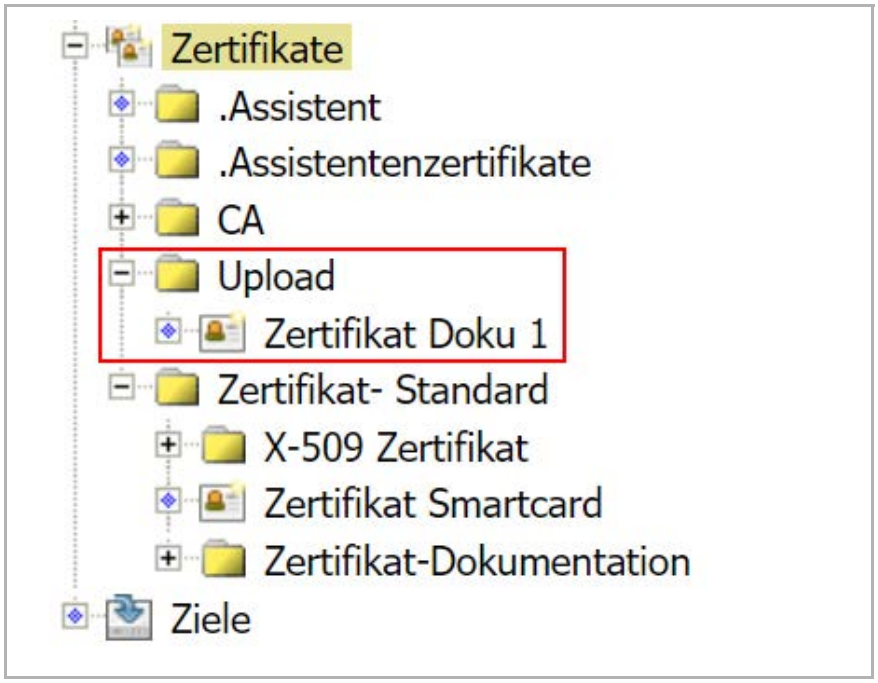
Im Zertifikate-Container können Zertifikate über den **»Upload«** Link im Feld **»Zertifikatsimport«** hochgeladen werden. Dabei werden sowohl binär wie auch base64 codierte Zertifikate akzeptiert, genauso wie PKCS#7 oder PKCS#12 Dateien. Es können weiterhin mehrere Zertifikate gleichzeitig ausgewählt und hochgeladen werden.



Das oder die hochgeladenen Zertifikate werden im Container **»Upload«** unterhalb des Zertifikate-Containers gespeichert. Falls der Container noch nicht existiert, so wird er automatisch angelegt. Falls in einer PKCS#7 oder PKCS#12 Datei mehrere Zertifikate enthalten sind, werden alle Zertifikate im Upload-Container angelegt. CA-Zertifikate, die schon vorhanden sind, egal in welchen Container, werden nicht noch einmal importiert, da ein CA-Zertifikat nur einmal auf der Appliance existieren darf.

Für jedes importierte Zertifikat wird ein neues Zertifikats- oder CA-Objekt angelegt, das jeweils den Common Name (CN) aus dem Subjekt des Zertifikats erhält.

Enthalten die hochgeladenen Dateien private Schlüssel, die durch ein Kennwort geschützt sind, wird dieses beim Upload abgefragt.



7.7.2 Direkter Upload im Zertifikatsobjekt

Im Zertifikatsobjekt besteht die Möglichkeit über den Upload-Link Zertifikate und zugehörige Schlüssel in verschiedenen Dateiformaten hochzuladen.

7.7.2.1 Zertifikat Upload

Ein Zertifikat, das als Datei vorliegt, kann in ein bestehendes Zertifikatsobjekt hochgeladen werden. Dabei werden sowohl binär wie auch base64 codierte Zertifikate akzeptiert, genauso wie PKCS#7 oder PKCS#12 Dateien. Enthält die Datei einen privaten Schlüssel, so wird dieser ebenfalls hochgeladen. Da PKCS#7 und PKCS#12 Dateien sowohl Zertifikate wie auch CA-Zertifikate enthalten können, wird das jeweilige Zertifikat hochgeladen, das zum Objekt passt. Nach dem Hochladen werden alle Felder des Zertifikatsobjektes mit den Werten aus dem Zertifikat gefüllt. Der **»Status«** ändert sich nach dem Hochladen zu **»Zertifikat hochgeladen«**.

7.7.2.2 Privater Schlüssel Upload

Sind Zertifikat und privater Schlüssel in zwei Dateien abgespeichert, so kann der

zum Zertifikat zugehörige private Schlüssel über den Upload-Link des Feldes **»Privater Schlüssel«** hochgeladen werden.

7.8 Externe Speicher für Zertifikate und Schlüssel

7.8.1 Zertifikat auf Smartcard ausrollen

Soll ein Zertifikat auf einer Smartcard ausgerollt werden, muss bei **» Smartcard-Zertifikat« »Smartcard«** aktiviert werden. Dies ermöglicht anschließend das Zertifikat auf einer Smartcard auszurollen.

Hierzu wird bei **»Erstellung des Zertifikats«** über das Auswahlmenü **»automatisch erstellen«** ausgewählt. Im Anschluss kann über den Link bei **»Enrollment«** der Ausrollvorgang gestartet werden.

→ *Siehe „9.2.4.5 | Zertifikate auf Smartcard schreiben" auf Seite 114*.

7.8.1.1 Das Schreiben des Zertifikats wiederholen

Ist eine Smartcard defekt oder verloren gegangen, kann das entsprechende Zertifikat auf eine neue Smartcard geschrieben werden. Hierzu wird bei **»Erstellung des Zertifikats«** über das Auswahlmenü **»reenroll«** selektiert, danach kann der Enrollment-Prozess des Zertifikats erneut erfolgen.

7.8.1.2 Ausrollstatus zurücksetzen

Wird bei der Erzeugung eines Zertifikats für eine Smartcard ein Vorgang nicht richtig abgeschlossen, kann der Enrollment-Status zurückgesetzt werden, so dass der Ausrollvorgang neu gestartet werden kann. Dazu wird im Zertifikatsformular bei **»Erstellung des Zertifikats« »Status löschen«** ausgewählt. Das Zertifikat-Formular wird auf den Ursprungswert zurückgesetzt.

7.8.2 Zertifikat auf Windows ausrollen

Im Zertifikatsformular kann über das Feld **»Smartcard Zertifikat«** auch festgelegt werden, dass das Zertifikat in den Windowszertifikatsstore ausgerollt werden soll. Dazu muss **»System«** ausgewählt werden. Das Vorgehen ist dasselbe wie beim Ausrollen auf eine Smartcard.

→ *Siehe „7.8.1 | Zertifikat auf Smartcard ausrollen" auf Seite 96*.

7.8.3 Privaten Schlüssel im HSM speichern

Wird im Feld **»Smartcard Zertifikat«** **»HSM«** (Hardware Security Modul) ausgewählt, wird der private Schlüssel für das Zertifikat auf dem HSM erzeugt und gespeichert.

7.9 Historie

Im Zertifikat-Formular kann über die Registerkarte **»Historie«** die Geschichte des Zertifikats nachverfolgt werden. Alle Veränderungen werden hier erfasst: wann das Zertifikat erstellt, geändert und gegebenenfalls zurückgezogen wurde. Außerdem sind noch weitere Informationen erfasst wie der **»Fingerprint«**, die **»Gültigkeit«**, das **»Subjekt«**, der **»Aussteller«** und die **»Seriennummer«**.

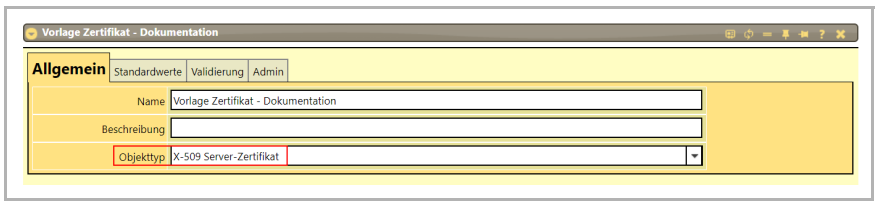
8 Vorlagen

Vorlagen sind ein Werkzeug, das die Erstellung von Objekten im Allgemeinen und Zertifikaten im Besonderen vereinfacht, indem Einstellungen (wie z.B. Gültigkeitsdauer bei Zertifikaten) vorgegeben werden können, ohne dass sie jedes Mal explizit eingestellt werden müssen. Ebenso können Validierungsregeln festgelegt werden, die sicherstellen, dass die betroffenen Objekte nur gemäß den Vorgaben erstellt und/oder geändert werden können.

8.1 Vorlage erstellen

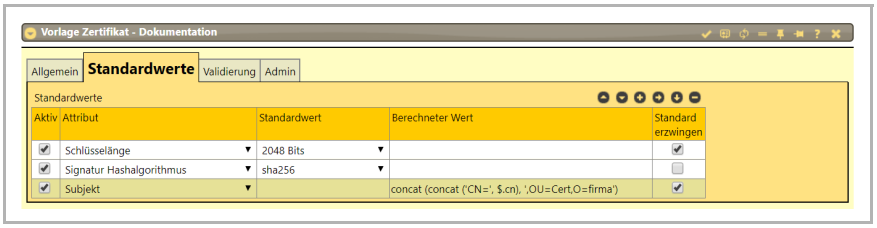
Über **»ECOS> Management> Vorlage«** werden Vorlagen erstellt und im Management Container angelegt.

Im Feld **»Objekttyp«** wird der Objekttyp ausgewählt, auf den die Vorlage angewandt werden soll (z.B bei Zertifikaten **»CA-Zertifikat«** oder **»X.509 Zertifikat«**).



8.1.1 Standardwerte

In der Tabelle auf dem Reiter **»Standardwerte«** kann für jedes Attribut des eingestellten Objekttyps ein Wert definiert werden, der als Vorgabe bei neuen Objekten dieses Typs gesetzt wird. Es kann entweder in der Spalte **»Default«** der gewünschte Werte für das ausgewählte Attribut eingestellt werden oder bei **»Berechneter Wert«** eine DocExpressions angeben werden, die den Wert berechnet. Wird bei **»Standard erzwingen«** ein Haken gesetzt, kann der Wert nicht durch den Benutzer oder die API geändert werden. Ist der Haken nicht gesetzt, so ist der Wert nur eine Vorgabe beim Neuanlegen von Objekten, kann aber vor dem Speichern geändert werden.



8.1.2 Validierung

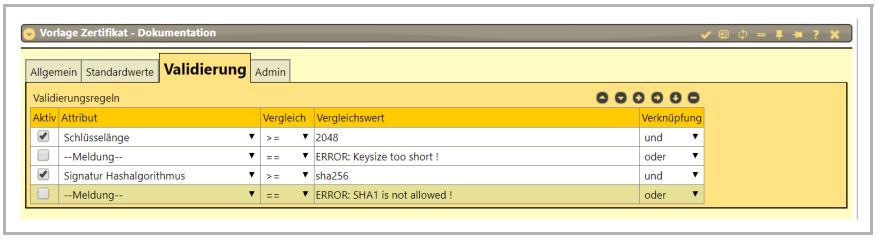
Auf dem Reiter **»Validierung«** kann geprüft werden, ob die Werte, die im Formular des Objektes beim Neuanlegen oder Ändern eingegeben wurden, bestimmten Regeln entsprechen.

In der Tabelle **»Validierungsregeln«** werden die gewünschten **»Attribute«**, ein **»Vergleich«**, sowie ein **»Vergleichswert«** ausgewählt/eingegeben → *Siehe „13.6.2.2 | Erstellen von Vergleichen der Attribute" auf Seite 174*. Wird bei **»Vergleich«** über das Auswahlmenü **»expr«** selektiert, kann, statt einem normalen Vergleich, eine DocExpressions verwendet werden, die dann in der Spalte **»Vergleichswert«** angegeben werden muss. Dadurch lassen sich auch komplexe Validierungen, die sich z.B. auf andere Objekte beziehen, realisieren.

Die einzelnen Vergleiche können mit **»und«** oder **»oder«** verknüpft werden.

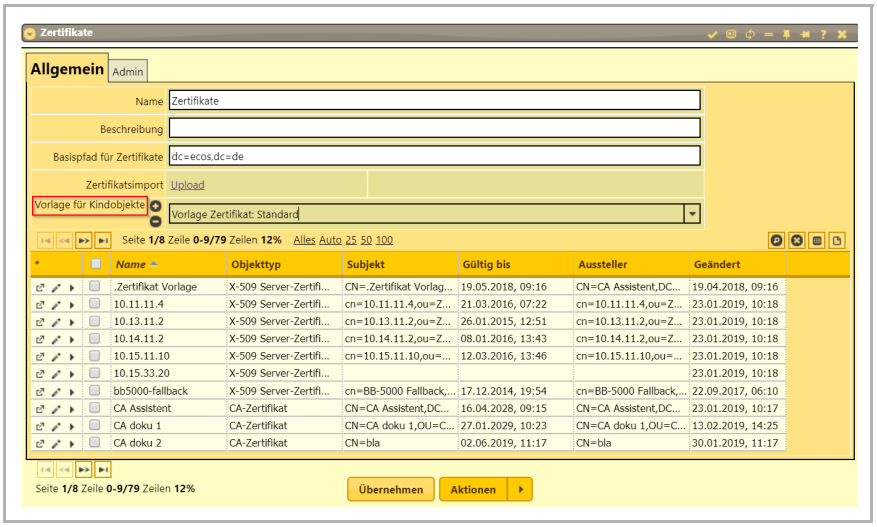
Wird bei **»Attribut« »Meldung«** selektiert, muss bei **»Vergleichswert«** ein Text, der im Fehlerfall erscheinen soll, eingetragen werden. Die Fehlermeldung erscheint immer dann, wenn ein vor dem Text stehender Vergleich fehlschlägt. So können mehrere Gruppen von Vergleichen und zugehörige Fehlermeldungen realisiert werden.

Schlägt eine der in der Tabelle angegebenen Regeln fehl, so erscheint die entsprechende Meldung und das Objekt kann nicht angelegt oder geändert werden.



8.2 Vorlagen anwenden

Damit eine Vorlage angewendet wird, muss sie einem Container zugewiesen werden. Über das Feld **»Vorlage für Kindobjekte«** in Containerobjekten können eine oder mehrere Vorlagen ausgewählt werden, welchen dann auf alle untergeordneten Objekte passenden Typs angewandt werden.



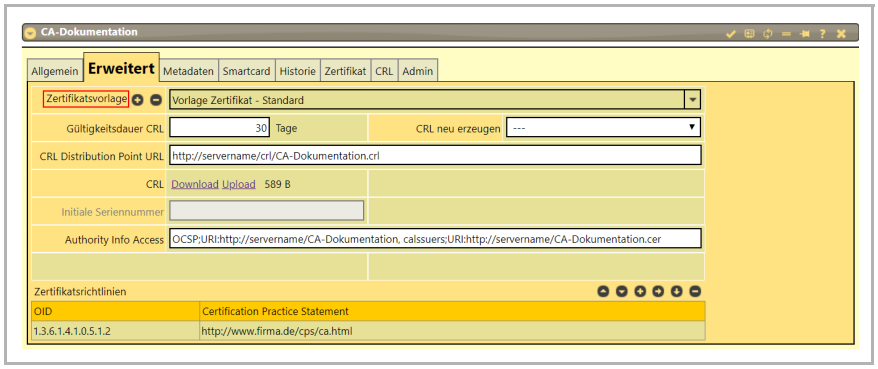
8.3 Vorlagevererbung

Unterhalb eines Containers können weitere untergeordnete Container angelegt werden, denen andere Vorlagen zugewiesen sind. Wird in diesem untergeordneten Container ein neues Objekt angelegt oder eines geändert, dann werden die Validierungsregeln aller übergeordneten Container geprüft. Schlägt eine der Regeln fehl, so erscheint die entsprechende Meldung und das Objekt kann nicht angelegt oder geändert werden.

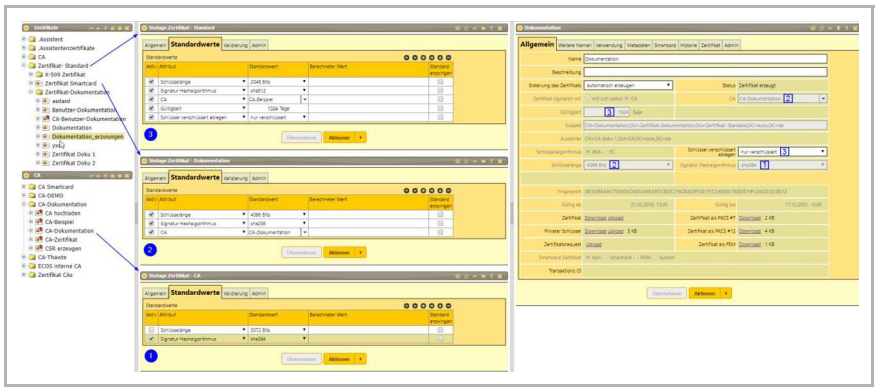
Auch die Vorgabewerte aller übergeordneten Container werden beim Anlegen bzw. Ändern eines Objektes zur Anwendung gebracht. Widersprechen sich zwei oder mehrere Vorgabewerte (dies kann vorkommen, wenn in einem der übergeordnetem Container das selbe Attribut mit unterschiedlichen Werten definiert wird), so wird der Wert zur Anwendung gebracht, dessen Vorlage in dem Container angegeben ist, der sich am nächsten in der Hierarchie zum Zielobjekt befindet. Wird jedoch ein Wert erzwungen, so hat dieser Vorrang vor einem Wert, der nicht erzwungen wurde, auch wenn letzterer näher in der Hierarchie an dem Objekt ist, auf das die Vorlage an-gewendet wird.

8.3.1 Vorlagevererbung bei Zertifikaten

Neben den oben beschriebenen Regeln für die Anwendung von Vorlagen ist es für Zertifikate zusätzlich möglich, eine Vorlage in der CA auszuwählen. Diese findet dann auf alle Zertifikate Anwendung, die diese CA nutzen.



Wird eine CA zum Erzeugen von Zertifikaten verwendet, in der eine Vorlage konfiguriert ist, werden deren Werte, genau wie bei anderen Vorlagen, die im Container konfiguriert wurden, behandelt. Widersprechen sich die Vorgabewerte, dann haben die Werte der Vorlage, die in der CA konfiguriert sind, Vorrang.



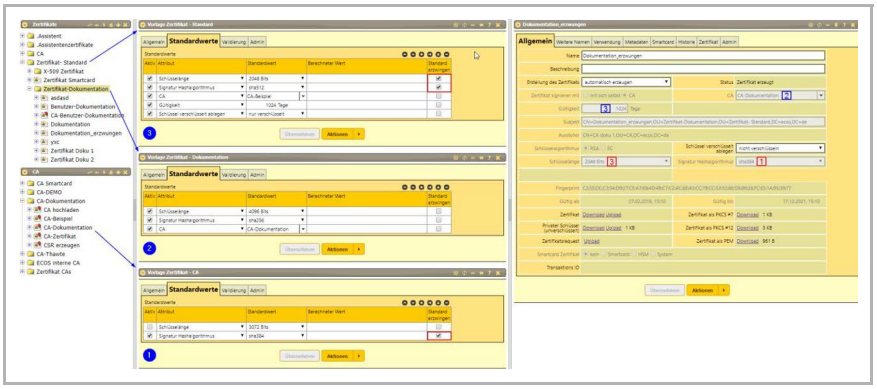
Die runden blauen Zahlen stellen die Reihenfolge dar, in der Vorgabewerte aus mehreren Vorlagen angewendet werden.

Die eckigen blauen Zahlen stellen die entsprechenden übernommenen Werte im Zertifikat dar.

Über die Vorlage besteht, wie oben beschrieben, die Möglichkeit Vorgabewerte zu erzwingen. Wird ein Vorgabewert in einem übergeordneten Container erzwungen,

dann werden die Werte aller nachfolgenden Vorlagen überschrieben, auch die aus der CA.

Die CA hat immer die höchste Priorität, außer wenn Werte von anderen Vorlagen erzwungen werden.



Die runden blauen Zahlen stellen die Reihenfolge dar, in der die Vorgabewerte angewandt werden. Die eckigen blauen Zahlen stellen die entsprechenden übernommenen Werte im Zertifikat dar.

Die Zahlen in den roten Kästchen stellen die Vorgabewerte dar, die erzwungen wurden.

9 ECOS Secure Boot Stick: Konfiguration und Enrollment

9.1 Lokale Konfiguration vs. zentrales Management

Die Konfiguration des ECOS Secure Boot Stick kann sowohl lokal auf dem Bootstick selbst als auch zentral über das Management verwaltet werden. Ein zentrales Management hat dabei den Vorteil, dass Konfigurationsänderungen nicht auf jedem Bootstick einzeln durchgeführt werden müssen, sondern einmalig im zentralen Management ausgeführt werden können und von dort auf alle betroffenen Bootsticks automatisch übertragen werden. Außerdem können zur einfacheren Verwaltung einer großen Anzahl von Bootstick-Vorlagen zentral angelegt werden, von denen die einzelnen Bootsticks ihre Konfiguration erben können. Ebenso ist das automatische Anlegen von Bootstickkonfigurationen aus anderen Verzeichnisdiensten mittels Verzeichnissynchronisation möglich.

Beim Einsatz von mehreren ECOS Secure Boot Sticks wird die Verwendung eines zentralen Managements dringend empfohlen.

9.2 Konfiguration des ECOS Secure Boot Stick

Der ECOS Secure Boot Stick ist im Auslieferungszustand nicht konfiguriert und muss erst für den jeweiligen Anwendungsfall konfiguriert bzw. personalisiert werden. Dafür wird auf dem Management eine Konfiguration für den Bootstick angelegt und dann mittels Easy Enrollment auf den Stick übertragen.

9.2.1 Notwendige Dienste auf der ECOS System Management Appliance (SMA)

Die ECOS System Management Appliance benötigt die folgenden Dienste für die Verwaltung von ECOS Secure Boot Stick (SBS):

- Der Radius-Dienst ist notwendig zur Überprüfung der Aktivierungscodes (gilt nicht bei Einsatz von SBS mit Smartcard)
- Der Software Update Server wird für das Easy Enrollment benötigt und versorgt die Bootsticks mit Software Updates.

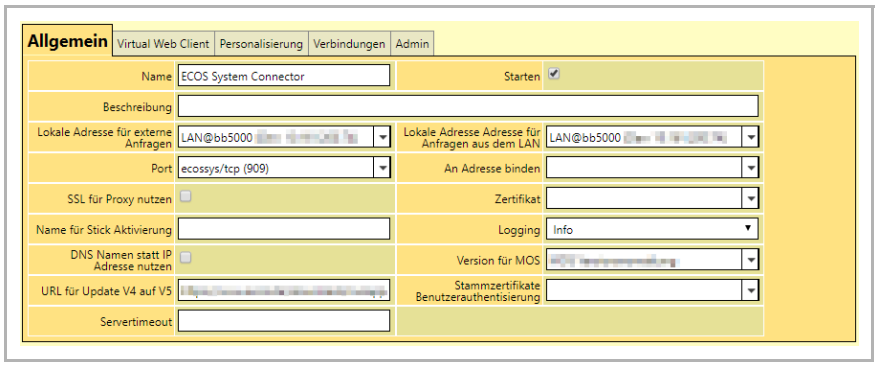
→ *Siehe „13.2 | Updates" auf Seite 164*.

Die Dienste müssen lediglich unter der ECOS System Management Appliance angelegt und durch Setzen des Häkchens bei **» Starten «** gestartet sein.

- Außerdem wird der ECOS System Connector benötigt. Dieser ist das elementare Bindeglied zwischen Appliance und Bootsticks sowohl beim Rollout als auch bei späteren Konfigurationsänderungen. Zu ihm verbinden sich die Bootsticks und über ihn werden Anfragen von den Sticks an die Appliance weitergeleitet.

9.2.2 ECOS System Connector für SBS einrichten

Der ECOS System Connector wird unter der ECOS Appliance im Container **» VPN «** angelegt. Damit er aktiv ist, muss das Häkchen bei **» Starten «** gesetzt sein.



Der ECOS System Connector benötigt eine im LAN/WAN erreichbare Netzwerkadresse, die im Feld **» Lokale Adresse für externe Anfragen «** angegeben wird. Über diese Adresse richten die angegliederten Bootsticks ihre Anfragen an die Appliance. Außerdem wird die Adresse zur Erstellung und Verifizierung der Aktivierungscodes der Bootsticks bzw. der Aktivierungsinformation auf der Smartcard benötigt.

Optional kann zusätzlich zu der **» Lokalen Adresse für externe Anfragen «** eine **» Lokale Adresse für Anfragen aus dem LAN «** angegeben werden. Sind beide Adressen gesetzt, schickt der Bootstick bei Verbindungsaufbau eine Anfrage an beide Adressen und verbindet sich mit derjenigen, die zuerst antwortet.

Im Feld **» Port «** kann der gewünschte Port, über den die Bootsticks den ECOS System Connector ansprechen, konfiguriert werden. Wird kein Port angegeben, wird der Standard-Port 909 verwendet.

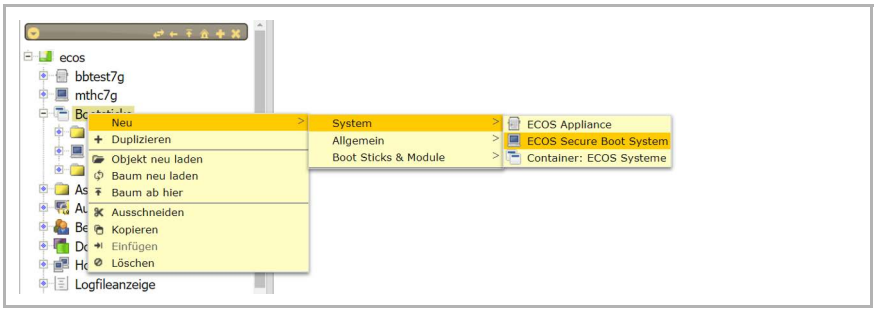
Für ein späteres Easy Enrollment im Personalisierungsprozess des Bootsticks muss entweder ein Aktivierungscode eingegeben oder eine Smartcard benutzt werden.

Im Aktivierungscode ist die Adresse des ECOS System Connector codiert. Bei Benutzung einer Smartcard wird die Adresse auf der Smartcard gespeichert. Dabei handelt es sich um die Adresse, die im Feld **» Lokale Adresse für externe Anfragen «** des ECOS System Connector angegeben werden muss. Die Adresse wird vom Bootstick genutzt, um sich während des Easy Enrollment mit dem ECOS System Connector zu verbinden. Wird das Feld **» Lokale Adresse für externe Anfragen «** im ECOS System Connector leer gelassen, wird die Adresse im Feld **» Lokale Adresse für Anfragen aus dem LAN «** zur Erstellung des Aktivierungscodes/ der Smartcard verwendet.

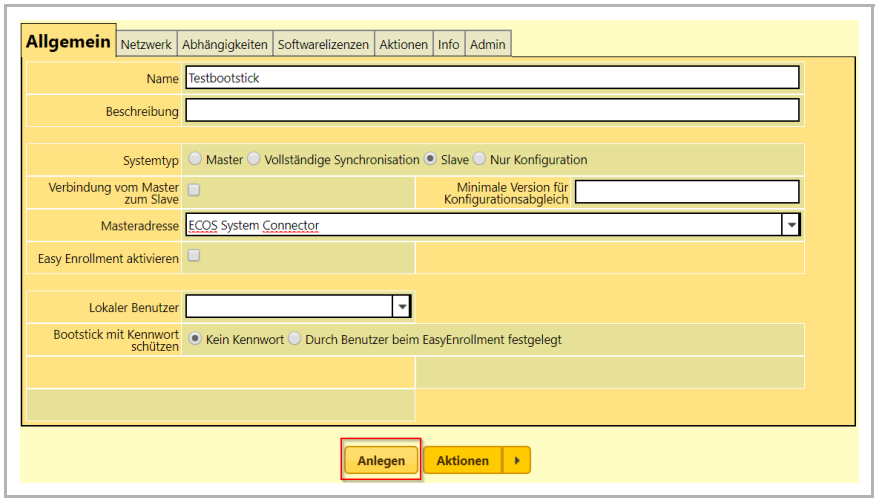
Für ein erfolgreiches Easy Enrollment muss die im Aktivierungscode / in der Smartcard hinterlegte Adresse für den Bootstick erreichbar sein. Wird die ECOS System Management Appliance zum Beispiel von einer Firewall geschützt, die Network Address Translation (NAT) zur Management Appliance macht, muss die externe Adresse der Firewall angegeben werden. Wird die Adresse im ECOS System Connector geändert, müssen gegebenenfalls bereits existierende Easy Enrollment Codes bzw. Smartcards für das Enrollment neu erzeugt werden.

9.2.3 SBS Objekte anlegen/konfigurieren

Um einen neuen ECOS BOOT STICK anzulegen, wählt man ein Konfigurationsobjekt vom Typ **» ECOS Secure Boot System «** durch Rechtsklick auf den Container **» Bootsticks «** in der linken Navigationsleiste unter **» Neu «**.

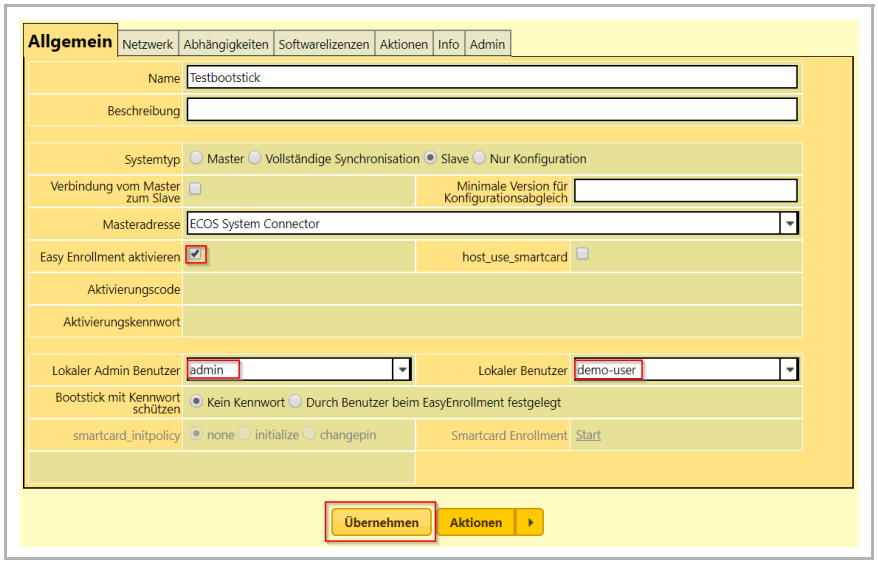


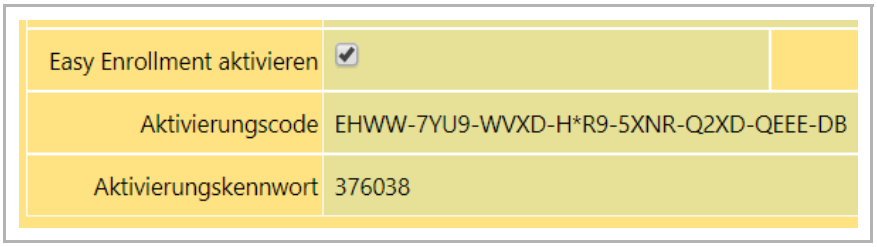
Im Reiter **» Allgemein «** muss der Name des neuen Bootsticks festgelegt werden. Im Feld **» Systemtyp «** muss nun die Option **» Slave «** ausgewählt werden. Ein Untermenü erscheint. Im Feld **» Masteradresse «** wird die Verbindung zur ECOS System Management Appliance konfiguriert. Hier sollte der zuvor konfigurierte ECOS System Connector angegeben werden. Alle notwendigen Parameter, die zum Verbindungsaufbau zur Appliance benötigt werden, wie z. B. IP-Adresse und Port, werden dann aus dem ECOS System Connector bezogen. Alternativ kann aber auch direkt die IP-Adresse des Masters angegeben werden. In diesem Fall ist der Port fest auf 909 eingestellt.



Für das Easy Enrollment mit Aktivierungscode (nicht für SBS mit Smartcard) muss die Option **» Easy Enrollment aktivieren «** durch Setzen des Häkchens aktiviert sein. Nach Klicken auf die **» Übernehmen «**-Schaltfläche wird automatisch ein Aktivierungscode und -kennwort generiert. Weitere Informationen zum Easy Enrollment → *Siehe „9.3.1 | Easy Enrollment mit Aktivierungscode" auf Seite 116*.

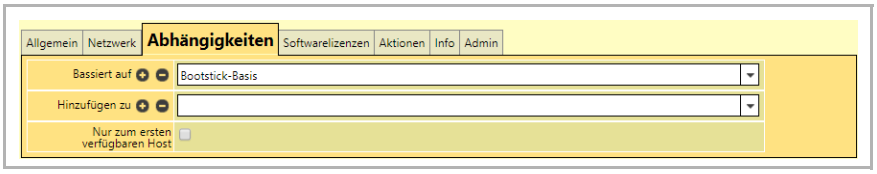
Außerdem sind die Felder **» Lokaler Admin-Benutzer «** und **» Lokaler Benutzer «** zu füllen, die im folgenden Abschnitt beschrieben werden.





Mit der Option **» Bootstick mit Kennwort schützen «** wird festgelegt, ob bei jedem Starten des Bootsticks, eine Kennwort-Authentifizierung notwendig ist. Wird die Option **» Durch Benutzer beim Easy Enrollment festgelegt «** ausgewählt, wird der Benutzer während der Aktivierung des Bootsticks dazu aufgefordert, ein Kennwort zu vergeben.

Über den Reiter **» Abhängigkeiten «** lässt sich die Konfiguration von Bootstick-Objekten vererben. Dies bedeutet, dass alle Einstellungen einer Basis-Konfiguration automatisch auf das Bootstick-Objekt angewendet werden. Für nähere Informationen zum Thema **» Vererbung von Bootstick-Konfigurationen «**. → *Siehe „9.6 | Vererbung" auf Seite 127*.



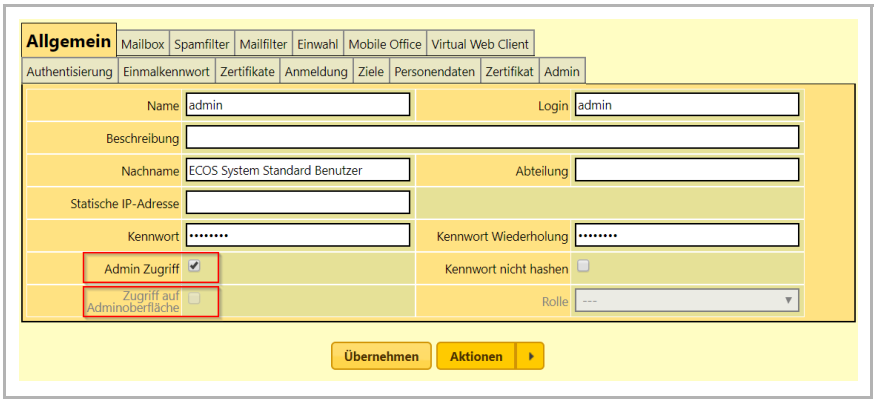
9.2.3.1 Lokaler Admin und Lokaler Benutzer

Im Bootstick-Objekt im Reiter **» Allgemein «** müssen ein lokaler Admin-Benutzer sowie ein lokaler Benutzer dem Bootstick zugeordnet werden. Diese erfüllen unterschiedliche Funktionen. Der lokale Admin-Benutzer kann über die Weboberfläche des Bootsticks Konfigurationsänderungen unabhängig von der ECOS System Management Appliance lokal durchführen. Dies ist zu Wartungszwecken möglich, wenn keine Verbindung zur Appliance hergestellt werden kann. → *Siehe „9.7 | Info zur Management-Verbindung" auf Seite 129*.

Es ist aber nicht sinnvoll den administrativen Benutzer der Appliance zu verwenden, sondern es sollte einen eigenen Benutzer angelegt werden → *Siehe „6 | Benutzer" auf Seite 74*. Dieser kann dann nur auf der Administration des Bootsticks zugreifen.

Als lokaler Admin-Benutzer können nur Benutzer benannt werden, die entweder über die Berechtigung **» Admin Zugriff «** oder **» Zugriff auf die Adminoberfläche «**

verfügen. Diese können durch Setzen der entsprechenden Häkchen im Reiter **» Allgemein «** des Benutzer-Objekts verliehen werden. Zusätzlich muss ein Kennwort zur Authentifizierung an der Administrationsoberfläche vergeben werden.



Der lokale Benutzer muss im Gegensatz zum lokalen Admin-Benutzer nicht über Admin-Rechte und ein Kennwort zur Authentifizierung an der Administrationsoberfläche verfügen. Der lokale Benutzer ist für die Auswahl der Ziele, die über den ECOS Secure Boot Stick erreicht werden können, zuständig. Ziele sind die Systeme, auf die der eigentliche Zugriff des Benutzers erfolgen soll wie z. B. Microsoft Terminalserver oder eine Citrix Farm. → *Siehe „5 | Ziele" auf Seite 67*.

Die Definition der Ziele, auf die ein Benutzer und damit der ihm zugewiesene Bootstick Zugriff hat, erfolgt im Reiter **» Ziele «** des Benutzer-Objektes. In der Tabelle **» Ziele «** können vorhandene Zielobjekte ausgewählt werden und durch Setzen der Häkchen bei **» Secure Boot «**, **» Mobile Office «** und **» Virtual Web «** für die einzelnen Produkte freigeschaltet werden. Damit der Benutzer Zugriff auf ein Ziel im ECOS Secure Boot Stick hat, muss ein Häkchen bei **» Aktiv «** und bei **» Secure Boot «** in der Ziele-Tabelle des Benutzer-Objektes gesetzt sein.

Beim Starten des Bootsticks werden die Ziele, die für den Benutzer freigeschaltet wurden, im Auswahl-Menü angezeigt. Die Modifikation der zur Auswahl stehenden Ziele erfolgt durch Aktivieren und Deaktivieren bzw. durch Hinzufügen und Löschen von Zielen in der Ziele-Tabelle im Formular des Benutzers.

Sollen mehreren Bootsticks die gleiche Auswahl an Zielen zur Verfügung stehen, ist es möglich ihnen denselben lokalen Benutzer zuzuordnen. Der lokale Benutzer entspricht in diesem Fall einer Benutzergruppe, die über dieselben Eigenschaften verfügt.

Andersherum ist es nicht möglich einem Bootstick mehrere Benutzer zuzuweisen. Das heißt, mit einem bestimmten Bootstick ist ausschließlich der Zugriff auf die dem lokalen Benutzer freigegebenen Zielsysteme erlaubt. Möchte man die Aus-

wahl der Zielsysteme anpassen, mit denen sich der Bootstick verbinden kann, so muss entweder die Freigabe der Zielsysteme für den Benutzer im Formular des Benutzers im Reiter **» Ziele «** geändert werden oder dem Bootstick-Objekt ein anderer lokaler Benutzer im Reiter **» Allgemein «** zugeordnet werden.

9.2.3.2 Ziele

Um über einen Bootstick den Remote-Zugriff auf einen Terminalserver oder ein anderes Zielsystem zu ermöglichen, müssen Ziele angelegt werden. Ziele sind die Systeme, auf die der eigentliche Zugriff des Benutzers erfolgen soll. In den dazu gehörigen Konfigurationsobjekten werden die nötigen Informationen zum Verbindungsaufbau hinterlegt. Für nähere Informationen zu den verschiedenen Ziel-Systemen und deren Konfiguration. → *Siehe „5 | Ziele" auf Seite 67*.

9.2.4 Zusätzliche Konfiguration für SBS mit Smartcard

Für die Nutzung der SMA mit ECOS Secure Boot Stick [FX] oder [SX] mit Smartcard-Authentisierung, sind noch einige weitergehende Konfigurationen notwendig, die zusätzlich zu den unter → *Siehe „9.2.1 | Notwendige Dienste auf der ECOS System Management Appliance (SMA)" auf Seite 103* und → *Siehe „9.2.2 | ECOS System Connector für SBS einrichten" auf Seite 104* beschriebenen Einstellungen eingerichtet werden müssen.

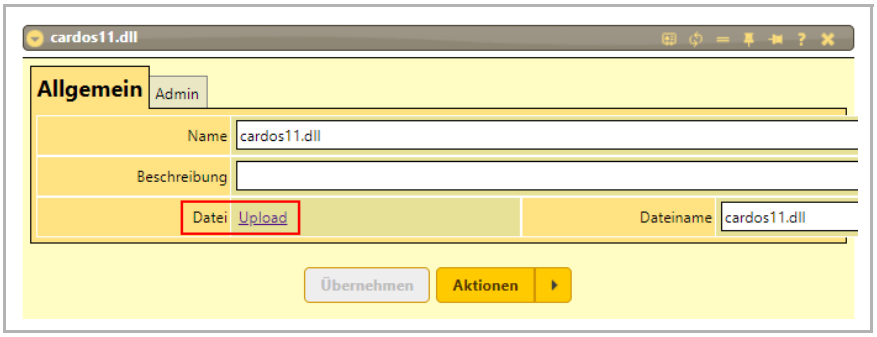
Neben dem Smartcard Enrollment Dienst, müssen noch die Zertifikate für die Kommunikation des SBS mit dem Management angelegt werden.

9.2.4.1 Smartcard-Enrollment-Dienst

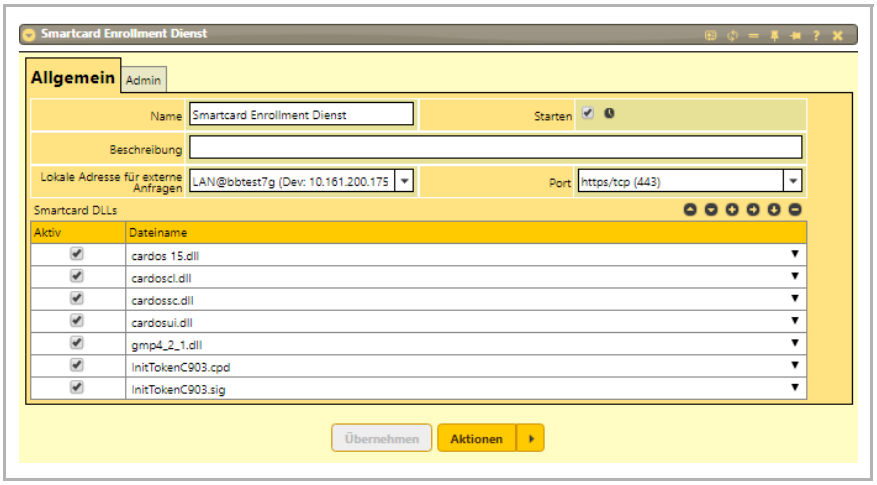
Der Smartcard-Enrollment-Dienst dient dem Ausrollen der Zertifikate auf die Smartcard. Neben dem vergeben eines Namens, muss der Dienst durch Setzen des Häkchens bei **» Starten «** gestartet werden. Außerdem benötigt er noch eine Netzwerkadresse, die im Feld **» Lokale Adresse für externe Anfragen «** angegeben wird, genauso wie einen Port. Über die Adresse und den Port kommuniziert das Smartcard-Enrollment-Tool mit dem Management, so kann es die richtigen Zertifikate auf die Smartcard schreiben. Im einfachsten Fall wird die **» Lokale Adresse «** und der Port genauso wie im System Connector konfiguriert.

Für das Schreiben der Zertifikate auf der Smartcard wird eine Middleware benötigt. Damit die Middleware nicht auf dem Zielsystem installiert werden muss, werden die notwendigen Dateien bei **» Smartcard DLL «** konfiguriert.

Die Middleware muss zuerst hochgeladen werden. Hierzu wird in der Wurzel des Baumes unterhalb des Containers **» Softwareupdates «** ein neuer Container, mit beliebigen Namen angelegt. Falls der Container **» Softwareupdates «** noch nicht existiert, kann er mittels **» Neu > Container für Softwareupdates «** angelegt werden. Unter diesem Container wird für jede Datei der Middleware eine **» Datei für Mobile Office «** angelegt.



In diese Objekte werden dann die Dateien der Middleware hochgeladen. Anschließend sind die Objekte mit den Dateien der Middleware im **» Smartcard-Enrollment-Dienst «** auszuwählen. Dieser findet sich unter dem Appliance Objekt **» Dienste > Smartcard-Enrollment-Dienst «** . Die Smartcard DLL-Dateien müssen mit einem Häkchen bei **» Aktiv «** aktiviert werden.



Beim ECOS Secure Boot Stick[SX] kommt ATOS Middleware zum Einsatz.

9.2.4.2 CA-Zertifikat(e) zur Smartcard Nutzung einrichten

Wird die Smartcard von der ECOS Appliance verwaltet, so muss ein neues CA-Zertifikat angelegt und erzeugt werden. → *Siehe „7.2.1 | CA/Parent-CA" auf Seite 78*.

Im Feld **» Schlüssellänge «** ist es, für die vom BSI zugelassene Version, erforderlich mindestens einen Wert von 3072 Bits auszuwählen. Weitere Informationen hierzu sind im Dokument „Einsatz- und Betriebsbedingungen ECOS Secure Boot Stick 6.0.x, BSI-VSA-10196" zu finden.

Wird eine bestehende Smartcard verwendet, müssen die CA-Zertifikate der auf der Smartcard verwendeten Zertifikate in der SMA konfiguriert werden, um eine Authentisierung per Smartcard Zertifikat am ECOS System zu ermöglichen. Hierzu wird unter Zertifikate mit **» Neu «** ein neuer Container, mit beliebigen Namen angelegt, in dem sämtliche zur Anwendung kommenden CA-Zertifikate konfiguriert werden.

Das Einrichten der einzelnen CA-Zertifikate lässt sich am einfachste erreichen, wenn unter Zertifikate mit **» Neu > Zertifikate & Smartcards > CA-Zertifikat «** ein neues Zertifikats-Objekt mit einem beliebigen Namen mit Ziffern-Suffix angelegt wird, wie z.B. **» CA-Zert 1 «**. Danach kann mit dem Menüpunkt **» Duplizieren «** dieses CA-Zertifikats Objekt beliebig eingefügt werden und erhält automatisch eine fortlaufende Nummerierung.

Nach dem Anlegen der CA-Zertifikat-Objekte muss für jedes CA-Zertifikat auf dem Reiter **» Allgemein «** unter **» Zertifikat «** mit **» upload «** das entsprechende Zertifikat in das angelegte CA-Zertifikats-Objekt hochgeladen werden.

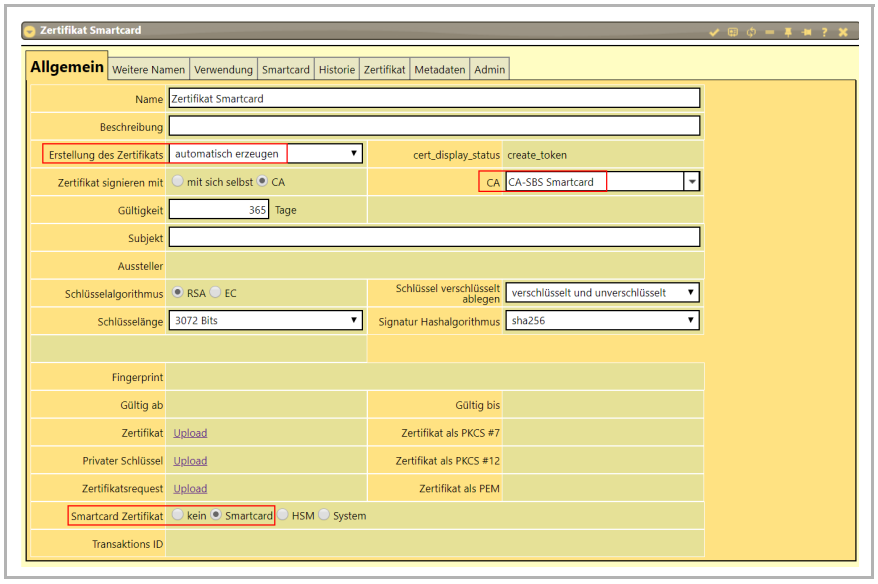
9.2.4.3 Zertifikate zur Smartcard Nutzung anlegen

Wird die Smartcard mittels des ECOS Managements zur Verfügung gestellt, so sind zunächst die notwendigen Zertifikate für den Bootstick anzulegen und diese danach auf die Smartcard auszurollen.

Hierzu müssen unter dem **» Bootstick-Objekt «** neue Zertifikate angelegt werden. → *Siehe „7 | Zertifikate" auf Seite 75*. Es ist jeweils ein Zertifikat für die Management-Verbindung, eins für die VPN Verbindung sowie für die Verschlüsselung des SBS erforderlich.

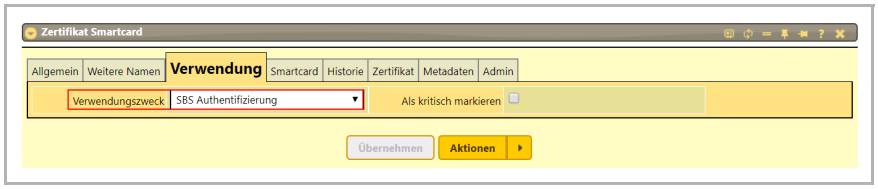
In den Zertifikats-Objekten müssen folgende Einstellungen vorgenommen werden. Das Feld **» Erstellung des Zertifikates «** muss auf automatisch gestellt und bei **» Smartcard-Zertifikat «** muss die Option **» Smartcard «** aktiviert werden. Dies ermöglicht es, anschließend die Zertifikate auf eine Smartcard auszurollen. Außerdem muss im Feld **» CA «** das vorher erstellte CA- Zertifikat ausgewählt werden.

Das Feld **» Subjekt «** muss leer gelassen werden. Es wird beim Erzeugen des Zertifikats automatisch, entsprechend der Hierarchie im Baum, gefüllt. Es muss dann sichergestellt sein, das im Feld **» Für Easy Enrollment zugelassene Zertifikatssubjekte «** im System-Connector, ein passender Ausdruck eingegeben wird, damit sich der SBS erfolgreich mittels des Zertifikats authentisieren kann



→ *Siehe „9.2.4.4 | ECOS System Connector zur Smartcard-Nutzung einrichten" auf Seite 112*.

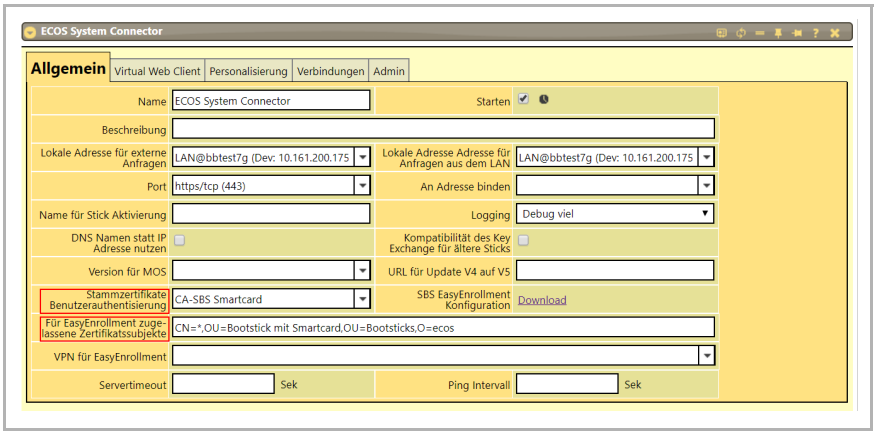
Für das Zertifikat, welches der Authentisierung der Management-Verbindung dient, ist zusätzlich im Reiter **» Verwendung «**, bei **» Verwendungszweck > SBS Authentisierung «** auszuwählen. Dadurch wird die SBS Konfiguration für das Easy Enrollment in eine Zertifikats-Extension eingebettet.



9.2.4.4 ECOS System Connector zur Smartcard-Nutzung einrichten

Für die Nutzung der SMA mit SBS und Smartcard sind noch zusätzliche Konfigurationsschritte notwendig, die zusätzlich zu den unter → *Siehe „9.2.2 | ECOS System Connector für SBS einrichten" auf Seite 104* angegebenen Schritten zu absolvieren sind.

Im Feld **» Stammzertifikate Benutzerauthentisierung «** die vorkonfigurierte CA, die für der ECOS Secure Boot Sticknzur Smartcard Nutzung angelegt worden ist, auswählen.



Außerdem müssen explizit die zur Authentisierung zugelassenen Zertifikate durch Konfiguration der Subject DN's konfiguriert werden. Hiermit lassen sich die zur Anmeldung zugelassenen Benutzer noch feingranularer als durch die verwendete CA einschränken. Dafür muss ein Filter-Ausdruck im Feld **» Für Easy Enrollment zugelassene Zertifikatssubjekte «** konfiguriert werden.

In diesem Filter müssen **alle** DN Bestandteile, die im Subjekt des zugrunde liegenden Zertifikatsenthalten sind, vorhanden sein oder können durch Platzhalter **(*)** ersetzt werden. Ein genereller Platzhalter für den gesamten DN ist nicht möglich. Mit einem logischen Oder **(|)** können mehrere Ausdrücke verknüpft werden.

Zum besseren Verständnis der Syntax des Filterausdrucks, im Folgenden einige mögliche Beispiel Konfiguration für einen Filter.

Syntax	Beispiel
C=DE,O=Firma xyz,OU=Vertrieb,CN=*	sämtliche Mitarbeiter (CN), im Vertrieb (OU), von der Firma xyz (O), aus DE (C)
C=DE,O=Firma xyz,OU=*,CN=*	sämtliche Mitarbeiter (CN), sämtliche Abteilungen (OU), von der Firma xyz (O), aus DE (C)
C=DE,O=Firma xyz,OU=Vetrieb,CN=* | C=DE,O=Firma xyz,OU=Produktion,CN=*	sämtliche Mitarbeiter (CN), im Vertrieb (OU), bei der Firma xyz (O), aus DE (C) oder sämtliche Mitarbeiter (CN), in der Produktion (OU) , von der Firma xyz (O), aus DE (C)

Tabelle 9-2 Konfiguration Filter

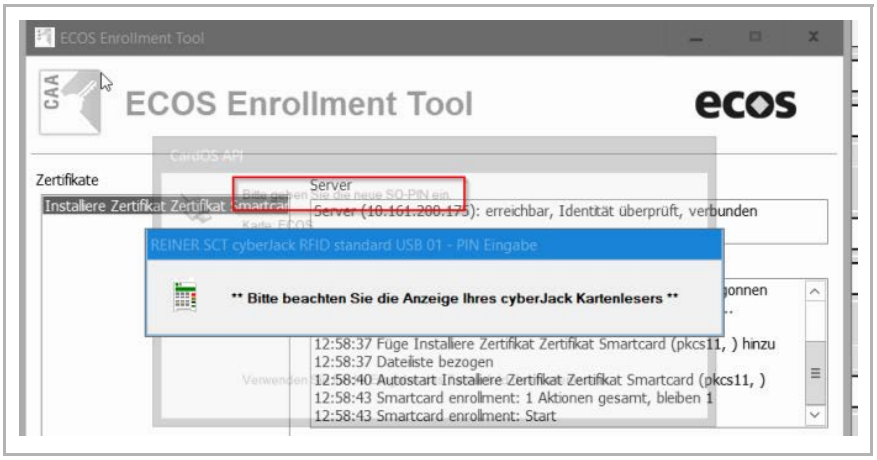
Eine korrekte Konfiguration dieses Feldes ist unerlässlich, damit die richtigen Zertifikate beim Easy Enrollment zugelassen werden.

9.2.4.5 Zertifikate auf Smartcard schreiben

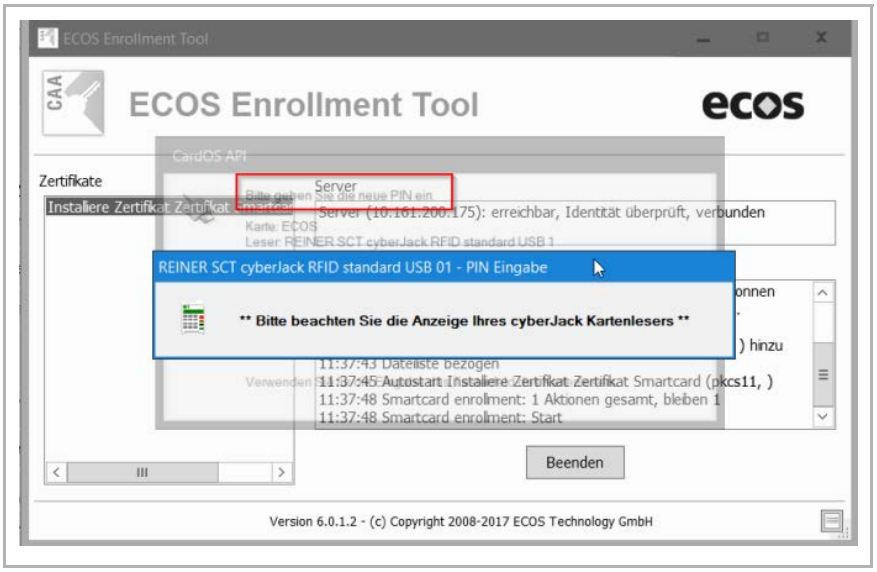
Bevor die Smartcard genutzt werden kann, müssen die zuvor angelegt Zertifikate auf die Smartcard geschrieben werden. Durch einen Klick auf **» Tool «** beim Smartcard-Enrollment im SBS-Objekt, startet das Zertifikats-Enrollment-Tool. Dies rollt die Zertifikate auf die Smartcard aus. Dazu muss die Smartcard an den Windows-PC angeschlossen sein, auf dem der Browser mit der Administrationsoberfläche aufgerufen worden ist.

Ist die Smartcard noch nicht initialisiert, geschieht dies automatisch.

Bei der Initialisierung ist die Eingabe einer neuen PUK, sowie einer neuen PIN notwendig. Je nach Smartcardreader erfolgt die Eingabe, direkt am Smartcardreader oder wird in einem Dialog am Bildschirm abgefragt. Bei Eingabe am Smartcardreader muss zunächst die PUK eingeben werden. Diese muss aus 10 Zahlen bestehen und am Kartenleser dreimal eingegeben werden.



Im Anschluss wird nach einer neuen PIN gefragt. Die PIN muss aus mindestens 4 Zahlen bestehen und muss ebenfalls dreimal eingegeben werden.



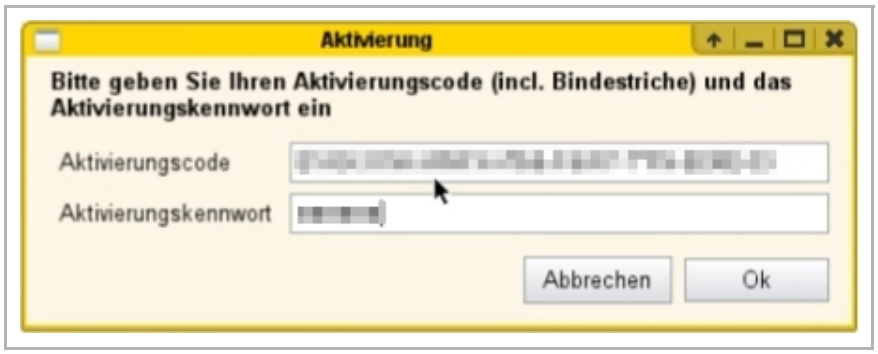
Es ist auch möglich beim Enrollment auf die Smartcard, diese vorher neu zu initialisieren, indem im Bootstick-Objekt im Feld Smardcard Init **» Formatieren «** ausgewählt wird.

9.3 SBS-Personalisierung

Die Aktivierung und Personalisierung des ECOS Secure Boot Stick erfolgt durch die Zuordnung der Konfiguration des Bootstick-Objektes mit dem physikalischen USB-Stick entweder über das Easy Enrollment oder über den Export der Konfiguration von der ECOS System Management Appliance zum Bootstick.

9.3.1 Easy Enrollment mit Aktivierungscode

Für das Easy Enrollment muss der Bootstick an einen Rechner angeschlossen und gestartet werden. Im Auslieferungszustand öffnet sich dort eine Eingabemaske, in der Aktivierungscode und Aktivierungskennwort eingegeben werden müssen.



Um den Aktivierungscode zu erzeugen, muss auf der Appliance vorab im Bootstick-Objekt der Haken für Easy Enrollment gesetzt sein.

Nachdem der Aktivierungscode auf dem Bootstick eingegeben wurde, kontaktiert der Bootstick das Management und lädt alle benötigten Konfigurationseinstellungen automatisch vom entsprechenden Masterserver herunter.

Hierfür ist im Aktivierungscode des Easy Enrollment die IP-Adresse des Managements codiert. Es handelt sich hierbei um die Adresse, die im Feld **» Lokale Adresse für externe Anfragen «** des ECOS System Connectors angegeben ist. → *Siehe „9.2 | Konfiguration des ECOS Secure Boot Stick" auf Seite 103*.

Für eine erfolgreiche Durchführung des Easy Enrollment muss der Bootstick in der Lage sein, eine Verbindung zur ECOS Management Appliance aufzubauen.

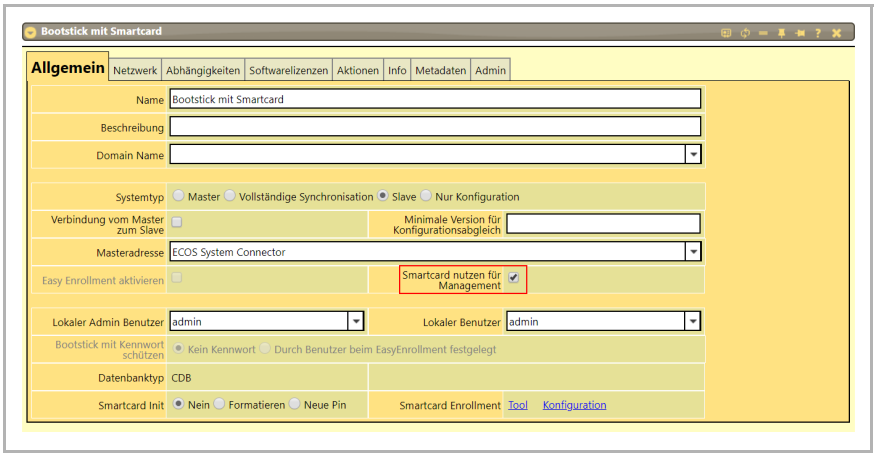
Wurde die Option **» Bootstick mit Kennwort schützen «** in der Bootstick Konfiguration aktiviert, muss der Benutzer bei der Durchführung des Easy Enrollment ein Bootkennwort vergeben. Dies wird in Zukunft bei jedem Start des Bootsticks abgefragt. Das Bootkennwort kann nachträglich im Menü des Bootsticks vom Benutzer geändert werden.

Soll das Bootkennwort zurückgesetzt werden – zum Beispiel, weil der Benutzer es vergessen hat – kann das Easy Enrollment erneut ausgeführt werden. → *Siehe „9.8.1 | Zurücksetzen des Sticks" auf Seite 129*.

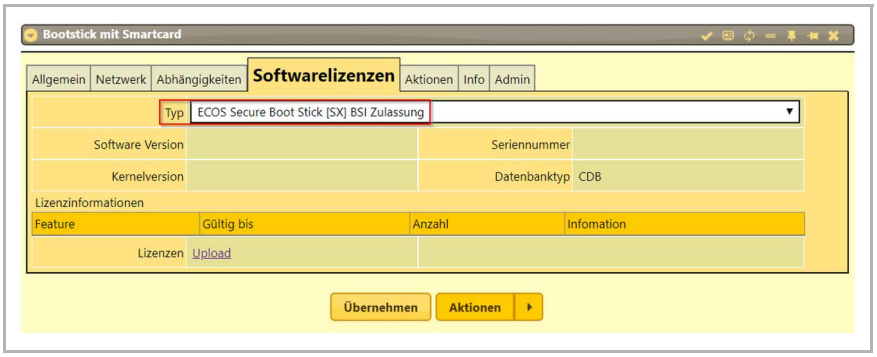
9.3.2 Easy Enrollment mit Smartcard

Um das Easy Enrollment mit Smartcard erfolgreich durchzuführen, ist es notwendig, die beschriebenen Schritte in → *Siehe „9.2.4 | Zusätzliche Konfiguration für SBS mit Smartcard" auf Seite 109*, konfiguriert zu haben.

Da die Management-Verbindung per Smartcard authentisiert wird, muss in der Registerkarte **» Allgemein «** beim Bootstick-Objekt die Option **» Smartcard nutzen für Management «** ausgewählt werden. In der BSI zugelassenen Version des SBS [SX] ist diese Konfiguration fest eingestellt.



Außerdem muss im Reiter **» Softwarelizenzen «** beim Bootstick-Objekt der passende Typ ausgewählt werden.



Werden bestehende Smartcards verwendet, so müssen die SBS vorkonfiguriert werden, um die Adresse der SMA zu erkennen. Dies kann entweder direkt bei der Auslieferung durch ECOS erfolgen oder auch nachträglich manuell. Eine entsprechende Vorkonfiguration kann im System Connector heruntergeladen und im Bootstick Konfigurationsobjekt, direkt auf dem Bootstick hochgeladen werden.

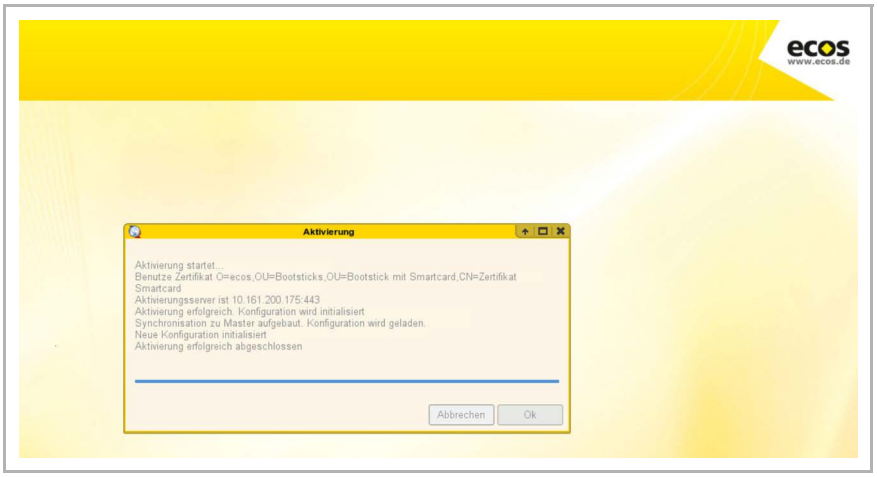
Wenn die Konfiguration komplett durchgeführt wurde, muss die Smartcard von der Karte ausgebrochen werden und in das Smartcard-Fach (am unteren Ende in die Schublade des Sticks) eingelegt werden. Danach kann der ECOS Secure Boot Stick an einen Computer angeschlossen und gebootet werden. Der Rechner muss dazu im BIOS auf USB-Boot umgestellt werden oder der ECOS Secure Boot Stick muss als temporäres Bootdevice ausgewählt werden. Sofern der Rechner im LAN eingebunden ist, wird der Stick dieses als Internet-Verbindung genutzt. WLAN oder LTE sind über das Netzwerk-Symbol unten rechts in der Taskleiste nutzbar.

Nachdem der Stick an den Rechner angeschlossen wurde, erscheint eine Meldung, die darauf hinweist, die Smartcard ins Smartcard-Fach einzulegen, falls diese Aktion noch nicht stattgefunden hat

Nach kurzer Zeit startet automatisch Easy Enrollment, welches den Stick für die erste Benutzung konfiguriert. Falls keine LAN-Verbindung besteht, sollte der Enrollment-Vorgang erneut gestartet werden, nachdem eine Verbindung zu LTE oder zum WLAN hergestellt wurde. Nach kurzer Zeit wird der Benutzer zur Eingabe des PIN-Codes der Smartcard aufgefordert. Der PIN-Code wird auf der Tastatur des Sticks eingegeben und mit der ↵-Taste bestätigt.

Bei der Aktivierung werden die Zertifikate von der Smartcard gelesen, hiermit werden die Smartcard und der Bootstick gekoppelt. Die Smartcard ist nur für den ECOS Secure Boot Stick bestimmt, mit dem sie ausgerollt wurde.

Während des Easy Enrollment verbindet sich der Bootstick mit dem Management, hiermit werden alle Konfigurationseinstellungen vom Masterserver geladen und aktiviert.



Nach abgeschlossenem Easy Enrollment sollte der Stick einmal neu gestartet werden. Sobald der Stick während des Boot-Prozesses blinkt, muss der PIN-Code der Smartcard auf der Tastatur des Sticks eingegeben werden und mit der ↵-Taste bestätigt werden.

Wenn der Stick fertig gestartet hat, kann das Zielsystem ausgewählt werden, um eine Verbindung aufzubauen.

9.3.3 Export

Statt Easy Enrollment kann man zur Aktivierung und Personalisierung eines Secure Boot Stick auch die Konfiguration manuell von der System Management Appliance auf diesen exportieren.

Bei der Nutzung einer Smartcard zur Authentisierung der Management-Verbindung ist die Aktivierung nicht mittels Export, sondern nur per Easy Enrollment möglich.

Hierfür ist es notwendig, zuvor die Firewall des SBS zu löschen. Dazu ruft man auf dem gestarteten SBS über das ECOS Symbol links unten in der Taskleiste das Startmenü auf. Hier öffnet man unter **System → Konsole** die Konsole und loggt sich mit dem Benutzernamen **» setup «** und dem unter Wartung eingestellten Kennwort ein. Wurde kein Kennwort vergeben, ist das Standardkennwort **» bb5000 «**. Anschließend öffnet sich ein Begrüßungsbildschirm. Durch Drücken einer beliebigen Taste öffnet sich ein Auswahlmenü. Die vorhandenen Firewall-Regeln werden durch Drücken der Taste **F** gelöscht.

Auf der System Management Appliance wählt man im SBS-Objekt im Reiter **» Aktion «** die Aktion **» Konfigurationsexport «**. Es öffnet sich ein Untermenü, in dem man manuell die Adresse des Zielsystems, den Port des Admin-Interfaces und den Admin-Benutzer mit Kennwort einträgt. Mit Klick auf **» Start «** wird der Konfigurationsexport gestartet.

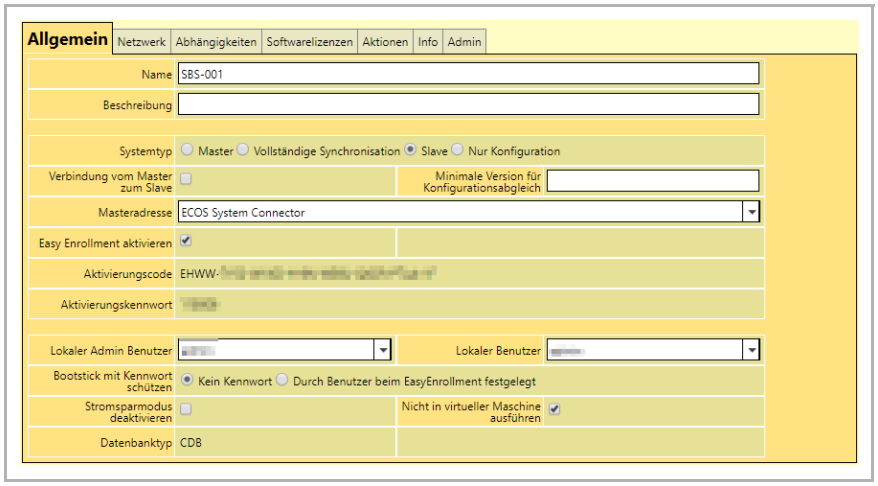
Der Konfigurationsexport ist nur dann möglich, wenn die Management Appliance den SBS per HTTPS-Verbindung erreichen kann **und** umgekehrt der SBS die SMA über den im ECOS System Connector spezifizierten Management-Port kontaktieren kann.

9.4 SBS und VPN

Um Ziele durch ein unsicheres Netz, wie z. B. das Internet zu erreichen, ist i.d.R. eine VPN-Verbindung notwendig. Dazu verfügt der SBS über integrierte IPsec- und SSL-VPN-Clients. Außerdem unterstützt der SBS Java für einen clientlosen VPN-Zugang via Browser. Dies ermöglicht den Verbindungsaufbau über VPN-Gateways aller gängigen Hersteller. Auch die System Management Appliance oder die Secure Gateway Appliance können als VPN-Gateway und Authentisierungsserver für den SBS eingesetzt werden.

Der SBS bietet zudem die Möglichkeit einer sog. Trusted Network Detection (TND). Durch TND kann der Aufbau einer VPN-Verbindung selektiv gesteuert werden. → *Siehe „9.4.3 | Trusted Network Detection (TND)" auf Seite 122*

Im Container **» VPN «**, der sich unter dem SBS-Objekt befindet, wird der gewünschte VPN-Client durch Rechtsklick auf den Container unter **» Neu «** ausgewählt und angelegt. Je nach VPN-Typ müssen im VPN-Client-Objekt unterschiedliche Einstellungen vorgenommen werden.



9.4.1 Start der VPN-Verbindung

Im VPN-Client-Objekt lässt sich einstellen, wann die VPN-Verbindung aufgebaut werden soll. Der VPN-Tunnel kann automatisch mit Starten des Bootsticks aufgebaut werden oder **» Bei Bedarf «**. In diesem Fall wird der VPN-Tunnel erst aufgebaut, wenn eine Applikation (Ziel), die diesen benötigt, gestartet wird. Das Ziel oder eine Gruppe von Zielen können im Feld **» Verbindungsaufbau durch Profil «** angegeben werden. Wird dort nichts angegeben, starten alle Ziele die VPN-Verbindung. Erfolgt dort jedoch eine Auswahl, wird die VPN-Verbindung nur beim Starten der ausgewählten Ziele aufgebaut.

9.4.2 IPsec

Internet Protocol Security (IPsec) ist eine Protokoll-Suite, die eine gesicherte Kommunikation über das Internet ermöglicht. Um die VPN-Verbindung des Bootsticks zum VPN-Gateway mithilfe von IPsec abzusichern, muss auf dem Bootstick ein IPsec-Client konfiguriert sein. Dieser muss im Container **» VPN «** unterhalb des Bootstick-Objektes angelegt werden. Zur Auswahl stehen **» IPsec Aggressive Mode-Verbindung «**, **» IPsec NCP Client «**, **» IPsec Shrewsoft-Client «** und **» IPsec Client-Verbindung «** angelegt werden.

Um Ziele oder Zielgruppen für eine VS-NfD-Klassifikation freizugeben, wird im Feld **» Allgemein: Verbindungsaufbau durch Ziel «** das jeweilige Ziel bzw. die Zielgruppe ausgewählt, die über das VS-NfD-Netzwerk aufgerufen werden sollen.

→ *Siehe „9.4.4 | Neuerungen mit SBS V8 (VS-NfD)" auf Seite 122*

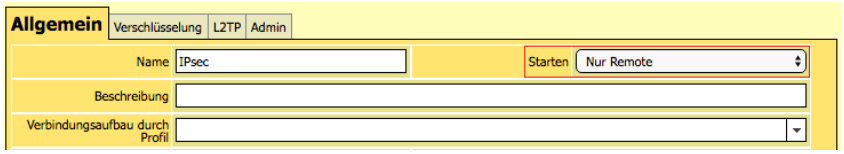
9.4.3 Trusted Network Detection (TND)

Ab Version 7 bietet der SBS eine TND-Funktion an. Befindet sich der SBS bereits in einem als sicher ("trusted") erkannten Netzwerk, werden Verbindungsziele innerhalb des sicheren Netzwerks ohne VPN-Verbindung erreicht. Für den Benutzer bleiben dabei unterschiedliche Netzwerksegmente und deren Sicherheitsstatus transparent, sodass er unabhängig vom Einsatzort mit den gleichen Verbindungszielen arbeiten kann.

Innerhalb der Netzwerkinfrastruktur entfällt die Notwendigkeit VPN-Gateways innerhalb gesicherter Netzwerke einzurichten, um eine sichere Kommunikation herzustellen, die ohnedies bereits gegeben ist.

Bei eingeschalteter TND-Funktion erkennt der SBS ein sicheres Netzwerk daran, dass eine Management-Verbindung zu einer SMA ohne vorherigen VPN-Aufbau hergestellt werden kann. Durch die gegenseitige Authentifizierung zwischen SBS und SMA (siehe 9.7) wird die TND-Funktion vor Missbrauch geschützt.

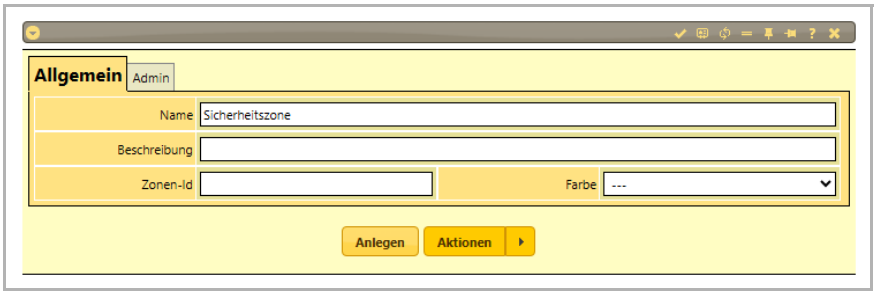
In der Standardeinstellung ist TND inaktiv und muss zunächst durch den Administrator eingeschaltet werden. Dies geschieht im VPN-Objekt durch die Einstellung **» nur Remote «** im Feld **» Starten «**.



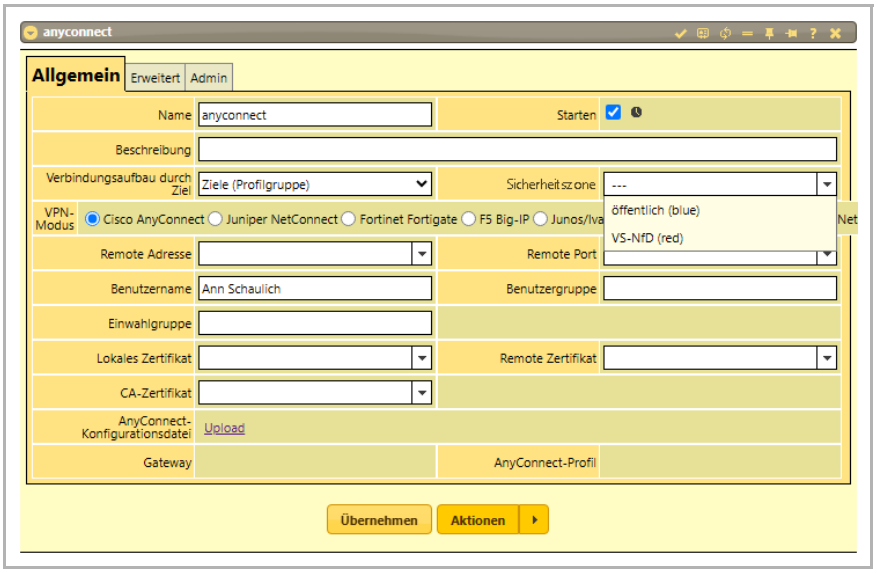
9.4.4 Neuerungen mit SBS V8 (VS-NfD)

Mit Version V8 (VS-NfD) können die Netzwerkverbindungen für einen SBS klassifiziert werden, um die Unterscheidung und Trennung verschiedene Sicherheitszonen in der Netzwerkkommunikation zu ermöglichen. Vorhandene VPN-Verbindungen werden abgebaut, bevor eine Verbindung zu einer abweichenden Sicherheitszone aufgebaut wird. Dadurch wird sichergestellt, dass beim Wechsel der Sicherheitszone keine ausspähbaren Daten im Speicher verbleiben. Ein gleichzeitiger Zugriff auf verschiedene Sicherheitszonen ist nicht möglich.

Dazu wird zunächst im Management-Container ein neues Konfigurationsobjekt vom Typ → **Sicherheitszone** angelegt und mit einem aussagekräftigen Namen, einer Zonen-ID sowie einer Farbe zur visuellen Unterscheidung versehen.:



Im VPN-Verbindungsobjekt müssen unter **» Allgemein: Verbindungsaufbau durch Ziel «** die im Zielcontainer konfigurierten Ziele bzw. Gruppe von Zielen für die VS-NfD-Umgebung angegeben werden. Im Feld **» Allgemein: Sicherheitszone «** wird die Zone ausgewählt:



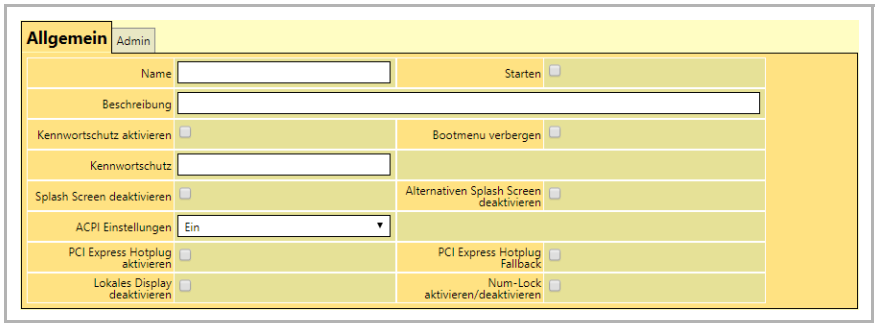
Nun wird beim Aufrufen eines Ziels geprüft, ob dieses als VS-NfD eingestuft ist.

Nutzt ein Ziel eine VPN-Verbindung, wird die Sicherheitszone von diesem übernommen. Nutzt ein Ziel keine VPN-Verbindung, wird die Sicherheitszone von der Netzwerkschnittstelle übernommen, über die das Zielsystem erreicht wird. Des Weiteren wird beim Start eines Ziels geprüft, ob bereits Ziele aktiv sind und ob diese eine andere Sicherheitszone als das aufgerufene Ziel haben. Ist das der Fall, werden alle aktiven Ziele beendet, um ein Abfließen von Daten zwischen unterschiedlich klassifizierten Netzwerken zu verhindern.

9.5 Optionale SBS-Funktionen

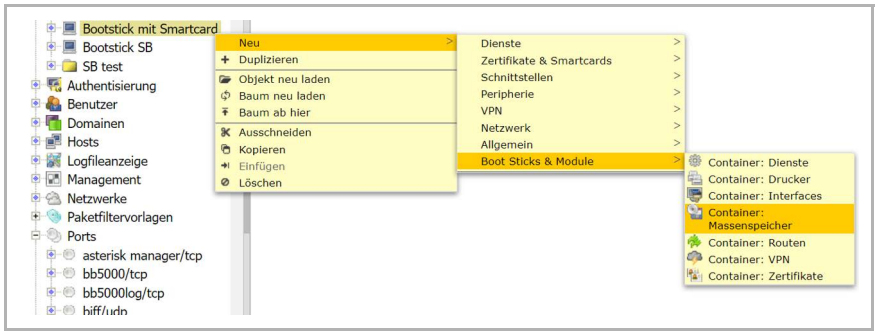
9.5.1 Bootloader

Unterhalb des Bootstick-Objektes muss im Container **» Dienste > Neu > Dienste > Bootloader Konfiguration «** angelegt werden, damit das Startverhalten des ECOS Secure Boot Stick beeinflusst und der Zugriff des Benutzers auf das Bootmenü eingeschränkt werden können.



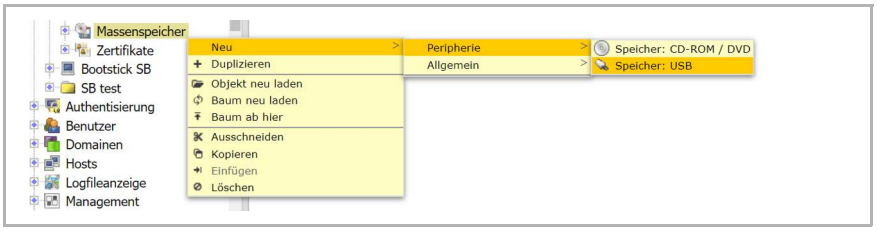
9.5.2 Massenspeicher

Sollen Massenspeicher wie z.B. USB-Sticks oder CD-ROMs in die Remote-Sitzung eingebunden werden, müssen diese gesondert freigeschaltet werden. Standardmäßig hat der Benutzer keinen Zugriff vom Terminalserver auf den Massenspeicher. Ist ein solcher Zugriff gewünscht, muss ein entsprechendes Speicher-Objekt in der Administrationsoberfläche unter dem Bootstick angelegt werden. Hierzu wird mit einem Rechtsklick auf das Bootstick-Objekt ein Container **»Massenspeicher«** angelegt.



Im Baum wird mit einem Rechtsklick auf den Massenspeicher-Container und unter

»Neu > Peripherie« den gewünschten Massenspeicher-Typ ausgewählt. Zur Auswahl stehen **»CD-ROM/DVD«** und **»USB«**.



Um den Zugriff auf ein Speichermedium zu erlauben, muss ein Häkchen bei **»Starten«** im Formular des Objektes gesetzt sein.

Im Falle eines USB-Sticks können die Felder **»Hersteller ID«**,**»Produkt ID«** und **»Seriennummer«** ausgefüllt werden. Es führt dazu, dass bestimmte Sticks zugelassen oder gesperrt werden können.

Hierzu können Filter gesetzt werden, in dem im USB-Objekt ein Haken bei **»Hersteller notwendig«**, **»Produkt notwendig«** und/oder **»Seriennummer«** gesetzt wird. Der Zugriff wird selektiv für bestimmte Hersteller, Produktreihen oder auch mithilfe der Seriennummer für einzelne Sticks erlaubt. Wird gewünscht den Zugriff zu verbieten, wird ein Haken bei **»Zugriff sperren«** gesetzt. Werden keine Einschränkungen eingegeben, werden alle USB-Sticks zugelassen.

Des Weiteren kann für das USB-Gerät zwischen den Lese- und Schreibzugriff unterschieden werden. Wird ein Haken bei **»Schreibzugriff«** gesetzt, können Daten auf dem Gerät hineingeschrieben werden.

Wird ein Haken bei **»Als RAW USB Gerät durchreichen«** gesetzt, wird das USB-Gerät nicht als Massenspeicher, sondern auf USB-Ebene umgeleitet. Dies ist normalerweise deutlich weniger performant, ist aber u.U. für bestimmte USB-Speicher notwendig

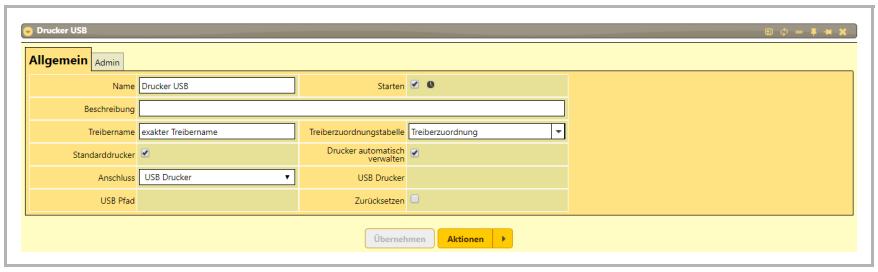
Diese Konfiguration wird nur bei Remote Zugriff per Citrix verwendet, wenn im Ziel-Objekt, ein Haken bei **»USB Umleitung aktivieren«** gesetzt ist.

9.5.3 Drucker

Ähnlich wie Massenspeicher, müssen auch Drucker zur Benutzung in der Remote-Sitzung freigeschaltet werden. Hierzu muss unter dem Bootstick-Objekt ein Drucker-Objekt angelegt werden. Dies geschieht über das Menü, das bei Rechtsklick auf das Bootstick-Objekt oder den darunter befindlichen Container **» Drucker «** im Baum erscheint. Das Drucker-Objekt befindet sich unter **» Neu > Peripherie «**.

Der ECOS Secure Boot Stick selbst beinhaltet keine Druckertreiber. Der passende Druckertreiber muss auf dem Terminalserver installiert sein. Der Bootstick teilt dem Terminalserver mit, welcher Drucker angeschlossen ist, sodass bei Verbindungsaufbau zum Terminalserver der richtige Treiber ausgewählt wird. Dabei reicht es meistens, wenige universelle Druckertreiber des jeweiligen Druckerherstellers zu installieren, um die meisten Druckermodelle bedienen zu können.

Unter dem Namen, der im Drucker-Objekt vergeben wird, wird dem Benutzer der Drucker innerhalb der Terminalserversitzung angezeigt.



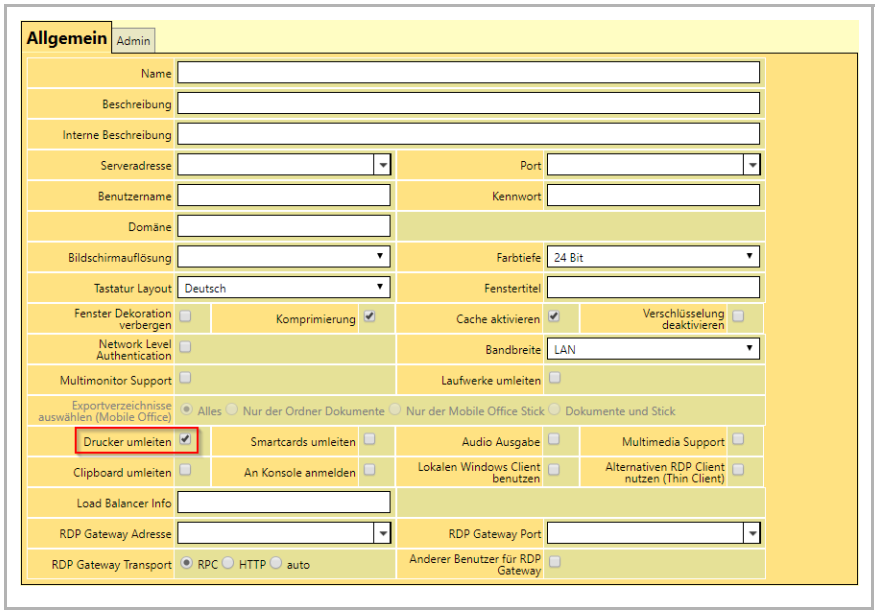
Im Drucker-Objekt muss der Anschluss des gewünschten Druckers angegeben werden. Ist der Drucker lokal angeschlossen, kann bei dem Feld **» Anschluss «** zwischen **» Parallel Port «** und **» USB Drucker «** gewählt werden. Soll ein Netzwerkdrucker genutzt werden, muss der Anschluss **» URI «** ausgewählt werden, daraufhin muss das Feld **» URI «** mit der Eingabe der Drucker-URI ausgefüllt werden.

Bei manueller Konfiguration eines Druckers muss der Treibername in das Feld **» Treibername «** eingetragen werden. Der Name muss genau so angegeben werden, wie der Druckertreiber auf dem Terminalserver benannt ist (inkl. Leerzeichen). In der Windows-Druckereinrichtung kann der entsprechende Name eingesehen werden. Bei automatischer Konfiguration sollte das Feld leer bleiben.

Wird ein Häkchen bei **» Drucker automatisch verwalten «** gesetzt, wird das Feld **» Treibername «**, je nach angeschlossenem Drucker, automatisch ausgefüllt und das Druckerobjekt aktiviert bzw. beim Entfernen des Druckers deaktiviert. Der Drucker muss dafür über USB angeschlossen sein.

Damit der Drucker vom Terminalserver aus genutzt werden kann, muss ebenso ein Häkchen bei **» Starten «** im Formular des Objektes gesetzt sein.

Da der über USB ermittelte Druckername nicht zwangsläufig dem Treibernamen entspricht, kann der Treibername mittels der Treiberzuordnungstabelle aus dem Druckernamen erzeugt werden. Dazu muss im Feld **» Treiberzuordnungstabelle «** auf eine Zuordnungstabelle verwiesen werden. In diesem Fall wird statt des Treibernamens, der im Feld **» Treibername «** eingetragen ist, der ihm zugeordnete Treibername aus der Zuordnungstabelle an den Terminalserver übermittelt.



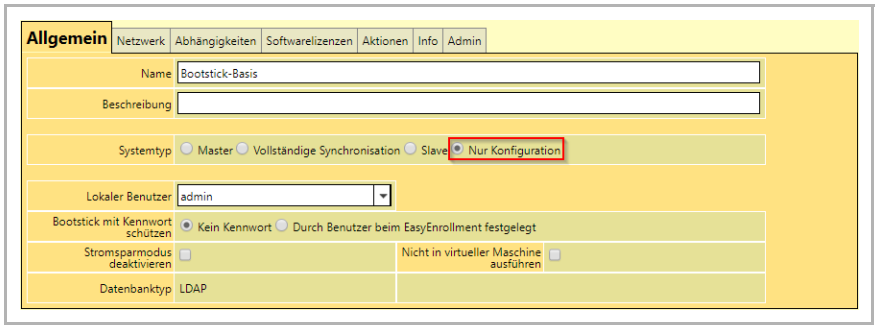
Zusätzlich muss im Formular des Remote Desktop Objektes bei dem Feld »Drucker umleiten« ein Haken gesetzt werden.

9.6 Vererbung

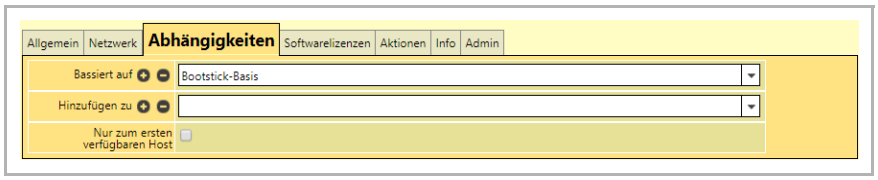
Möchte man mehrere Bootsticks mit ähnlicher Konfiguration erstellen, so empfiehlt sich eine Basis-Konfiguration, von der die Bootstick-Objekte die Konfiguration erben. Dadurch müssen Einstellungen nur einmal getätigt werden und auch spätere Änderungen müssen in der Konfiguration nur an einer zentralen Stelle ein-

gepflegt werden.

Um eine Bootstick-Basiskonfiguration anzulegen, muss zunächst wie bei der Erstellung eines einzelnen Bootsticks vorgegangen werden. Mit einem Rechtsklick auf den Container **» Bootsticks «** öffnet sich ein Menü, in welchem man unter **» Neu «** ein ECOS System-Objekt auswählt. Anstatt Systemtyp **» Slave «**, muss nun der Typ **» Nur Konfiguration «** im Reiter **» Allgemein «** ausgewählt werden. Nun können Konfigurationsobjekte, die für alle/viele Bootsticks identisch sind, unterhalb des Basis-Konfigurations-Objekts angelegt werden, wie z. B. der Software Update-Dienst oder VPN-Clients, soweit sie identische Einstellungen für alle Bootsticks haben.



Wird nun ein neuer Bootstick angelegt, muss lediglich im Reiter **» Abhängigkeiten «** im Feld **» Basiert auf «** die gewünschte Basis-Konfiguration angegeben werden. Dadurch übernimmt der Bootstick automatisch die Konfiguration aller unter der Basis-Konfiguration angelegten Dienste und Objekte.



Soll die Konfiguration eines Bootsticks an einzelnen Stellen von der Basiskonfiguration abweichen, müssen unterhalb des eigentlichen Bootstick-Objekts die entsprechenden Konfigurationsobjekte angelegt werden. Dadurch werden die entsprechenden Einstellungen in der Basiskonfiguration überschrieben.

Von manchen Objekttypen, zum Beispiel von Netzwerk-Interfaces, lassen sich mehrere Objekte desselben Typs anlegen. Ist ein solches in der Basisklasse und unter dem Bootstick-Objekt definiert, so wird das Objekt in der Basisklasse nicht überschrieben, sondern beide Objekte existieren nebeneinander.

Es besteht die Möglichkeit, von mehreren Basiskonfigurationen gleichzeitig Ein-

stellungen zu erben. Sind in den Basiskonfigurationen unterschiedliche Einstellungen für die Parameter getätigt worden, so übernimmt der Bootstick die Einstellungen der Basiskonfiguration, die an erster Stelle im Reiter **» Abhängigkeiten «** des Bootstick-Objektes konfiguriert sind.

9.7 Info zur Management-Verbindung

Bei Starten eines personalisierten ECOS Secure Boot Stick an einem ans Netz angeschlossenen Rechner, baut der Bootstick automatisch eine Verbindung zum Management auf. Die Verbindung kann über einen beliebigen TCP-Port erfolgen, der im Formular des ECOS System Connector konfiguriert wird.

→ *Siehe „9.2.2 | ECOS System Connector für SBS einrichten" auf Seite 104.*

Die Verbindung zum Management erfolgt verschlüsselt, basierend auf dem SSH-Protokoll. Es ist nicht möglich, die Verbindung zwischen Management und Bootstick über einen Proxy herzustellen, da sich die ECOS System Management Appliance und der ECOS Secure Boot Stick gegenseitig authentisieren, um eine sichere Verbindung zu garantieren und Manipulationen auszuschließen.

Zwischen ECOS System Management Appliance und dem ECOS Secure Boot Stick besteht eine Master-Slave-Beziehung. Sobald eine Verbindung zwischen beiden besteht, wird die Konfiguration für den Slave automatisch vom Master auf den Slave übertragen. Dabei werden nur Konfigurationsobjekte übertragen, die für den Slave notwendig sind. Die Änderungen werden mit der Übertragung sofort wirksam.

Über einen lokalen Admin-Benutzer ist es möglich, Konfigurationsänderungen lokal auf dem Bootstick vorzunehmen. Dies ist nicht zum Konfigurieren des Bootsticks gedacht, sondern nur dann, wenn Änderungen vorgenommen werden müssen, während keine Verbindung zur Management Appliance besteht. Änderungen, die auf dem Slave vorgenommen wurden, werden nicht zum Master übertragen und beim nächsten Master-Slave-Kontakt von den Einstellungen, die auf dem Master vorliegen, überschrieben.

9.8 Konfiguration des SBS zurücksetzen

9.8.1 Zurücksetzen des Sticks

Um ein Bootstick zurückzusetzen, drückt man im Dialog, indem normalerweise das

Bootkennwort eingeben wird, die Tastenkombination F12 und Enter. Daraufhin startet der Bootstick ohne Konfiguration. Nun ist ein erneutes Easy Enrollment möglich. Dies kann ebenso durch Klicken auf das ECOS-Symbol links unten in der Taskleiste und anschließendes Wählen der Optionen **» System** > **Aktivierung «** gestartet werden.

Bei Einsatz eines SBS ohne Smartcard wird ein neuer Aktivierungscode erforderlich. Der Aktivierungscode für das Easy Enrollment ist nur einmal gültig. Soll auf einem bereits aktivierten Bootstick erneut ein Easy Enrollment durchgeführt werden, muss zunächst ein neuer Aktivierungscode über die Management Appliance generiert werden.

→ *Siehe „9.3.1 | Easy Enrollment mit Aktivierungscode" auf Seite 116*.

9.8.2 Zurücksetzen des Sticks mit Smartcard

Soll der Bootstick mit einer anderen Smartcard gekoppelt werden, sollte die Konfiguration des Bootsticks zunächst gelöscht werden, bevor eine neue Smartcard eingesetzt wird. Diese würde sonst von dem Bootstick nicht erkannt und zu einer Fehlermeldung führen.

Das Zurücksetzen eines Sticks kann zentral über das Management, lokal auf dem Bootstick selbst oder beim Booten erfolgen.

Soll der Stick von der ECOS Appliance aus zurückgesetzt werden, muss das Bootstick-Objekt geöffnet werden, in der Registerkarte **» Aktionen «** muss die Option **» Konfiguration löschen «** ausgewählt werden. Daraufhin besteht die Möglichkeit **» Nur aktuelle Version «** oder **» Alle Versionen «** zu selektieren, anschließend muss auf **» Start «** gedrückt werden, um die Konfiguration zu löschen. Dieses Vorgehen erfordert, dass eine aktive Managementverbindung zwischen Stick und Management besteht.

Wenn der Stick gebootet ist, gibt es zwei Möglichkeiten den Stick zurückzusetzen. Die erste Möglichkeit erfolgt durch Klicken auf das ECOS-Symbol links unten in der Taskleiste, dort muss die Optionen **» System «** und **» Konsole «** ausgewählt werden. Daraufhin wird nach einem Login und einem Passwort gefragt. Das Login ist immer **» setup «**, das Passwort ist standartmäßig **» bb5000 «**, kann aber im Wartungsobjekt geändert werden. Nach der Eingabe dieser Daten, muss die Taste **» R «** für **» In Auslieferungszustand versetzen «** gedrückt werden.

Die zweite Möglichkeit besteht durch Klicken auf das ECOS-Symbol links unten in der Taskleiste und die Auswahl der Optionen **» Einstellungen «** und **» Administration «**. Dabei erscheint zunächst das Anmeldefenster der Administrationsoberflä-

che zur Authentifizierung (im Auslieferungszustand: Benutzer: admin; Kennwort: bb5000). Bei erfolgreicher Authentifizierung öffnet sich die Administrationsoberfläche. Das Zurücksetzen erfolgt wie oben schon für das Zurücksetzen über das Management besprochen (Bootstick-Objekt>Aktionen>Konfiguration löschen).

Wenn die Smartcard verloren gegangen oder defekt ist und der Stick somit nicht gestartet werden kann, so muss eine neue Smartcard mit Zertifikaten erstellt werden und diese in den Bootstick eingelegt werden

→ *Siehe „9.2.4.5 | Zertifikate auf Smartcard schreiben" auf Seite 114*.

Nun kann der Stick wieder gestartet werden. Wenn die Meldung **» bitte legen Sie die Smartcard ein «** angezeigt wird, muss die Taste F12 und Enter gedrückt werden, diese Tasten- Kombination löscht die Konfiguration.

9.8.2.1 Smartcard-Kopplung des Sticks zurücksetzen

Soll ein Stick mit einer anderen Smartcard benutzt werden, muss neben dem Löschen der alten Konfiguration die Kopplung des Sticks mit der Smartcard aufgehoben werden.

Das Zurücksetzen erfolgt durch die Tasten am Stick. (Siehe Administrator Handbuch ECOS Secure Boot Stick [SX]+[FX], Kapitel „1.7.4 Smartcard-Kopplung des Sticks zurücksetzen"). Danach kann der Bootstick nicht mehr genutzt werden und muss neu aktiviert werden. Ebenso gehen alle Daten im Datensafe verloren.

Nur wenn die Konfiguration des Sticks und der Smartcard-Kopplung des Sticks zurückgesetzt sind, ist es möglich den ECOS Secure Boot Stick für ein erneutes Easy Enrollment mit einer anderen Smartcard zu benutzen.

→ *Siehe „9.2.4.5 | Zertifikate auf Smartcard schreiben" auf Seite 114*.

10 ECOS Mobile Office Stick: Konfiguration und Enrollment

Der ECOS Mobile Office Stick (MOS) ist im Auslieferungszustand nicht konfiguriert und muss zunächst für den jeweiligen Anwendungsfall konfiguriert bzw. personalisiert werden. Dafür wird auf der System Management Appliance (SMA) eine Konfiguration für den MOS angelegt und dann mittels Easy Enrollment auf den Stick übertragen.

Folgende Elemente sind für die Verwaltung und Nutzung eines MOS erforderlich:

- Ein **»System Connector«**: Er ist das elementare Bindeglied zwischen der Appliance und den Sticks sowohl beim Rollout als auch bei späteren Konfigurationsänderungen. Zu ihm verbinden sich die Sticks und über ihn werden Anfragen von den Sticks an die Appliance weitergeleitet.
- Ein **»Software Update Server«**: Über den **»Software Update Server«** wird die Firmware des MOS Sticks auf dem aktuellen Stand gehalten.
- Ein **»Benutzer«** und dessen MOS-Optionen
- Ein **»Authentisierung«**-Objekt, das ermöglicht Authentisierungseinstellungen z.B. eine Passwort-Policy vorzunehmen.
- **»Ziele«** : Über die (Verbindungs-) Ziele kann der Benutzer des Mobile Office Sticks auf seine Anwendungsumgebung (z.B. einen Terminalserver) zugreifen. Nach der initialen Konfiguration auf Seiten der SMA kann der MOS mittels Easy Enrollment ausgerollt werden. Dabei wird der Stick erstmalig für den Benutzer personalisiert und kann unmittelbar nachfolgend genutzt werden.

Optional können folgende Elemente zusätzlich konfiguriert werden:

Ein **»Virtual Web Client«** (VWC) Dieser ermöglicht die Nutzung der MOS Software aus dem lokalen System ohne die Bindung an einen Stick. Für diesen Einsatzfall wird ein **»Virtual Web Client«** konfiguriert.

- Erscheinungsbild des MOS bzw. des VWC um eine Angleichung an CI Vorgaben im Einsatzgebiet zu ermöglichen.

10.1 Konfiguration des System Connector für MOS

Der **»ECOS System Connector«** wird unter der SMA im Container **»VPN«** angelegt. Die Anlage erfolgt im Allgemeinen nur einmalig. Danach wird der **»System Connector«** von allen MOS gleichermaßen verwendet.

Der MOS wird am Mac- oder Windows-Rechner angesteckt und baut eine gesicherte, verschlüsselte Verbindung zum **»System Connector«** auf. Vorher überprüft der MOS die Identität des Connectors anhand des Fingerabdrucks des öffentlichen Schlüssels.

Der **»System Connector«** benötigt eine im LAN/WAN erreichbare Netzwerkadresse, die im Feld **»Lokale Adresse für externe Anfragen«** angegeben wird, damit die nutzenden MOS ihre Anfragen an die Appliance richten können. Die Verbindung wird ebenfalls zur Erstellung und Verifizierung der Aktivierungscodes der Sticks verwendet.

Optional kann zusätzlich zur **»Lokalen Adresse für externe Anfragen«** eine **»Lokale Adresse für Anfragen aus dem LAN«** angegeben werden. Sind beide Adressen gesetzt, schickt der MOS bei Verbindungsaufbau eine Anfrage an beide Adressen und verbindet sich mit derjenigen, die zuerst antwortet.

Im Feld **» Port«** wird der gewünschte Port, über den der MOS den **»System Connector«** anspricht, konfiguriert.

Im Feld **»Version für MOS«** wird die gewünschte Softwareversion für den Stick ausgewählt. Die Version muss zur Verfügung stehen bzw. vorab als Update zur Verfügung gestellt werden.

→ *Siehe „10.2 | Software Update Server - Updates für MOS" auf Seite 133*.

Damit der **»System Connector«** aktiv wird, muss das Häkchen bei **»Starten«** gesetzt werden.

10.2 Software Update Server - Updates für MOS

Der **»Software Update Server«** dient dazu Software Updates innerhalb der Organisation bereitzustellen. Damit der MOS Updates beziehen kann, muss der **»Software Update Server«** gestartet sein → *Siehe „3.4.5 | Software-Update-Server" auf Seite 55*. Im Allgemeinen wird der **»Software Update Server«** nur einmalig eingerichtet und dient danach für alle eingesetzten Sticks als zentraler Update Service.

10.2.1 Software Update Image

Unter dem Container »Software Updates« wird ein »Software Update Image«-Objekt angelegt → *Siehe „13.3.1 | Bereitstellung eines Image für Update-Server" auf Seite 165*. Dieses Objekt dient dazu die verschiedenen Mobile Office Software-Versionen als Image bereitzustellen und zu verwalten. Das Image beinhaltet die benötigten Windows- und Mac-Dateien, um das Mobile Office System lokal ausführen zu können. Wird eine neue Version hochgeladen, wird diese nachfolgend an die Sticks verteilt - je nach Zuordnung des Images zum »Versionsverwaltung«-Objekt, sobald sich diese mit dem Update Server verbinden.

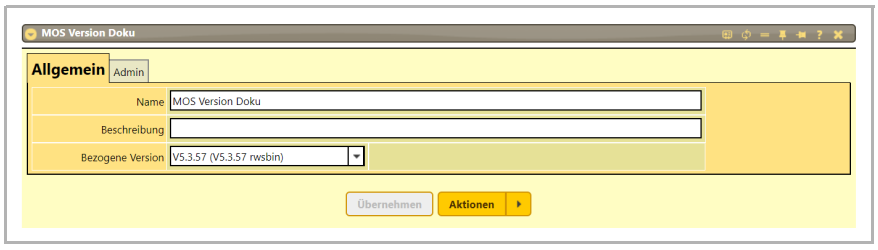
Der MOS und der VWC nutzen dabei das gleiche Image.

10.2.2 »Mobile Office Versionsverwaltung«-Objekt anlegen

Das »Mobile Office Versionsverwaltung«-Objekt dient dazu, die Softwareversionen für MOS zu verwalten. Dieses Objekt wird im Baum durch Rechtsklick auf den Container »Softwareupdates> Neu> Softwareupdates> Mobile Office Versionsverwaltung« angelegt.

Über das Feld »Bezogene Version« wird die gewünschte MO Version ausgewählt.

→ *Siehe „13.3.1 | Bereitstellung eines Image für Update-Server" auf Seite 165*.



10.3 Benutzer-Objekt für MOS einrichten

Der einzelne MOS wird zentral über die Appliance und dort über das »Benutzer«-Objekt in der Registerkarte »Mobile Office« verwaltet.

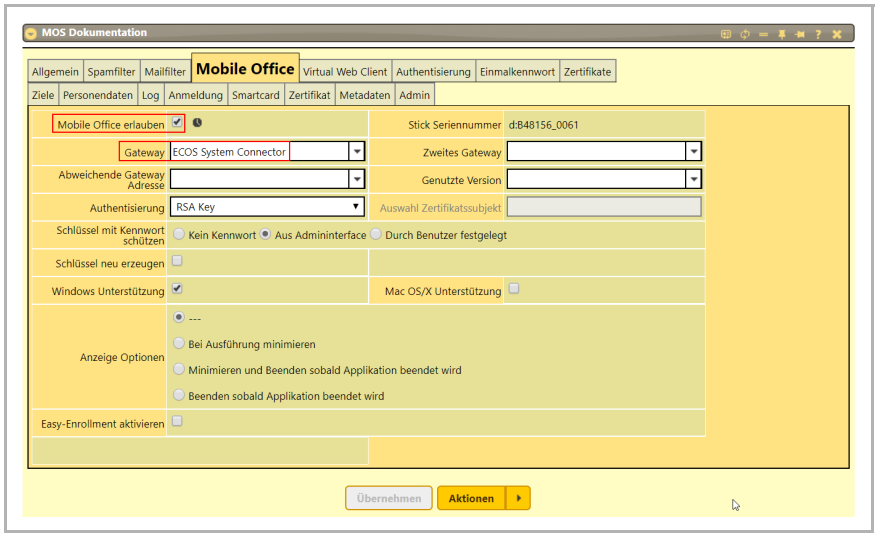
Um den Einsatz des MOS zu aktivieren wird ein Häkchen bei »Mobile Office erlauben« gesetzt.

Über **»Gateway«** muss der **»System Connector«** gewählt werden, um eine Verbindung mit dem MOS herzustellen. Über den System Connector werden dem MOS die Daten aus dem Serverobjekt (z.B. die lokale Adresse des Servers) zur Verfügung gestellt.

Optional kann bei **»Zweites Gateway«** ein zweiter System Connector angegeben werden. Der MOS verbindet sich dann mit demjenigen Connector, der schneller antwortet.

Für den Fall, dass die bei Gateway angegebene Serveradresse nicht erreichbar ist, kann im Feld **»Abweichende Gateway Adresse«** eine alternative Serveradresse angeben werden. Hierüber kann der Server zusätzlich bzw. aus einer anderen Umgebung mit abweichenden Adressen für den Client erreichbar werden.

Bei **»Windows Unterstützung«** oder **»Mac OS/X Unterstützung«** wird mit einem Häkchen markiert welches Betriebssystem benutzt werden darf.



10.3.1 MOS-Authentisierungsoptionen

Bei einem MOS muss sich ein Benutzer authentisieren. Über das Feld **»Authentisierung«** wird festgelegt, welcher Mechanismus zur Authentisierung des Benutzers verwendet wird. Die Auswahl richtet sich nach der verwendeten Art des MOS. Zur Auswahl steht: **»RSA Key«**, **»RSA aus Zertifikat«**, **»RSA, Konfiguration in Zertifikat«**, **»Zertifikat«**, **»Zertifikat per Subjekt auswählen«**, **»Zertifikat oder RSA Key«** oder **»Kennwort«**. Die Auswahl der Option legt fest, wie die Verschlüsselung erzeugt wird (mit welcher der Server die Authentisierung prüft) und was die Konfiguration für den Client zur Authentisierung am Server bereitgestellt wird.

Wird **»RSA Key«** ausgewählt, wird der **»RSA Key«** automatisch erzeugt und kann dann direkt zum MOS übertragen werden. Der **»RSA Key«** ist unbegrenzt gültig.

Wird **»Zertifikat«** ausgewählt, wird ein **»Zertifikat«** zur Authentisierung verwendet. Dabei werden Gültigkeitszeitraum und einen gegebenenfalls vorhandene CRL berücksichtigt. Das Zertifikat wird im Benutzerobjekt bei dem Reiter **»Zertifikate«** erzeugt oder hochgeladen. Zu dem Zertifikat muss eine passende CA existieren.

Wird **»Zertifikat per Subject auswählen«** ausgewählt, kann das Zertifikat auf einer Smartcard erzeugt werden oder als Softwarezertifikat vorhanden sein. Bei Benutzung dieses Features kann bei der Registerkarte **»Zertifikate«** das Häkchen **»Smartcard Zertifikat für VPN benutzen«** gesetzt sein und ein Smartcard Provider gewählt werden. Das Zertifikat kann vorher hochgeladen werden, es wird dann über das Subjekt automatisch auf der Smartcard gefunden.

Wird **»Zertifikat oder RSA Key«** ausgewählt, wird zur Authentisierung ein Zertifikat verwendet. Dabei werden Gültigkeitszeitraum und einen gegebenenfalls vorhandene CRL berücksichtigt. Das Zertifikat ist auf einer Smartcard hinterlegt. Welches Zertifikat auf der Smartcard verwendet wird, kann über einen regulären Ausdruck bestimmt werden, der im Feld Auswahl Zertifikatssubjekt angegeben wird.

Wird **»RSA aus Zertifikat«** ausgewählt, wird zur Authentisierung ein Zertifikat auf den Stick übertragen, es kann aber auch der passende RSA Key verwendet werden.

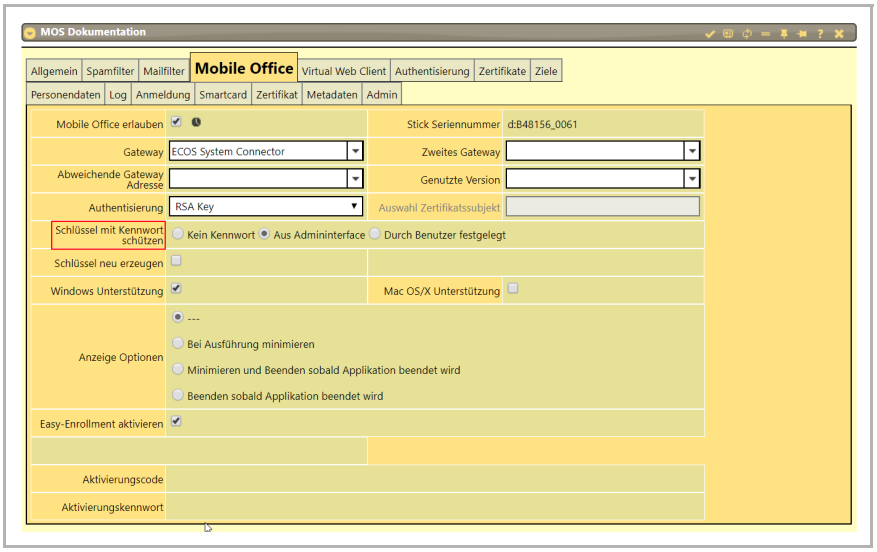
Wird **»RSA, Konfiguration in Zertifikat«** ausgewählt, wird der RSA Schlüssel aus dem Benutzerzertifikat verwendet. Diese Einstellung ist notwendig, wenn die Authentisierung für den MOS mit einem Token oder einer Smartcard erfolgen soll, das Token aber kein beschreibbares Bereich zur Verfügung stellt. Die Konfiguration wird dann innerhalb des Zertifikats gespeichert.

Wird **»Kennwort«** ausgewählt, erfolgt die Anmeldung per Benutzername/Kennwort. Diese ist die einzige Option ohne Privaten Schlüssel. Aus Sicherheitsgründe wird hier dann auch ein OTP (One Time Passwort) konfiguriert.

→ *Siehe „10.3.3 | Das Authentifizierungspasswort einrichten" auf Seite 138*.

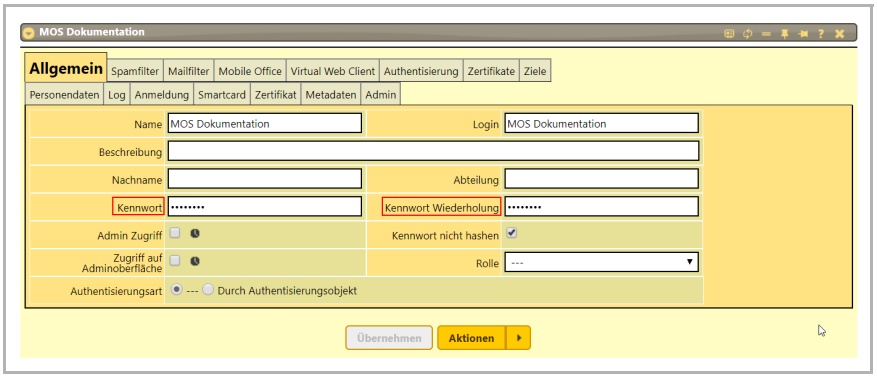
10.3.2 Die Authentisierung-Schlüssel schützen

Für die Authentisierung des SSH-Tunnels müssen die Schlüssel durch ein Kennwort geschützt werden. Hierzu wird bei dem Feld **»Schlüssel mit Kennwort schützen«** **»Kein Kennwort«**, **»Aus Admininterface«** oder **»Durch Benutzer festgelegt«** ausgewählt.



Wird **»kein Kennwort«** ausgewählt, wird der Schlüssel mit einem statischen Kennwort verschlüsselt, der die Stick-Seriennummer enthält. Wird die Konfiguration auf einem anderen Stick verwendet, scheitert daher das Auspacken des Schlüssels. Der private Schlüssel ist in diesem Fall auf der Appliance hinterlegt.

Wird **»Aus Admininterface«** ausgewählt, wird der Schlüssel mit der Seriennummer und dem Admin Kennwort verschlüsselt. Der private Schlüssel ist in diesem Fall auf der Appliance hinterlegt. Dazu muss in der Registerkarte **»Allgemein«** des Benutzer-Objektes ein Benutzerkennwort im Feld **»Kennwort«** angegeben werden. Zur Bestätigung dieses Kennwortes wird bei dem Feld **»Kennwort Wiederholung«** das Passwort noch mal angegeben. Eine Verbindung kann nur durch Eingabe des Kennwortes auf dem Client gestartet werden.



Wird **»Durch Benutzer festgelegt«** ausgewählt, wird der Schlüssel während des Easy Enrollment vom Stick generiert und mit der Seriennummer und vom Benutzer vergebenen Kennwort geschützt. Der private Schlüssel ist in diesem Fall NICHT auf der Appliance hinterlegt- nur der öffentliche Schlüssel. Hierzu kann der Administrator das Kennwort nicht ändern. Die Qualität des vom Benutzer vergebenen Kennworts wird vom globalen Authentisierungsobjekt festgelegt.

10.3.3 Das Authentifizierungspasswort einrichten

Im Objekt **»Authentisierung«** wird bei der Registerkarte **»Einstellungen«** das Authentifizierungspasswort eingerichtet. Hierzu wird in der Tabelle **»Kennwort und PIN Policy«** der Typ und die Qualitätsrichtlinien von Kennwörtern festgelegt.

Der **»Typ«** bestimmt die Art des Zugriffs. Zur Auswahl stehen **»Mobile Office Stick Kennwort«**, **»Mobile Office Stick Smartcard PIN«** und **»Secure Boot Stick Boot Kennwort«**. Mit **»Mobile Office Stick Kennwort«** sind nur die vom Benutzer selbst vergebenen Kennwörter gemeint.

Abhängig von den im Kennwort verwendeten Zeichenklassen wird eine Mindestlänge festgelegt. Triviale Kennwörter wie 12345678 werden ebenfalls verhindert.

Als eine Zeichenklasse gelten jeweils Kleinbuchstaben (a-z), Großbuchstaben (A-Z), Zahlen 0-9 und Sonderzeichen wie !$%.

Bei dem Feld **»Eine Zeichenklasse«** bestimmt die eingegebene Zahl die Mindestlänge des Kennworts bei der Verwendung einer Zeichenklasse, z.B. nur Kleinbuchstaben.

Bei **»Zwei Zeichenklassen«** bestimmt die eingegebene Zahl die Mindestlänge des Kennworts bei der Verwendung zweier Zeichenklassen, z.B. Groß/Kleinbuchstaben gemischt.

Bei **»Drei Zeichenklassen«** bestimmt die eingegebene Zahl die Mindestlänge des Kennworts bei Verwendung dreier Zeichenklassen (z.B. 0-9, a-z, A-Z).

Bei **»Vier Zeichenklassen«** bestimmt die eingegebene Zahl die Mindestlänge des Kennworts bei der Verwendung von vier Zeichenklassen (z.B. 0-9, a-z, A-Z und Sonderzeichen wie $%& ...).

10.3.3.1 Einmalkennwort

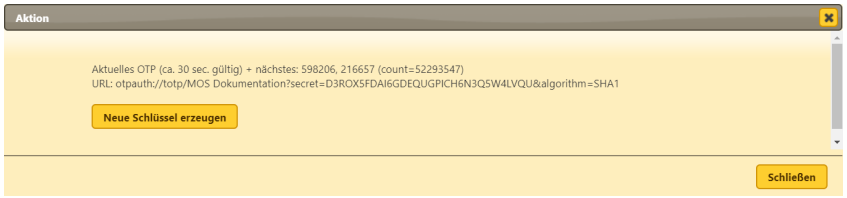
Das Einmalkennwort ist für eine einmalige Benutzung gültig. Für die Verwendung eines OTP-Kennworts (One Time Password) ist es erforderlich, dass der Benutzer und das System das Passwort kennen. Hierzu müssen zwei Verfahren angewendet werden, um dies zu erreichen: das Erstellen von Kennwortlisten und die Kennwortgenerierung. Bei den Kennwortlisten sind mehrere Kennwörter auf der Benutzer- und Systemseite hinterlegt. Die Konfiguration des Einmalkennworts erfolgt in der Registerkarte **»Einmalkennwort«** des Benutzer-Objektes.

Bei dem Feld **»Einmalkennwort Quelle«** wird festgelegt, wie das Einmalkennwort generiert wird. Zur Auswahl steht: **»nicht benutzen«**, **»Software«**, **»Manual«** und **»SMS«**. Ebenfalls kann ein angelegtes Token ausgewählt werden.

Wird **»nicht benutzen«** ausgewählt, schaltet es die OTP-Authentisierung für einen Benutzer aus.

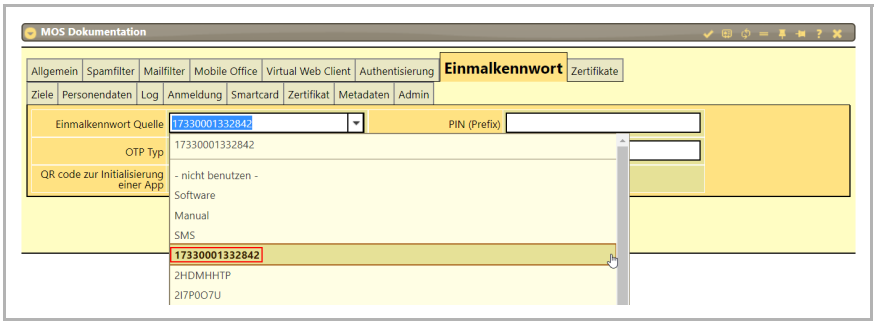
Wird **»Software«** ausgewählt, muss dafür vorab eine Applikation (z. B. Google Authenticator) über ein externes Gerät heruntergeladen werden, um dieses Verfahren benutzen zu können. Bei dem Feld **»QR code zu Initialisierung einer App«** über den Link **»Anzeigen«** wird den QR Code angezeigt. Durch die „Google App" wird der QR code eingescannt. Nach dem Scan des QR Codes erscheint auf dem Gerät in der Authenticator App ein sechsstelliger Code- das Einmalkennwort.

Wird **»Manual«** ausgewählt, werden von der Appliance Tokens generiert. Um die Passwörter anzeigen zu lassen, wird auf **»Start«** bei **»OTP Anzeigen«** gedrückt. Hierzu erscheint folgende Eingabemaske:



Wird **»SMS«** ausgewählt, bekommt der Benutzer eine SMS mit dem Einmalkennwort zugeschickt. Dazu muss die Mobilfunknummer bei dem Feld **»Mobilnummer für SMS«** angegeben werden. Alternativ kann auch in dem Feld eine Email-Adresse eingetragen werden.

Im Feld **»Einmalkennwort Quelle«** können auch Tokens ausgewählt werden.



Bei **»OTP Typ«** wird **»Zeitbasiert«** (TOTP) oder **»Ereignisbasiert«** (HOTP) SHA1/SHA256 ausgewählt. Die Auswahl des OPT Typs hängt davon ab, welche Art von Token benutzt wird. Werden OTP-Token einen neuen Code auf Knopfdruck generiert, wird **»Ereignisbasiert«** ausgewählt. Der Code ist hiermit so lange gültig, bis er von der Anwendung genutzt wird. Wird **»Zeitbasiert«** ausgewählt, werden OTP-Token Codes, die nur für eine bestimmte Dauer (z. B. 30 Sekunden) gültig sind, generieren. Nach Ablauf dieses Zeitraums muss ein neuer Code generiert werden.

Um noch mehr Sicherheit bei der Anmeldung zu erhöhen, besteht die Möglichkeit einen Wert bei dem Feld **»PIN (Prefix)«** einzugeben. Hierzu muss bei der Anmeldung dem erzeugten Passwort vorangestellt werden, damit sich der Benutzer anmelden kann. Es wird zum Beispiel **»VWC«** eingetragen, muss vor dem PIN dieser Wert eingegeben werden. Hierzu wird z.B. wie folgt geschrieben: VWC1234

Wird keine PIN eingetragen, so kann sich potenziell jeder, der den Token in die Hand bekommt und die weiteren Verbindungsdaten kennt am System anmelden.

10.4 »Zielen« bei einem MOS einrichten

Bei der Registerkarte **»Ziele«** des Benutzer-Objektes werden die vorangelegte Profile ausgewählt → *Siehe „5 | Ziele" auf Seite 67*, die dem Benutzer zugeordnet werden sollen. Die Einstellung kann über das Formular für den **»ECOS Secure Boot Stick«,** den **»ECOS Mobile Office Stick«** und den **»ECOS Virtual Web Client«** getrennt vorgenommen werden.

Beim **»ECOS Mobile Office Stick«** und **»ECOS Virtual Web Client«** gibt das Profil an, welche Applikation nach dem Tunnel-Aufbau gestartet werden soll, welche Netzwerkverbindungen dafür notwendig sind und welche Parameter die Applikation benötigt.

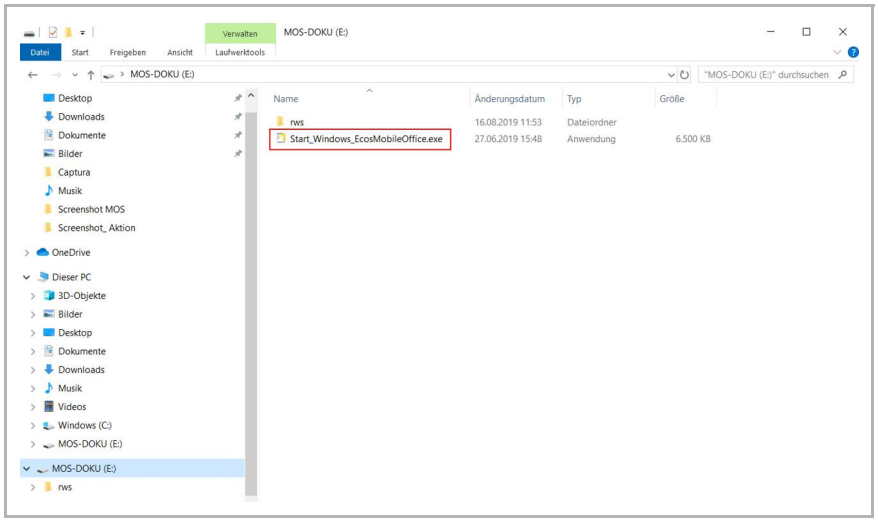
Es kann auch ein Container ausgewählt werden, der Profile enthält. Der Benutzer sieht dann alle Profile, die in diesem Container enthalten sind. Werden bestimmte Profilarten auf einem Gerät oder unter einem Betriebssystem nicht unterstützt, so werden sie dem Benutzer nicht angezeigt, obwohl sie für den Benutzer ausgewählt sind.

Die verschiedenen Profilarten sind z.B. **»Browser«**, **»Citrix We«**, **»Citrix ICA«, »RDP«**, **»Tunnel«**, **»SSL VPN«**, **»VNC«**, etc.

10.5 Easy Enrollment mit einem MOS

Das Easy Enrollment sorgt für eine soweit wie möglich automatisierte Personalisierung des MOS anhand der auf der SMA vorgenommenen individuellen Konfiguration.

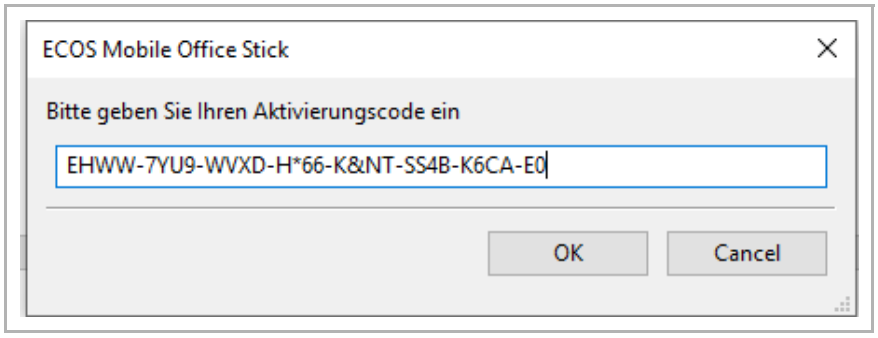
Für das Easy Enrollment muss der MOS an einen Rechner angeschlossen werden. Im Auslieferungszustand öffnet sich dort ein Fenster, in dem zwei Dateien sichtbar sind. Beim Aufruf des MOS-Start-Programms erscheint eine Eingabemaske, in der zunächst der »Aktivierungscode« und nach Bestätigung mittels **»OK«** das **»Aktivierungskennwort«** eingegeben werden muss.

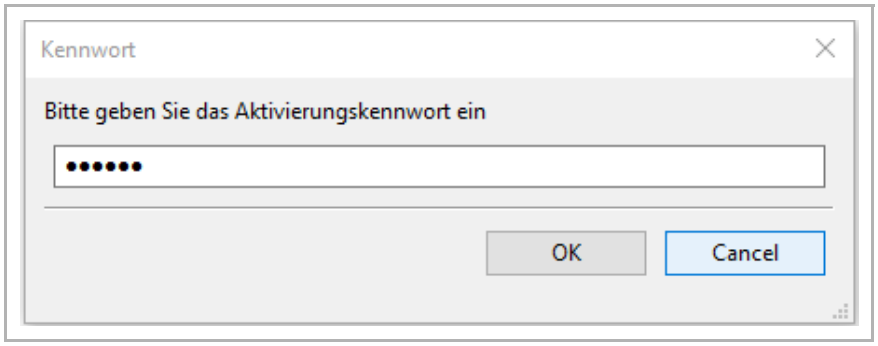


Aktivierungscode und -kennwort werden zuvor auf der SMA erzeugt.

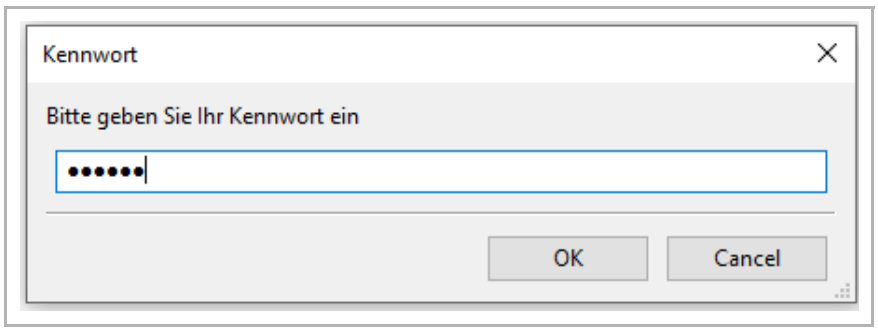
Dazu setzt ein Administrator auf der SMA im Benutzer-Objekt auf der Registerkarte **»Mobile Office«** den Haken bei **»Easy Enrollment aktivieren«**. Beim Klicken auf der Schaltfläche **»übernehmen«** werden der **»Aktivierungscode«** und das **»Aktivierungskennwort«** erzeugt und können nachfolgend dem Benutzer zur Aktivierung ausgehändigt bzw. zugesendet werden.

Nachdem der **»Aktivierungscode«** und das **»Aktivierungskennwort«** vom Benutzer auf dem Stick eingegeben wurden, kontaktiert der Stick das Management und lädt alle benötigten Konfigurationseinstellungen automatisch herunter.





Wurde beim dem Feld **»Schlüssel mit Kennwort schützen«** die Option **»Durch Benutzer festgelegt«** in der Registerkarte **»Mobile Office«** des Benutzer-Objektes aktiviert, muss der Benutzer bei der Durchführung des Easy Enrollment ein Kennwort vergeben. Dies wird in Zukunft bei jedem Start des Sticks abgefragt.



Soll das Kennwort des Benutzers zurückgesetzt werden - zum Beispiel, weil der Benutzer es vergessen hat - muss das Easy Enrollment erneut ausgeführt werden.

10.6 Der Virtual Web Client

Der **»Virtual Web Client«** (VWC) erlaubt den installationslosen Start der Mobile Office Software über einen Browser unter Windows oder MAC. Dazu wird im Browser die Start-URL auf der Appliance aufgerufen. Diese Seite enthält einen Download-Link, der die Mobile Office Software zur Verfügung stellt. Nach dem Download kann das Mobile Office gestartet werden.

10.6.1 Konfiguration im »System Connector«

Der **»VWC«** verbindet sich ebenso wie die Stick-gebundene Version MOS mit dem

System Connector der SMA. Hierzu muss die notwendige Konfiguration im Reiter **»Virtual Web Client«** des System Connector Objekts vorgenommen werden. Um die Nutzung des VWC freizuschalten,wird ein Häkchen bei **»Virtual Web Client Zugang zulassen«** gesetzt.

Bei **»Port«** wird ein tcp-Port ausgewählt, über den VWC Zugang per https erfolgt. Falls der **»System Connector«** durch gängige Web-Proxy-Server erreichbar sein soll, sollte hier der Standard-Port 443 (https) ausgewählt werden.

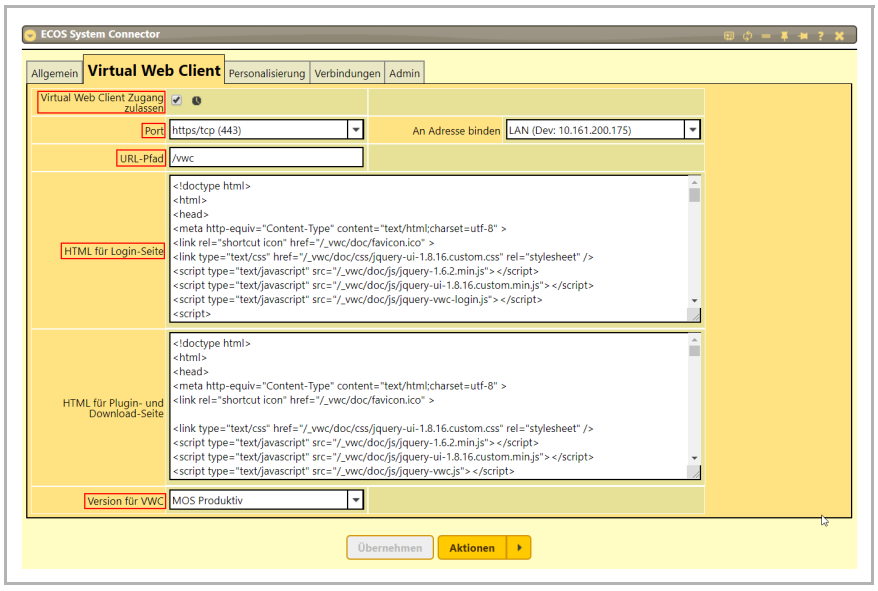
Ist bei **»An Adresse binden«** kein Ziel eingegeben, kann der Virtual Web Client Zugang über alle IP-Adressen der Appliance erfolgen. Alternativ kann der Zugang auch über eine hier angegebene Adresse aufgebaut werden.

Bei dem Feld **»Version für VWC«** wird die Version ausgewählt, die verwendet wird. Die verwendete Version des VWC muss nicht dieselbe wie die ausgewählte **»Version für MOS«** in der Registerkarte **»Allgemein«** des System Connectors sein.

Unter **»URL-Pfad«** wird ein lokaler Pfad (relativ zu der Adresse der Appliance) eingegeben, unter dem der VWC im Browser des Nutzers aufrufbar sein soll. Der Aufruf des VWC aus der Sicht des Browsers des Anwenders sieht damit folgendermaßen aus:

https://<Adresse der Appliance>/vwc bzw.

https://<Adresse der Appliance><:port>/vwc (bei Abweichung vom Standardport)



Das Aussehen der Anmeldung bei dem Virtual Web Client wird über **»Login-Seite«** konfiguriert. Hierzu wird der zu verwendende HTML-Code direkt bearbeitet.

10.6.2 Konfiguration im Benutzer-Objekt

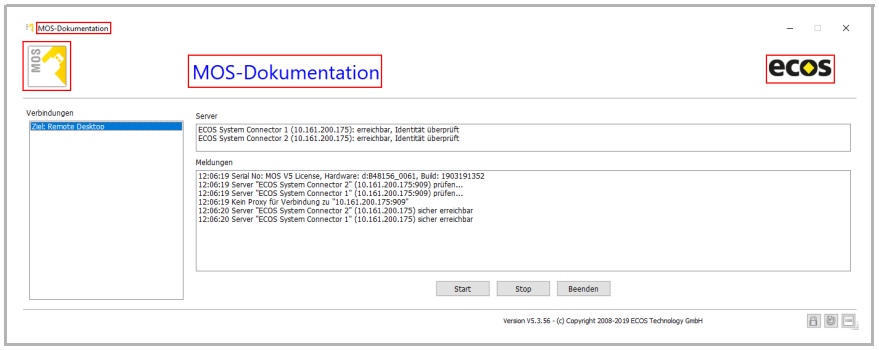
Der **»VWC«** wird im Benutzerobjekt über der Registerkarte **»Virtual Web Client«** konfiguriert. Diese Registerkarte hat analoge Möglichkeiten im entsprechenden Reiter wie die **»Mobile Office«** Registerkarte. → *Siehe „10.3 | Benutzer-Objekt für MOS einrichten" auf Seite 134*.

Um den Zugang zum VWC freizugeben, wird ein Häkchen bei **»Virtual Web Client erlauben«** gesetzt. Im Feld **»Authentisierung«** ist die Standard-Einstellung **»RSA Key«**. Für den VWC ist als 2. Faktor eine OTP- Authentisierung sinnvoll.

10.7 Erscheinungsbild von MOS sowie VWC

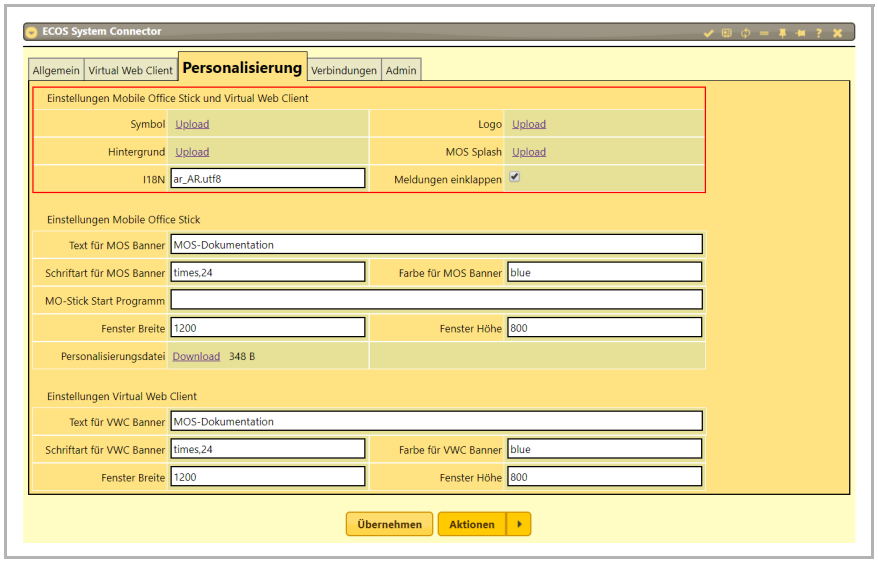
Über die Registerkarte **»Personalisierung«** des **»System Connector«** können Einstellungen vorgenommen werden, um das Aussehen der Oberfläche von einem MOS oder einem VWC an die Arbeitsumgebung des Nutzers anzupassen.

Das Programmfenster des MOS/VWC startet standardmäßig in der hier dargestellten Form:



Über der Registerkarte **»Personalisierung«** des **»System Connector«**-Objektes können das Logo im Eck oben-rechts und ein zusätzliches **»Symbol«** (im Eck oben-links hochgeladen werden. Die Bilder für das Logo und das Symbol werden in allen wichtigen Formaten (png, jpeg, gif) unterstützt. Um dabei einen freigestellten Hintergrund zu erzielen, muss das png-Format mit geeigneter Transparenzmaske im Bild verwendet werden.

Die Bilder werden mit einer Auflösung von 132 x 60 Pixel erwartet. Abweichende Auflösungen können zu fehlerhaften Darstellungen führen.



Ebenso kann ein Bild für den **»Hintergrund«** über den Upload-Link hochgeladen werden. Das Hintergrundbild muss 60 Pixel hoch und mindestens 800 Pixel breit sein. Die maximale Fensterbreite wird dabei auf die Hintergrundbreite gesetzt.

Beim Starten des Programms erscheint für eine Sekunde ein Startbild am Bildschirm, auch **»Splash«** genannt. Dieses Symbol kann auch über den Upload Link bei dem Feld »**MOS Splash«** hochgeladen werden.

Mittels **»Sprache«** wird die gewünschte Sprachversion für den Nutzer eingestellt.

Der Text - mittig im oberen Bannerbereich wird in dem Feld **»Text für MOS Banner«** bzw. **»Text für VWC Banner«** eingetragen. Der Text wird zudem auch im Fenstertitel des Programm-Fensters verwendet. Zudem können **»Schriftart für MOS Banner«** bzw. **»Schriftart für VWC Banner«** und Textfarbe **»Farbe für MOS Banner«** bzw. **»Farbe für VWC Banner«** abgestimmt werden. Als Farbwerte werden die für HTML bzw. CSS gängigen Farbnamen (z.B. BLACK) sowie RGB-Werte (z.B. #008000) verwendet.

Damit die Anpassungen des Erscheinungsbilds bereits vor der Personalisierung eines MOS sichtbar werden, kann auf Basis der vorgenommenen Konfiguration eine Motiv-Datei **»custom.xml«** heruntergeladen werden und im Ordner **»rws\win\rws«** auf dem noch nicht personalisierten Stick abgelegt werden.

11 Hochverfügbarkeit (High Availability)

Die Hochverfügbarkeitskonfiguration dient dazu, beim Ausfall eines Systems den Betrieb sicherzustellen. Dazu werden zwei oder mehr Appliances so konfiguriert, dass die notwendigen Funktionen von mehr als einer Appliance zur Verfügung gestellt werden können. Im Normalbetrieb ist es dabei sowohl möglich, dass nur eine Appliance aktiv ist, wie auch, dass mehrere Appliances aktiv sind. In diesem Fall besteht die Möglichkeit eine Lastverteilung für bestimmte Dienste einzurichten. Alle Appliances zusammen bilden ein Cluster.

11.1 Voraussetzungen für High Availability (HA)

Um ein Cluster aufzubauen und hochverfügbar zu machen, müssen mindestens zwei Systeme konfiguriert werden:

- Genau eine Appliance vom Systemtyp **»Master«**

Das Master-System ist das erste System, welches konfiguriert wird. Auf diesem wird die vollständige Konfiguration erstellt. Dieses Objekt wird als Master-Appliance bezeichnet → *Siehe „11.1.1 | Master-Appliance einrichten" auf Seite 147*.

- Eine oder mehrere Appliances vom Systemtyp **»Vollständige Synchronisation«**

Nach dem Erstellen der Konfiguration auf dem Master wird eine bidirektionale Synchronisation mit diesem System eingerichtet. Im Folgenden wird es als Master-Slave-Verbindung genannt. Danach sind beide Systeme gleichberechtigt. Dieses Objekt wird als vollsynchronisierte Slave-Appliance bzw. Slave-Appliance bezeichnet → *Siehe „11.1.2 | Vollsynchronisierte Slave-Appliance einrichten" auf Seite 148*.

Optional können noch weitere System-Objekte angelegt werden, die der Vereinfachung der Konfiguration bzw. dem Umschwenken der Konfiguration zwischen den Systemen beim Ausfall eines Systems dienen. Diese Appliance-Objekte sind vom Systemtyp **»Nur Konfiguration«**
→ *Siehe „11.2 | Vereinfachung der Konfiguration durch Vererbung" auf Seite 149* und → *Siehe „11.3 | Konfiguration bei Ausfall umschwenken" auf Seite 151*.

11.1.1 Master-Appliance einrichten

Die Master-Appliance benötigt ein **»ECOS System Connector«** Objekt, damit sich

die Slave-Appliance verbinden kann. Der **»ECOS System Connector«** wird unter der ECOS Appliance im Container **»VPN«** angelegt. Damit er aktiv ist, muss das Häkchen bei **»Starten«** gesetzt sein. Zusätzlich muss die Netzwerkadresse, über die er erreichbar sein soll, im Feld **»Lokale Adresse für externe Anfragen«** angegeben werden. Optional kann zusätzlich zu der **»Lokale Adresse für externe Anfragen«** eine **»Lokale Adresse für Anfragen aus dem LAN«** angegeben werden. Es ist nur eine der beiden Adressen notwendig, diese muss aber von der Slave-Appliance aus erreichbar sein. Im Feld **»Port«** kann der gewünschte Port für die Master-Slave-Verbindung konfiguriert werden. Wird kein Port angegeben, wird der Standard-Port 909 verwendet.

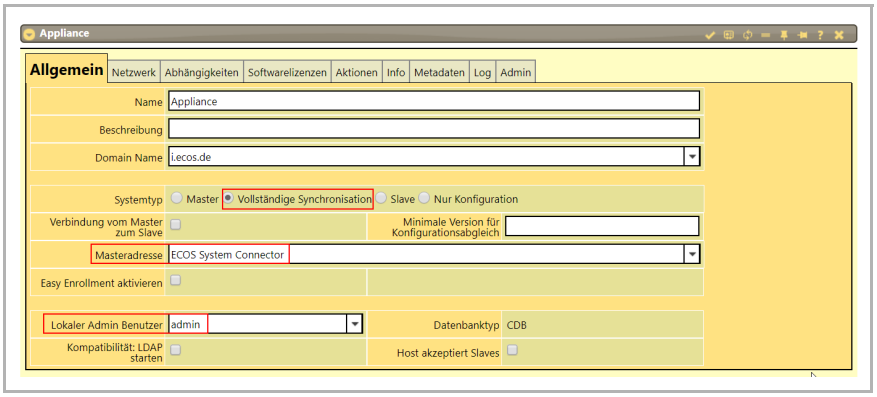
Um die Konfigurationen verteilen zu können, wird das **»Software Update Server«** Objekt benötigt. Dieses wird unterhalb der Master-Appliance im Container **»Dienste«** angelegt. Damit es aktiv ist, muss das Häkchen bei **»Starten«** gesetzt sein.

11.1.2 Vollsynchronisierte Slave-Appliance einrichten

Um die Slave-Appliance anzulegen, dupliziert man am einfachsten die Konfiguration der Master-Appliance und passt diese an. Hierzu erstellt man bei der Master-Appliance durch Klicken auf die Schaltfläche **»Aktionen > Duplizieren«** eine zweite Appliance.

Im Formular der zweiten Appliance muss zunächst der Name abgeändert werden und der **»Systemtyp«** auf **»Vollständige Synchronisation«** statt **»Master«** eingestellt werden.

Im Feld **»Masteradresse«** wird der zuvor angelegte **»ECOS System Connector«** ausgewählt. Bei **»Lokaler Admin Benutzer«** muss ein Benutzer, der dadurch Admin-Rechte auf der Slave-Appliance bekommt, ausgewählt werden. Gegenbenenfalls muss im Reiter **»Netzwerk«**, das Gateway sowie der DNS Server angepasst werden.



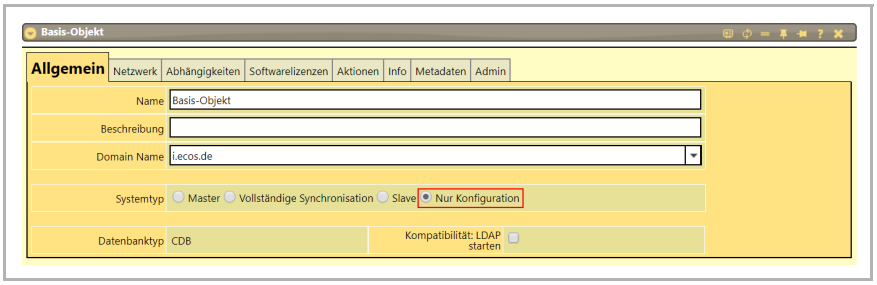
Weiterhin ist es notwendig, die IP-Adresse im **»Netzwerk-Interface«** Objekt → *Siehe „3.2.1 | Interfaces" auf Seite 46* abzuändern. Ggf. sind weitere Abweichungen zwischen den Appliances entsprechend anzupassen. Das **»ECOS System Connector«** Objekt wird auf der Slave-Appliance nur dann benötigt, wenn diese als Master für den ECOS Secure Boot Stick dienen soll. Ansonsten kann es gelöscht werden.

11.2 Vereinfachung der Konfiguration durch Vererbung

Es besteht die Möglichkeit, Konfigurationsobjekte, die für beide Appliances gleich sind, in eine gemeinsame Basis-Konfiguration auszulagern. Dies hat den Vorteil, dass die Konfiguration nur einmal vorhanden sein muss und dass bei Änderungen diese automatisch auf beide Appliances angewendet wird.

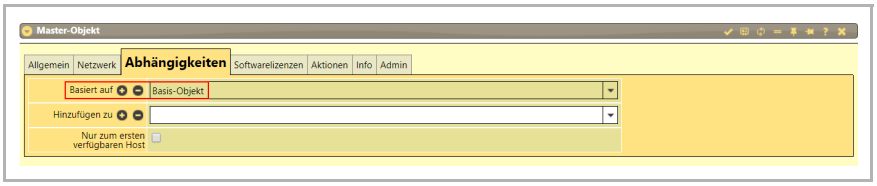
11.2.1 Basis-Konfiguration erstellen

Eine Basis-Konfiguration wird wie eine normale Appliance angelegt, nur, dass im Appliance-Objekt beim **»Systemtyp« »Nur Konfiguration«** ausgewählt wird. Ansonsten können unterhalb des Appliance-Objektes alle Konfigurationsobjekte ganz normal angelegt werden und bilden damit die Basis-Konfiguration.



11.2.2 Vererbung konfigurieren

Bei allen Appliances, die von einer Basis-Konfiguration erben sollen, muss auf der Registerkarte **»Abhängigkeiten«** im Feld **»Basiert auf«** das Basis-Objekt ausgewählt werden.



Die so konfigurierten Systeme erben nun die Konfiguration der Basis-Konfiguration, d.h. alle Dienste, die in der Basis-Konfiguration angelegt sind, werden damit auch Teil der Konfiguration des Systems, das erbt. Sind in der Konfiguration des Systems, das erbt, bereits Konfigurationen vorhanden, so haben diese Vorrang vor der Konfiguration in der Basis-Konfiguration. Für Objekte, von denen es mehr als eines geben kann (wie z.B. Netzwerkinterfaces), werden sowohl die Konfigurations-Objekte aus der Basis-Konfiguration, wie auch die Konfigurations-Objekte aus dem System, das erbt, Teil der Konfiguration.

Eine Appliance kann dabei von mehr als einer Basis-Konfiguration erben, ebenso wie Basis-Konfigurationen wieder von anderen Basis-Konfigurationen erben können.

Soweit vorhanden, können Konfigurationen, die auf allen Appliances vorhanden sind, damit in die Basis-Konfiguration verschoben werden.

11.3 Konfiguration bei Ausfall umschwenken

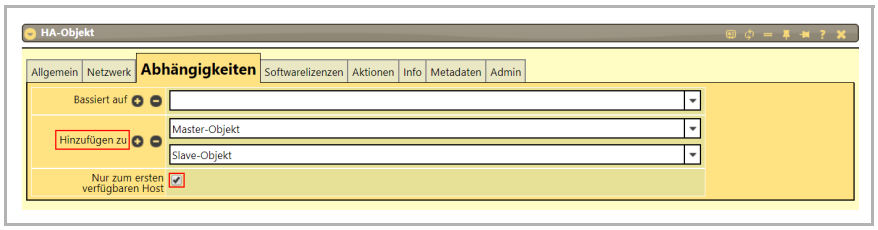
Es besteht die Möglichkeit, Konfigurationseinstellungen nur auf einem System zu aktivieren und diese bei Ausfall dieses Systems, auf ein anderes System umzuschwenken. Dies ermöglicht z.B. das „Wandern" einer HA-IP-Adresse von einem System zum anderen, sobald das System, auf dem die HA-IP-Adresse konfiguriert wurde, nicht mehr verfügbar ist. Dadurch sind nun unter der gleichen IP-Adresse die Dienste der zweiten Appliance erreichbar. Dies ist nicht nur für IP-Adressen, sondern für jegliche Konfiguration möglich.

11.3.1 HA-Konfiguration einrichten

Konfigurationseinstellungen, die von einem System zum anderen "wandern" sollen, werden als HA-Konfiguration, ähnlich wie eine Basis-Konfiguration angelegt → *Siehe „11.2.1 | Basis-Konfiguration erstellen" auf Seite 149*. Auch hier ist der **»Systemtyp« »Nur Konfiguration«** zu wählen.

11.3.1.1 HA-Konfiguration zu Appliance-Objekten hinzufügen

Um den gewünschten Effekt zu erzielen, muss im Appliance-Objekt der HA-Konfiguration ausgewählt werden, zu welchen Systemen sie hinzugefügt werden soll. Dazu auf der Registerkarte **»Abhängigkeiten«**, über das Feld **»Hinzufügen zu«** die Master-Appliance und dann die Slave-Appliance auswählen. Wird ein Haken bei **»Nur zum ersten verfügbaren Host«** gesetzt, wird die HA-Konfiguration nur zu der Konfiguration hinzugefügt, die als erstes in der Liste angegeben ist. Ist dieses System nicht verfügbar, so wird sie zum zweiten Objekt hinzugefügt. Dadurch „wandern" die Konfigurationseinstellung der HA-Konfiguration quasi zwischen den Systemen, sobald das erste System nicht mehr verfügbar ist oder wieder verfügbar wird.



11.4 Synchronisation aufbauen

11.4.1 Übertragen der Konfiguration vom Master zu Slave

Um die Konfiguration vom Master zu Slave zu übertragen, wird in dem Konfigurationsobjekt der Master-Appliance über die Registerkarte **»Aktionen« »Konfigurationsexport«** ausgewählt. Es öffnet sich ein Untermenü, in dem die Felder **»Admin Benutzer des Zielsystems«, »Admin Kennwort«, »Adresse des Zielsystems«** und **»Port der Admininterface«** gefüllt werden müssen. Durch Klicken auf die Schaltfläche **»Start«** wird der Konfigurationsexport gestartet. Dadurch verbindet sich das Master-System mit dem Slave-System, überträgt die komplette Konfiguration und richtet die Synchronisation ein.

11.4.2 Privater Schlüssel der CA übertragen

Aus Sicherheitsgründen wird der private Schlüssel der CAs während der Konfigurationsübertragung nicht weitergegeben. Private Schlüssel der Root CAs werden nicht synchronisiert. Damit der private Schlüssel vom Master auf die Slave-Appliance übertragen wird, muss auf der Master-Appliance im CA-Objekt über das Feld **»Zertifikat als PKCS#12«** der private Schlüssel heruntergeladen werden und dann im Admin-Interface der Slave-Appliance im selben Objekt wieder hochgeladen werden.

11.4.3 Systeme Prüfen

Im System Connector Objekt im Reiter **»Verbindungen«** wird angezeigt, welche die Slave-Appliances sind, mit denen der Master sich verbunden hat.

Um die Synchronisation zu testen, können Konfigurationsänderungen auf einer Appliance vorgenommen werden (z.B. Name oder Beschreibung). Bei erfolgreicher Synchronisation kann man die Änderung im Admin-Interface der anderen Appliances sehen. Änderungen werden in beide Richtungen übertragen.

12 DocExpressions

DocExpressions dienen dazu Werte aus verschiedenen Quellen zusammen zu setzen bzw. zu berechnen. DocExpressions führen eine oder mehrere Operationen auf ihr Eingangswerte aus und liefern ein Ergebnis. Dieses kann dann für Validierungen oder als Standardwert in **»Vorlagen«** verwendet oder im Rahmen von **»Assistenten«** herangezogen werden. Weiterhin ist es bei **»Abfragen«** möglich komplexe Abfragen mittels DocExpressions zu formulieren.

Als Eingangswerte können in DocExpressions neben Konstanten auch Attribute von Konfigurationsobjekten verwendet werden. Ebenso ist es möglich Verweise innerhalb von Konfigurationsobjekten auf andere Konfigurationsobjekten zu verfolgen und dann deren Attribute als Eingangswerte zu verwenden.

DocExpressions greifen immer nur lesend auf Konfigurationsobjekte zu. Innerhalb der DocExpressions findet keine Veränderung an Konfigurationsobjekten statt.

12.1 DocExpressions Anwendungen

12.1.1 Validierung

Innerhalb von **»Vorlagen«** können DocExpressions dazu verwendet werden, um sicherzustellen, dass nur erlaubte Werte in ein Konfigurationsobjekt gespeichert werden. DocExpressions kommen dann zum Einsatz, wenn die Validierung mit den einfachen Operatoren nicht abgebildet werden kann.

12.1.2 Vorbelegung

DocExpressions liefern einen Wert, der in **»Vorlagen«** oder **»Assistenten«** zur Vorbelegung benutzt werden kann. Dieser Wert kann aus beliebigen anderen Attributen, anderen Objekten oder auch z.B. auch mittels Datum und Zeit berechnet werden. Neu anzulegende Objekte können so sinnvoll vorbelegt werden. Für Zertifikate kann z.B. eine Gültigkeit bis zu einem festen Termin in der Zukunft berechnet werden → *Siehe „12.4 | Beispiel" auf Seite 162*.

12.2 Konfigurationsobjekt »DocExpression Debugger«

DocExpressions sind unter Umständen komplex zu schreiben. Um diese korrekt zu entwickeln und zu testen, bevor sie angewendet werden, kann man ein **»DocExpression Debugger«** Objekt verwenden. Dies kann durch Rechtsklick auf dem Management-Objekt **»Neu > Management > DocExpression Debugger«** angelegt werden.

12.2.1 Reiter »Allgemein«

Im Reiter **»Allgemein«** wird über das Feld **»Dokument«** ein beliebiges Objekt ausgewählt. Attribute innerhalb der DocExpressions beziehen sich dann auf dieses Objekt. Wird kein Objekt ausgewählt, bezieht sich die DocExpressions auf den **»DocExpression Debugger«** selbst.

Über das Feld **»Docexpression«** wird der Ausdruck eingegeben. Ist die Schreibweise korrekt eingegeben, erscheint der Rückgabewert im Feld **»Ergebnis«**. Ist die DocExpression falsch eingegeben, erscheint eine Meldung im Feld **»Fehler«**.

Im **»Docexpression«** Feld werden Zeichen, die nach einem #-Zeichen kommen ignoriert.

Das Feld **»Wiederholungen«** ermöglicht die Performance der DocExpressions zu messen.

Über die Tabelle **»Arrayvariablen«** (Name des Attributes: „docexpr_vars“) können Arrays getestet werden. Das erste Element des Arrays hat den Index 0.

12.2.2 Reiter »Metadaten«

Das Attribut **»metadata«** entspricht den Metadaten im Reiter **»Metadaten«** und kann zum Testen von Hashes verwendet werden.

12.2.3 Reiter »Funktionen«

Im Reiter **»Funktionen«** sind alle Funktionen die in DocExpressions verwendet werden können aufgelistet. Diese Übersicht dient als Hilfestellung.

→ *Siehe „12.3.4 | Funktionen" auf Seite 157*

12.3 Syntax

DocExpressions bestehen aus Konstanten, Attributen von Konfigurationsobjekten, Operatoren und Funktionen.

DocExpressions sind formatfrei und können beliebig umgebrochen bzw. eingerückt werden. Leerzeichen werden, außer in Zeichenkettenkonstanten, ignoriert.

12.3.1 Konstanten

12.3.1.1 Zahlen

Als numerische Konstanten wird die Ganzzahl (z.B. 123) und die Gleitkommazahl (z.B. 0.123) unterstützt.

12.3.1.2 Zeichenketten

Zeichenketten sind in einfache oder doppelte Anführungszeichen (' oder ") eingeschlossen.

Beispiel: 'abc' oder "abc"

12.3.2 Attribute

Konfigurationsobjekte bestehen aus Attribute. Alle Attribute, die in einem Konfigurationsobjekt aktuell gesetzt sind, können über die »Admin« Registerkarte im Quelltext des Konfigurationsobjektes angezeigt werden. In der DocExpressions Syntax beginnen Attribute immer mit einem $ Zeichen z.B $description.

Attribute können dabei von unterschiedlichem Typ sein. Zeichenkette, Ganzzahl, Kommazahl, aber auch Array, Hash oder Datasource.

12.3.2.1 Array Attribute

Um auf ein Element innerhalb eines Arrays zuzugreifen, muss der Index in eckigen Klammern stehen z.B $docexpr_vars[1].

12.3.2.2 Hash Attribute

Um auf ein Element innerhalb eines Hashes zuzugreifen, muss der Schlüsselwert in geschweiften Klammern stehen, z.B. $metadata{'Option2'}.

12.3.2.3 Datasource Attribute

Datasource Attribute verweisen auf Werte in anderen Konfigurationsobjekten. DocExpressions ermöglichen es, diesem Link zu folgen und auf die Werte in diesen anderen Objekten zuzugreifen. Für den Verweis wird der Operator »->« verwendet. Auf der linken Seite steht das Attribute, welches auf ein anderes Objekt verweist, auf der rechten Seite, das Attribute in dem Objekt auf das verwiesen wird, auf welches zugegriffen werden soll. Beispiel: $cert_ca->cert_subject: Das Attribute »cert_ca« verweist auf die CA eines Zertifikats. In dem Beispiel wird somit das Subjekt der CA eines Zertifikates ermittelt.

12.3.3 Operatoren

Die einzelnen Werte und Attribute können mittels Operatoren verknüpft werden. Unterstützt werden folgende Operatoren:

- + Addition
- - Subtraktion
- / Division
- * Multiplikation
- && Logisches Und
- || Logisches Oder
- -> Verweise auf ein anderes Konfigurationsobjekt
- == Gleich (Zahl oder Zeichenkette)
- != Nicht gleich (Zahl oder Zeichenkette)
- < Kleiner (Zahl)
- <= Kleiner gleich (Zahl)
- > Größer (Zahl)
- || Größer gleich (Zahl)
- ! Nicht

12.3.4 Funktionen

Funktionen wenden, ähnlich wie die DocExpressions selbst, eine Operation auf ihre Argumente an und liefern das Ergebnis zurück. Funktionsargumente stehen in runden Klammern, die Klammern müssen auch angegeben werden, wenn die Funktion keine Argumente hat.

Funktionen können eine beliebige Anzahl von Argumenten haben. Es müssen immer alle Argumente angegeben werden. Ausnahme sind Argumente, die Standardwerte haben (in der Auflistung unten mit eckigen Klammern [] gekennzeichnet). Solche Argumente können weggelassen werden. In diesem Fall werden die Standardwerte verwendet.

Argumente von Funktionen können auch wiederum DocExpressions sein. Sie können also beliebig geschachtelt werden.

12.3.4.1 Liste der verfügbaren Funktionen

- **all(array, re [, throw()])**
  ist wahr, wenn alle Elemente von Array auf »re« matchen (sonst false/throw).

- **and(a, b) bzw. a && b**
  ist die logische und-Verknüpfung von »a« und »b«.

- **any(array, str [, throw()])**
  ist wahr, wenn wenigstens ein Element von »array« exakt »str« ist (sonst false/throw).

- **apply(array, expr)**
  erzeugt ein neues Array, wobei »expr« auf jedes Element angewendet wird ($_ in »expr« ist aktuelles Element).

- **array_add(array, elem [, pos])**
  erzeugt ein neues Array mit Element an »pos« / am Ende.

- **array_count(array, elem [, pos])**
  liefert die Anzahl der Elemente im Array.

- **array_delete(array [, pos])**
  löscht das Element »pos« / das Letzte.

- **array_element(array, i1 [, i2])**
  liefert das Array Element »i« bzw. »i1«,»i2«.

- **array_index_of(array, str)**
  liefert die Position von »String« im »Array«.

- **array_sort(array)**
  liefert eine sortierte Kopie.

- **base64decode(str)**
  dekodiert den base64 String.

- **base64encode(str)**
  liefert »str« base64 kodiert.

- **concat(str1, str2)**
  hängt »String2« an »String1« an.

- **cond(c, wahr, falsch)**
  liefert den Wert von »wahr« /»falsch«, je nach »c«. Für »wahr« /»falsch« kann »throw()« verwendet werden.

- **datasource(attribut, data)**
  liefert den Wert »data« des Datasource-Attributs Data.

- **date(t [, delta])**
  liefert Datum zu »t« als dd.mm.yy (+ delta sec.).

- **datediff_days(t1 , t2)**
  liefert Differenz von »t1« und »t2« in Tagen.

- **datetime(t [, delta])**
  liefert Datum + Zeit zu »t« als dd.mm.yy HH:MM:SS (+ delta sec.).

- **datetimetz(t [, delta])**
  liefert Datum + Zeit zu »t«als dd.mm.yy HH:MM:SS + TZ (+ delta sec.).

- **div(zaehler, nenner)**
  bzw. Zähler / Nenner berechnet einen Quotienten.

- **docpath([id])**
  Array, der die Containerhierarchie liefert (docpath[0] == root()).

- **eq(x,y)**
  bzw. x==y ist ein Prädikat, das Wahr liefert, wenn zwei Zahlen oder Strings gleich sind (d.h 2.0 == 2).

- **ge(x,y) bzw. x >= y**
  ist ein Prädikat, das Wahr liefert, wenn »arg1 >= arg2«.

- **get_doctype([id])**
  bestimmt den Dokumenttyp von »id« (selbst).

- **get_id_byname(name [, type [, fail [, root]]])**
  liefert die »id« von Name mit Type, gesucht ab Root. Fail kommt, wenn nicht gefunden.

- **gt(x,y) bzw. x > y**
  ist ein Prädikat, das Wahr liefert, wenn »arg1 > arg2«.

- **hash_elementhash_element(hash, key)**
  liefert den Wert von »Key« im »Hash«.

- **hash_fromarray(array)**
  erzeugt aus einem Array (key1, value1, key2, ...) einen Hash {key1 => value1, key2 =>...}.

- **hash_fromarrays(key_array, value_array)**
  erzeugt aus zwei gleich großen Arrays einen Hash.

- **hash_keys(hash)**
  liefert ein Array mit den Schlüsseln des Hashes.

- **hash_toarrayhash_toarray(hash)**
  liefert ein Array mit den Schlüsseln und Werten des Hashes.

- **hash_values(hash)**
  liefert ein Array mit den Werten des Hashes.

- **host(cn)**
  liefert die ID des mit »cn« bezeichneten Host. Ist »cn« leer, wird der Host gesucht, auf dem die DocExpression ausgeführt wird.

- **hosts()**
  Array des Hosts liefern (#0 ist immer Master).

- **is_a(type [, id])**
  ist wahr, wenn ID (selbst) den Typ »type« hat.

- **is_unique(attribut [, wert [, root]])**
  ist wahr, wenn der Wert »val« für das Attribut (ab »root«) eindeutig ist.

- **join(trenner, array)**
  wandelt ein Array in einen String, wobei die Werte mit dem Trenner (zB ",") getrennt werden.

- **lc(STRING)**
  wandelt »STRING« in »string«.

- **le(x,y)**
  » x<=y« ist ein Vergleichsoperator für »x« und »y«.

- **lt(x,y)**
  »x<y« ist ein Vergleichsoperator für »x« und »y«.

- **master()**
  liefert die ID des Masters.

- **matches(str, pattern, res)**
  liefert ein Ergebnis, wenn der String auf das Muster »pattern« matcht (Ergebnis darf kein »throw« sein).

- **matchesnot(str, pattern, res)**
  liefert ein Ergebnis, wenn der String NICHT auf das Muster »pattern« matcht (Ergebnis darf kein »throw« sein).

- **month(time)**
  liefert dem Monat (1..12) zum Zeitstempel »time«.

- **mult(x,y)**
  bzw. »a * b« berechnet das Produkt von »a« und »b«.

- **ne(x,y)**
  bzw. »a != b« ist das Prädikat zur Ungleichheit des Strings oder der Zahlen »a« und »b«.

- **not(a)**
  bzw. »!a« liefert logische Negierung von »a«.

- **or(a,b)**
  bzw. »a || b« liefert logisches oder von »a,b«.

- **parent([id])**
  liefert den nächst höheren Container zu einer ID (default: selbst).

- **quote(arg)**
  liefert Arguments als String zurück.
- **root()**
  liefert den Wurzelcontainer.
- **sort(array)**
  Array sortieren.
- **split(trenner, string)**
  String am Trennzeichen in Array spalten: »a,b,c -> (a, b, c)«.
- **streq(a,b)**
  vergleicht die Strings »a« und »b« (dH streq("2.0", "2") ist falsch).
- **sub(x,y)**
  »x-y« bildet eine Differenz.
- **subst(str, suche, ersetze)**
  ersetzt in String das erste Muster »suche« mit »ersetze«.
- **substall(str, suche, ersetze)**
  ersetzt in String jedes Muster »suche« mit »ersetze«.
- **throw(Fehlermeldung)**
  Wirft eine Ausnahme mit der angegebenen Fehlermeldung.
- **time()**
  Sekundengenauer; UTZ Zeitstempel (format yyyyMMDDhhmmssZ).
- **today()**
  Heutiges Datum als TT.MM.YYYY.
- **uc(string)**
  wandelt »String« in »STRING«.
- **year(dbzeit)**
  liefert das 4-stellige Jahr, das zum Zeitpunkt gehört.

12.4 Beispiel

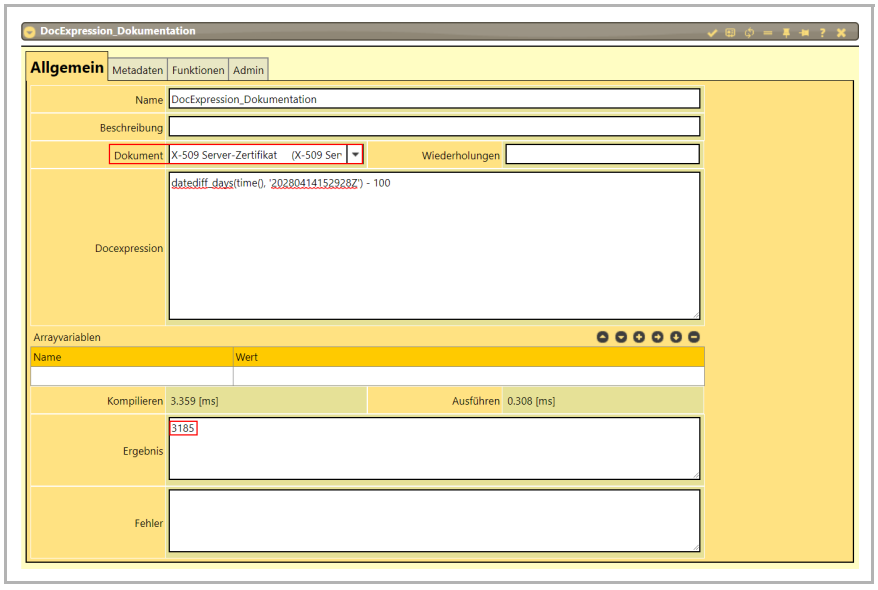
Die folgende DocExpressions berechnet die Gültigkeitsdauer eines X.509 Zertifikats: **datediff_days(time(), '20280414152928Z') - 100**

Die Funktion **»datediff_days«** berechnet die Differenz in Tagen.

Die Funktionsargumente sind die Funktion **»time()«**, die das aktuelle Datum und Uhrzeit liefert und eine Zeichenkettenkonstante, die in diesem Fall den Endzeitpunkt der CA angibt. Von der Differenz in Tagen, die die Funktion **»datediff_days«** berechnet, wird die Zahl 100 abgezogen.

Alle Zertifikate, die mit einer so berechneten Gültigkeit angelegt werden, laufen 100 Tage vor dem angegebenen Zeitpunkt, hier der 14.4.2028 um 15:29:28 GMT, ab , egal wann sie angelegt werden.

Im Screenshot unten sieht man wie man diese DocExpressions im **»DocExpression Debugger«** testen kann. Sie bezieht sich auf ein X.509 Zertifikatsobjekt, was aber in diesem Fall nicht nötig wäre, weil kein Attribut verwendet wird. Durch einen Klick auf die Schaltfläche »Übernehmen« wird die DocExpressions kompiliert und ausgeführt. Hat man sich vertippt, kommt im Feld **»Fehler«** eine Meldung. Sind die DocExpressions richtig eingegeben, wird im Feld **»Ergebnis«** das Resultat angezeigt. (Das angezeigte Ergebnis ist natürlich vom Zeitpunkt der Ausführung abhängig).

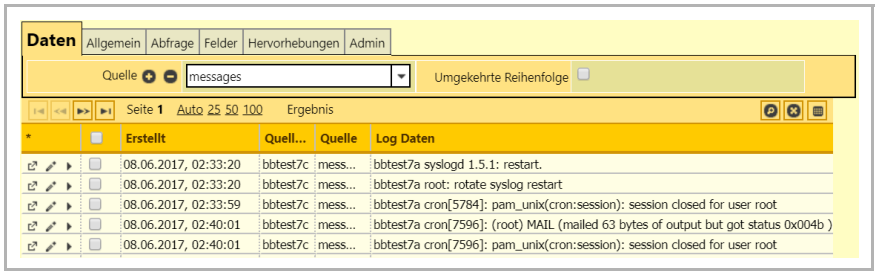


13 Weiterführende Themen

13.1 Logfiles

13.1.1 Ansehen/Auswerten

Für eine übersichtliche Ansicht von Logdateien wird das Logfileanzeige-Objekt verwendet. Dieses lässt sich durch Rechtsklick auf einen beliebigen Container unter **» Neu > Daten «** anlegen. Im Reiter **» Allgemein «** des Logfileanzeige -Objektes wird in dem Feld **» Quelle «** der Prozess angegeben, von dem Log-Einträge angezeigt werden sollen. Außerdem muss im Reiter Allgemein eine Name für das Logfileanzeige-Objekt vergeben werden. Mit einem Klick auf **» Suche «** oder **» Übernehmen «**, werden die Einträge des Logfiles in Tabellenform angezeigt.



13.1.2 Konfigurieren

Im Reiter **» Abfrage «** des Logfileanzeige-Objekts können Kriterien spezifiziert werden, welche Einträge des Logfiles angezeigt werden sollen. Im Reiter **» Felder «** kann eingestellt werden, welche Felder in der Tabelle ausgegeben werden sollen. Für nähere Information zur Konfiguration der Abfrage und der Felder.

→ *Siehe „13.6 | Abfragen" auf Seite 173.*

Die Kriterien der Abfrage der Log-Einträge und die Felder der Tabelle lassen sich beliebig anpassen.

Durch Klicken auf das Lupen-Symbol **» Filter anzeigen «** öffnen sich Suchfelder oberhalb jeder Tabellenspalte. Hiermit können die Einträge der Tabelle nach Stichworten durchsucht werden. Gefundene Suchbegriffe werden in der Tabelle rot hervorgehoben. Durch Klicken auf die Pfeile links neben den Suchfeldern kann zum nächsten bzw. zum vorherigen Fund gewechselt werden. Für Spalten, die Daten

oder Uhrzeiten enthalten, funktioniert die Filterfunktion wie folgt: Bei Eingabe eines Tages, wie z. B. **» 1. «**, werden alle Daten gesucht, die am ersten dieses Monats stattfinden. Wird ein Tag und ein Monat, wie z. B. **» 1.1. «** eingegeben, werden alle Daten vom 1. Januar dieses Jahres herausgesucht. Wird nach einer Uhrzeit gesucht, werden nur Einträge mit dieser Uhrzeit vom gleichen Tag gesucht.

Durch Klicken auf das Kreis-Symbol links neben den Suchfeldern, werden die Logfile-Einträge gefiltert. Nur Einträge, die der Suche entsprechen, werden angezeigt.

Durch Setzen des Häkchens **» Umgekehrte Reihenfolge «** im Reiter **» Daten «** werden die neuesten Logfile-Einträge zuoberst in der Tabelle angezeigt.

Im Falle einer hohen Anzahl von Logfile-Einträgen werden diese auf mehrere Seiten aufgeteilt. Durch Klicken auf die Pfeile links unter der Tabelle kann durch die Seiten geblättert werden. Alternativ kann auch mithilfe der Pfeiltasten auf der Tastatur oder der **» Bild Auf «**- und **» Bild Ab «**-Tasten geblättert werden.

13.1.3 Log-Informationen exportieren

Um Informationen aus einer Logdatei zu exportieren, legt man ein Logfileanzeige-Objekt an, in dem man die Kriterien der Log-Informationen, die exportiert werden sollen, festlegt. Befinden sich alle gewünschten Informationen in der Tabelle des Logfileanzeige-Objektes, lässt sich diese durch Klicken auf das Gitter-Symbol rechts oberhalb der Tabelle exportieren. Durch Klicken auf das Symbol erscheint ein Auswahl-Menü, in welchem man zwischen verschiedenen Datei-Formaten wählen kann. Tabellen können als .xlsx- oder .cvs-Dateien oder als Liste exportiert werden.

13.2 Updates

13.2.1 Lokaler Update-Server vs. ECOS Update-Server

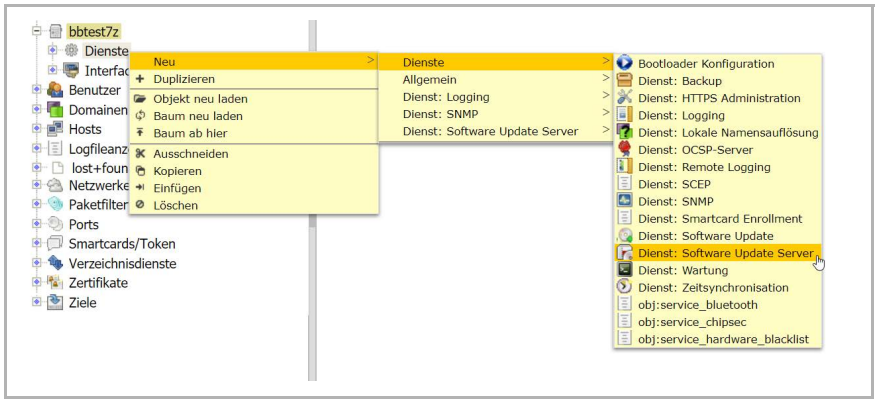
Updates können auf zwei verschiedenen Wegen auf den ECOS Secure Boot Stick aufgespielt werden - über einen lokalen Updateserver oder über den ECOS Updateserver. Das Update über den ECOS Updateserver erfolgt direkt über die Internetverbindung und erfordert eine HTTPS-Verbindung zum ECOS Updateserver.

Alternativ können die Updates auch intern von der ECOS System Management Appliance zur Verfügung gestellt werden. In diesem Fall erfolgt das Update über die bestehende Master-Slave-Verbindung. Dies ermöglicht den Einsatz von Bootsticks

mit verschiedenen Versionen, da die Steuerung, welcher Stick welche Updates zur Verfügung gestellt bekommt, über das zentrale Management erfolgt. Somit hat der Administrator die volle Kontrolle über das Updaten der Bootsticks.

13.3 Dienst: Software-Update-Server einrichten

Zur Einrichtung eines lokalen Updateservers benötigt man den Dienst **» Software Update Server «**. Dieser befindet sich, falls bereits vorhanden, im Container **» Dienste «** unter der ECOS System Management Appliance. Andernfalls kann er dort neu angelegt werden.



Standardmäßig erfolgt das Updates von Slaves (Bootsticks oder weiteren Appliances) über die bestehende Master-Slave-Verbindung. Nur wenn die Verbindung für die Updates über einen anderen Weg geroutet werden soll, kann eine zusätzliche Verbindung mit den Feldern **» HTTPS-Server Adresse «** und **» HTTPS-Server Port «** konfiguriert werden.

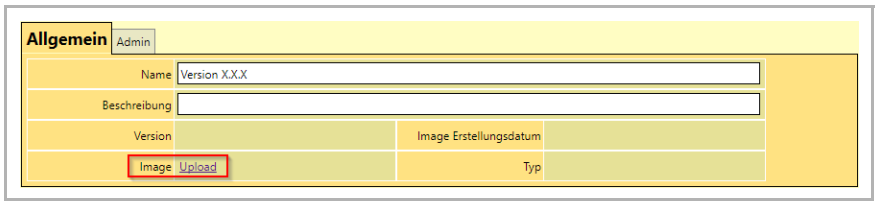
Im Feld **» Standard für Updates «** besteht die Möglichkeit, eine Standard-Softwarequelle anzugeben . die für alle Bootsticks gültig ist, sofern nicht innerhalb des Bootsticks im Dienst **» Software-Update «** eine abweichende Quelle konfiguriert ist. → *Siehe „13.4 | Dienst: Software-Update einrichten" auf Seite 166*.

Damit der Update Server aktiv ist, muss ein Häkchen bei **» Starten «** gesetzt sein.

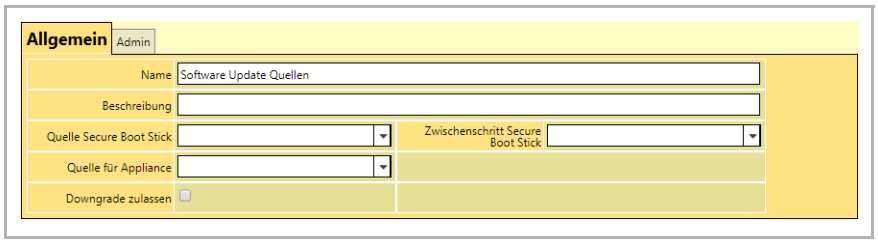
13.3.1 Bereitstellung eines Image für Update-Server

Im Falle eines lokalen Updateservers müssen diesem die Software Update-Images zur Verfügung gestellt werden.

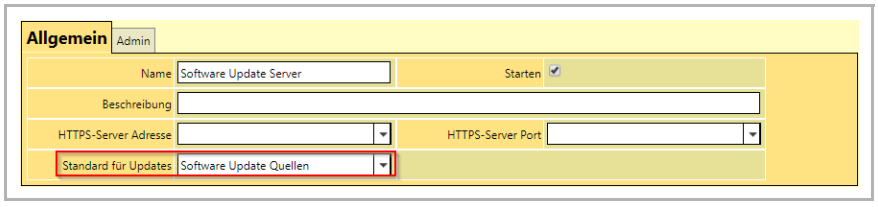
Dafür wird ein Konfigurationsobjekt **» Software Update-Image «**, welches unter **» Neu > Software-Update «** zu finden ist, angelegt. Nach Vergabe eines Namens und Klicken auf **» Übernehmen «** kann hier im Feld **» Image «** über **» Upload «** eine Image-Datei hochgeladen werden.



Des Weiteren muss ein Konfigurationsobjekt **» Software Update-Quelle «** erstellt werden, in dem das Software Update-Image wiederum als Quelle für den Bootstick oder die Appliance referenziert wird.

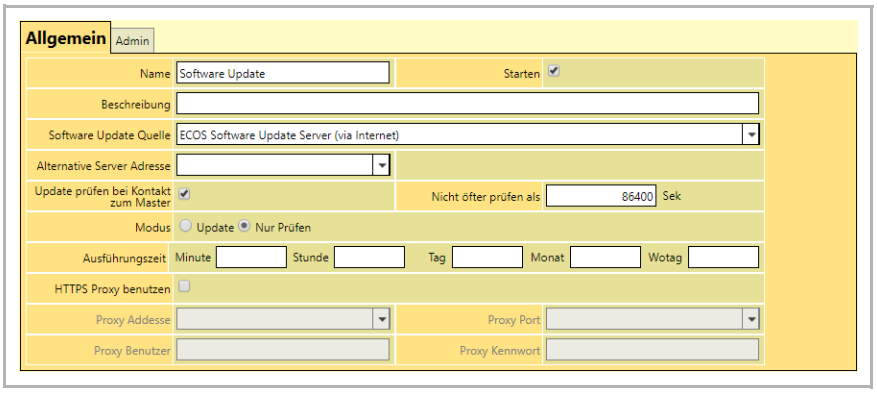


Dieses Quelle-Objekt kann dann im lokalen Update Server- oder Software Update-Objekt im Feld **» Standard für Updates «** angegeben werden.



13.4 Dienst: Software-Update einrichten

Zum Updaten der Appliance bzw. der Bootsticks wird der Dienst **» Software Update «** benötigt. Dieser wird im Container **» Dienste «** unterhalb des Appliance-Objektes bzw. unterhalb des Bootstick-Objektes angelegt.



Im Feld **» Software Update-Quelle «** wird die Quelle für die Updates spezifiziert. Diese kann entweder ein Updateserver oder direkt ein hinterlegtes ein Software-Update Quelle-Objekt sein.

Ist ein Häkchen im Feld **» Update prüfen bei Kontakt zum Master «** gesetzt, prüft der Bootstick bei jeder Verbindung zum Master, ob Updates vorliegen. Diese Einstellung ist für Bootsticks sinnvoll, da diese nicht permanent laufen und somit zeitgesteuerte Updates nicht zuverlässig möglich sind.

Mit dem Feld **» Modus «** lässt sich konfigurieren, ob nur auf neue Updates geprüft wird oder diese auch direkt installiert werden.

Im Feld **» Ausführungszeit «** kann ein bestimmter Zeitpunkt angegeben werden, zu dem automatisch auf ein Update geprüft wird. Dieses wird dann gegebenenfalls automatisch installiert.

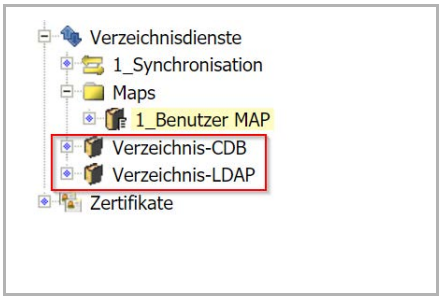
Wird nicht die Managementverbindung für das Update benutzt, kann über die Option **» HTTPS Proxy benutzen «** die Kommunikation über einen HTTPS-Proxy erfolgen. Dieser kann im Untermenü konfiguriert werden. Ist die Option deaktiviert, muss,wenn nicht die Managementverbindung für das Update genutzt wird, eine direkte HTTPS-Verbindung ins Internet möglich sein, um Updates ausführen zu können.

13.5 Verzeichnissynchronisation

Mittels der Verzeichnissynchronisation ist es möglich, Objekte aus einem Verzeichnisdienst zu im- oder exportieren, z. B. können Benutzer oder Bootsticks automatisch für alle Benutzer angelegt werden, die im Active Directory (AD) in einer bestimmten Gruppe Mitglied sind. Dazu werden die drei Konfigurationsobjekte **» Verzeichnisdienst «**, **» Mapping «** und **» Verzeichnissynchronisation «** benötigt.

13.5.1 Verzeichnisdienst

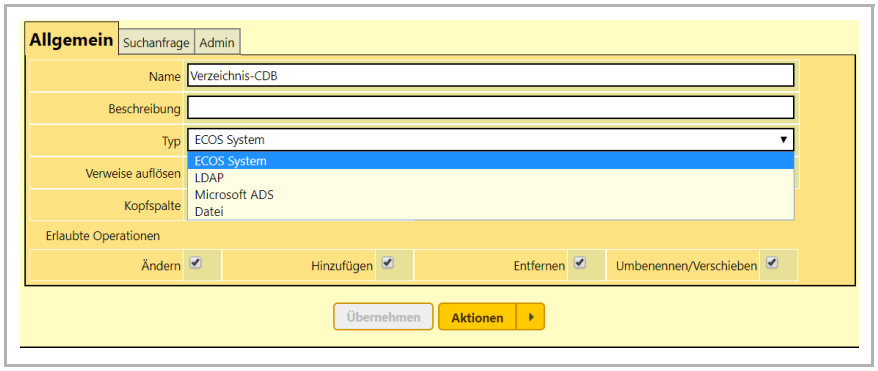
Es werden zwei Konfigurationsobjekte **» Verzeichnisdienst «** benötigt. In einem wird die Quelle und im anderen das Ziel der Verzeichnissynchronisation konfiguriert.



Im Feld **» Typ «** wird der Typ des Verzeichnisses ausgewählt. Einer der folgenden Werte ist möglich:

- ECOS System: die ECOS System Management Appliance selbst
- LDAP: ein beliebiger LDAP-Server
- Microsoft ADS: Microsoft Active Directory
- Datei

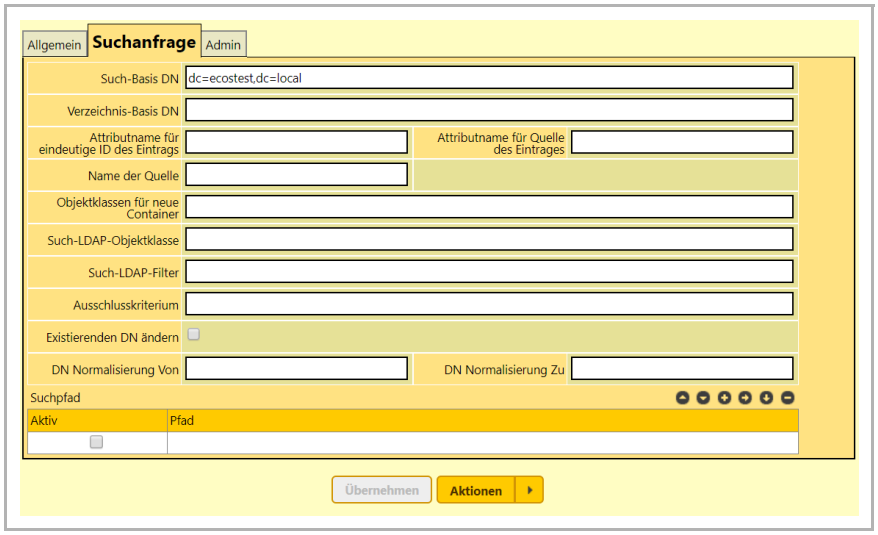
Je nach Auswahl öffnet sich ein Untermenü, in welchem die notwendigen Einstellungen für den jeweiligen Typ getroffen werden.



Unter **» Erlaubte Operationen «** werden folgende Lese- und Schreibberechtigungen für das Verzeichnis vergeben:

- Ändern: Objekte dürfen geändert werden
- Hinzufügen: Die Verzeichnissynchronisation darf neue Objekte hinzufügen
- Entfernen: Die Verzeichnissynchronisation darf bestehende Objekte löschen, soweit sie im Quellverzeichnis nicht mehr vorhanden sind
- Umbenennen/Verschieben: Die Verzeichnissynchronisation darf bestehende Objekte verschieben und umbenennen

Im Reiter **» Suchanfrage «** können weitere Einstellungen zur Suche der zu synchronisierenden Objekte getroffen werden.



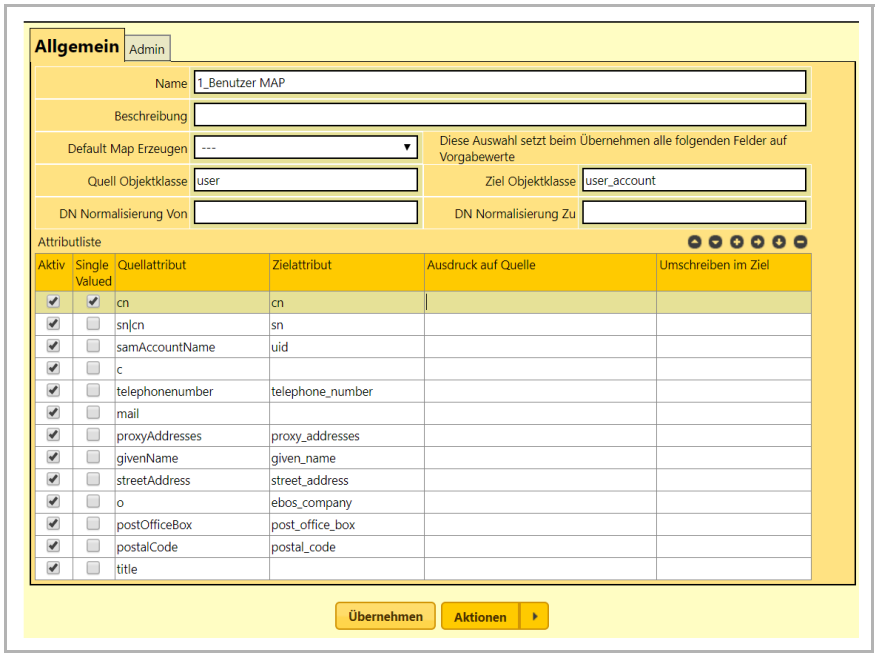
Im Feld **» Such-Basis DN «** wird die Basis angegeben, unter der die zu synchronisierenden Objekte für den Report gesucht werden. Hier ist die Angabe eines vollständigen DN's notwendig. Wird das Feld leer gelassen, wird das gesamte Verzeichnis durchsucht. Bei dem Ziel **» Verzeichnisdienstobjekt «** legt das Feld **» Such-Basis-DN «** den Container fest, in dem die neuen Objekte angelegt werden.

Beim Typ **» LDAP «** kann ein LDAP-Suchfilter angegeben werden und so die Quellobjekte z. B. auf eine Gruppe eingeschränkt werden.

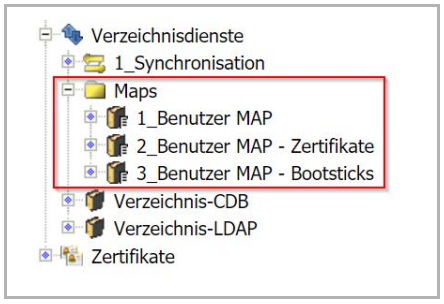
13.5.2 Verzeichnis-Map

Im Objekt **» Verzeichnis-Map «** wird eine Attributliste angelegt, in der die Quellattribute entsprechenden Zielattributen zugeordnet werden. Im Feld **» Quell Objektklasse «** wird die Objektklasse definiert, für die das Mapping angewendet werden soll. Das Feld **» Ziel Objektklasse «** gibt an, welche Objektklasse beim Anlegen neuer Objekte verwendet wird.

Das ECOS System hat bereits verschiedene Default-Mappings vorkonfiguriert. Mithilfe des Feldes **» Default Map erzeugen «** und Klicken auf **» Übernehmen «**, können diese aufgerufen werden. Dabei werden alle anderen Felder überschrieben. Die vorkonfigurierten Felder können anschließend bei Bedarf noch angepasst werden.



Es können mehrere **» Verzeichnis-Map «**-Objekte in einem Container angelegt werden, in denen das Mapping einzelner Objektklassen definiert wird. Der Container kann anschließend im Objekt **» Verzeichnissynchronisation «** als Map übergeben werden. Dadurch ist es möglich, aus einem Quellobjekt (z. B. aus einem Benutzer), mehrere Zielobjekte (z. B. einen Benutzer und einen Bootstick) anzulegen.



13.5.3 Verzeichnissynchronisation

Im Konfigurationsobjekt **» Verzeichnissynchronisation «** müssen Quelle und Ziel, sowie ein Mapping zwischen den beiden Verzeichnissen angegeben werden.

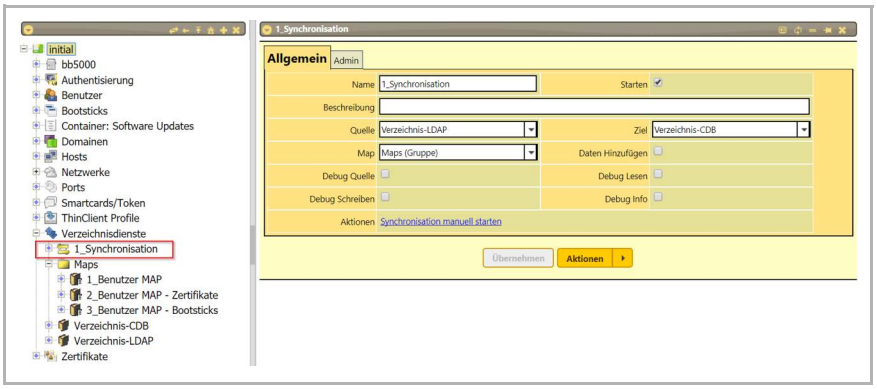
Durch Setzen eines Häkchens bei **» Starten «** wird die automatische Verzeichnissynchronisation aktiviert. Wann diese jeweils ausgeführt wird, wird im Container **» Verzeichnisdienste «** festgelegt. Eine manuelle Verzeichnissynchronisation kann unabhängig davon, ob das Objekt aktiviert ist oder nicht, ausgeführt werden.

Die Felder **» Quelle und Ziele «** bestimmen den Provider, welcher die Quelldaten zur Verfügung stellt, bzw. den Provider, über den die Daten in das Zielverzeichnis geschrieben werden.

Im Feld **» Map «** wird das Verzeichnis-Map-Objekt referenziert, in dem festgelegt ist, welche Attribute synchronisiert werden und wie diese gegebenenfalls einander zugeordnet werden. Es kann auch ein Container mit mehreren Mapping-Objekten ausgewählt werden. In diesem Fall wird das passende Mapping anhand der Quellklasse im Mapping-Objekt bestimmt bzw. mehrere Zielobjekte angelegt, wenn mehrere Quell-Objektklassen übereinstimmen.

Ist das Häkchen bei **» Daten Hinzufügen «** gesetzt, werden in bestehenden Objekten Daten hinzugefügt, nicht aber neue Objekte angelegt oder bestehende Objekte gelöscht. Dies ist nur dann sinnvoll, wenn mehrere Verzeichnissynchronisationen in das gleiche Zielobjekt schreiben sollen. Normalerweise sollte diese Option nicht ausgewählt sein.

Über die Aktion **» Synchronisation manuell starten «** wird die Verzeichnissynchronisation direkt gestartet. Dies geschieht unabhängig davon, ob das Häkchen bei **» Starten «** im Objekt gesetzt ist.



13.6 Abfragen

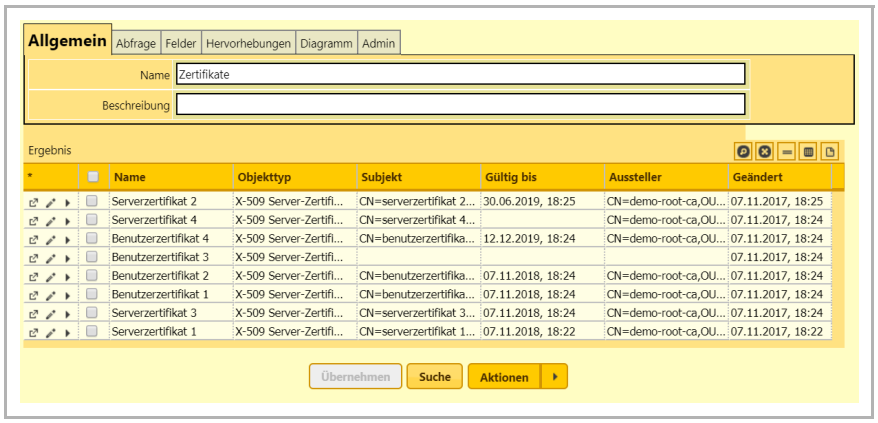
Mithilfe des Abfrageobjektes lassen sich Übersichtstabellen von beliebigen anderen Konfigurationsobjekten erstellen und verwalten. Die Tabelle besitzt dabei alle Eigenschaften und Funktionen, die im Kapitel → *Siehe „2.6.4 | Tabellen" auf Seite 32* erläutert sind.

Das Formular des Abfrageobjektes besteht aus den Registerkarten **» Allgemein «**, **» Abfrage «**, **» Felder «** und **» Hervorheben «**.

13.6.1 Registerkarte Allgemein

In der Registerkarte **» Allgemein «** kann der Name des Konfigurationsobjektes und, falls gewünscht, eine Beschreibung eingegeben werden. Außerdem wird die Übersichtstabelle angezeigt.

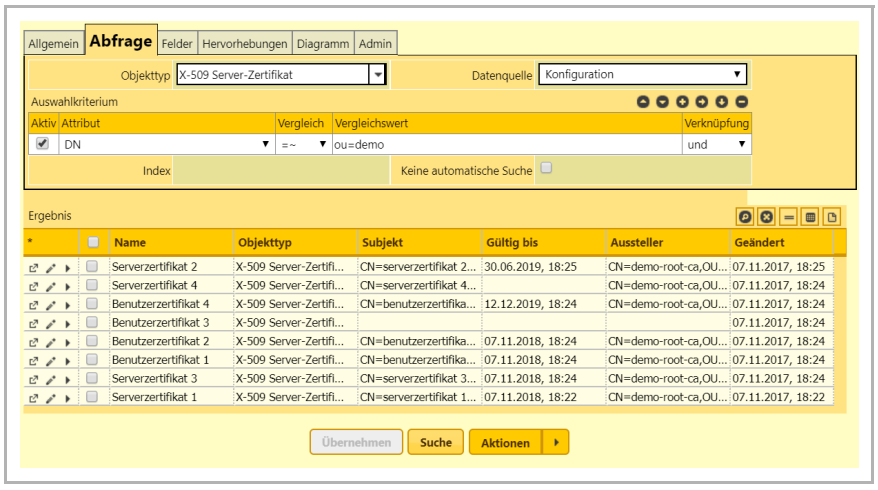
Die Konfiguration der Tabelle erfolgt in den weiteren Registerkarten.



13.6.2 Registerkarte Abfrage

13.6.2.1 Auswahl des Dokumenttyps

In der Registerkarte **» Abfrage «** wird zunächst der Dokumenttyp bestimmt, für den eine Abfrage erstellt werden soll. Nach Auswahl eines Dokumenttyps, wie im Beispiel X-509 Server Zertifikat, werden alle Konfigurationsobjekte dieses Typs in der Tabelle aufgelistet.



13.6.2.2 Erstellen von Vergleichen der Attribute

Sollen nur Konfigurationsobjekte mit einem bestimmten Attribut-Wert angezeigt werden, kann das in der Registerkarte **» Abfrage «** eingestellt werden. Dafür das gewünschte Attribut aus dem Auswahl-Menü, das erscheint, wenn man auf den

Pfeil im Feld **» Attribut «** klickt, auswählen, wie im Beispiel **» Gültig bis «** und den Vergleich, mit dem der Attribut-Wert verglichen werden soll.

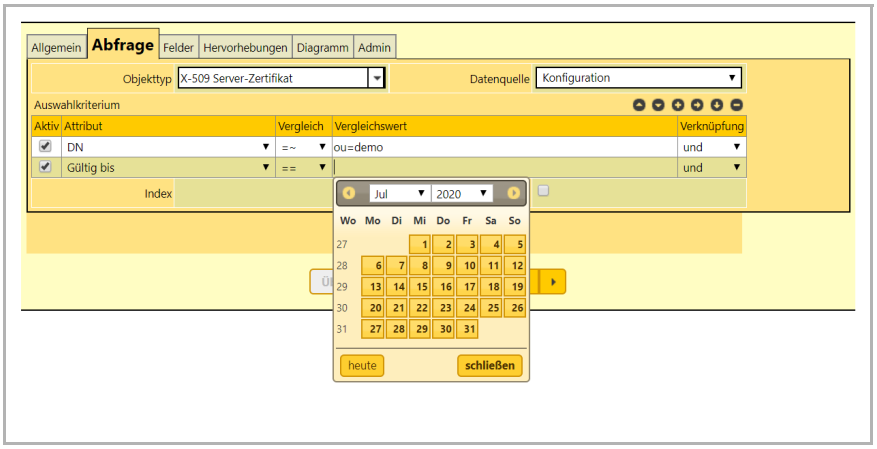
Mögliche Vergleichsoperatoren:

Vergleichs-operator	Vergleich	Erklärung
==	gleich	
!=	ungleich	
>	größer	
<	kleiner	
>=	größer gleich	
<=	kleiner gleich	
=*	Wildcard	Suche nach Begriffen, die Platzhalter enthalten: ? für genau ein Zeichen * für beliebig viele (auch null) Zeichen)
!*	nicht Wildcard	Gibt alle Werte zurück, die nicht den Vergleichswert enthalten (Gegenteil von Wildcard)
=~	regulärer Ausdruck	http://perldoc.perl.org/perlre.html#Regular-Expressions
!~	nicht regulärer Ausdruck	Gibt alle Werte zurück, die nicht den regulären Ausdruck enthalten

Tabelle 13-3 Vergleichsoperatoren

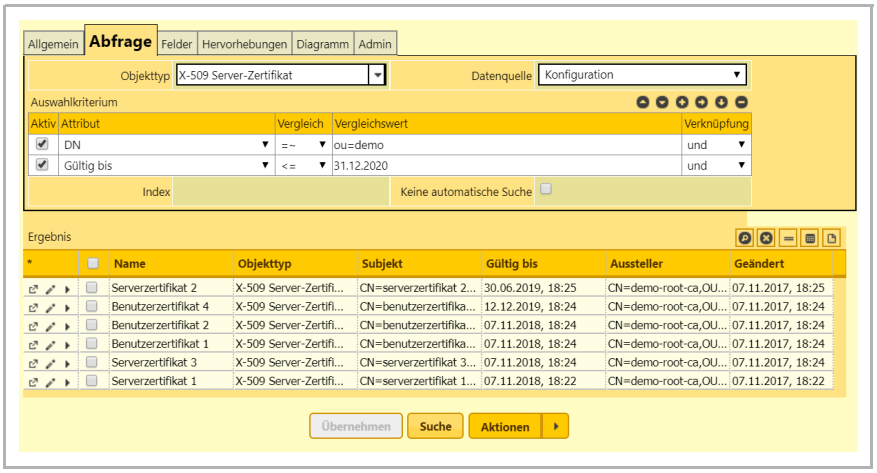
Das Feld **» Vergleichswert «** passt sich dabei immer dem ausgewählten Attribut an. Handelt es sich um ein Datum wie bei **» Gültig bis «**, wird ein Kalender angezeigt, in dem man den Vergleichswert auswählen kann (alternativ lässt sich das Datum auch eintippen).

Wählt man dagegen zum Beispiel **» CA «**, erscheint durch Anklicken des Pfeils im Feld **» Vergleichswert «** ein Auswahl-Menü mit den möglichen Eingaben.



Bei einem Datumsfeld besteht des Weiteren die Möglichkeit, einen Ausdruck wie z. B. **» d+30 «** einzugeben. Dabei steht **» d «** für day (Tag) und **» +30 «** für die Anzahl der Tage, also 30 Tage nach dem heutigen Tag. Wahlweise besteht die Möglichkeit **» m «** für month (Monat) und **» y «** für year (Jahr) zu verwenden. Soll ein Datum in der Vergangenheit ausgewählt werden, wird anstatt dem **» + «** ein **» - «** verwendet. Auf diese Weise lassen sich Abfragen in Abhängigkeit vom aktuellen Datum erstellen. Zum Beispiel: Welches Zertifikat läuft in den nächsten 30 Tagen aus?

Im folgenden Beispiel werden nur X-509 Server Zertifikate aufgelistet, deren Gültigkeit vor dem 31.12.2020 ausläuft und bei deren CA es sich um die **» ECOS Demo CA «** handelt.



Mittels der Symbole + und − aus der Symbolleiste der Auswahlfunktion lassen sich weitere Vergleiche hinzufügen bzw. bereits vorhandene Vergleiche löschen. Um einen Vergleich zu löschen, muss er zuvor durch Anklicken markiert werden.

Änderungen werden erst angezeigt, wenn der Vergleich durch einen Haken bei **» Aktiv «** aktiviert wurde und die Änderungen durch **» Übernehmen «** abgespeichert wurden.

13.6.2.3 Keine automatische Suche

Normalerweise lädt sich die Tabelle der Abfrage automatisch, wenn die Abfrage geöffnet wird und jedes Mal, wenn Parameter der Abfrage geändert und durch **» Übernehmen «** bestätigt werden. Wird ein Haken bei **» Keine automatische Suche «** gesetzt, wird dies unterbunden.

Mithilfe der Schaltfläche **» Suchen «** am Ende des Formulars, wird die Tabelle manuell neu geladen.

13.6.3 Registerkarte Felder

In der Registerkarte **» Felder «** wird bestimmt, welche Eigenschaften der aufgelisteten Konfigurationsobjekte in der Tabelle auftauchen sollen. Dabei kann unter **» Quelle für Feldliste «** zwischen **» Standard «**, **» Definieren «** und **» Aus anderer Abfrage wählen «** ausgewählt werden. Wird **» Standard «** ausgewählt, werden in der Tabelle die vordefinierten Attribute angezeigt, die für das entsprechende Konfigurationsobjekt sinnvoll sind.

13.6.3.1 Felder selbst definieren

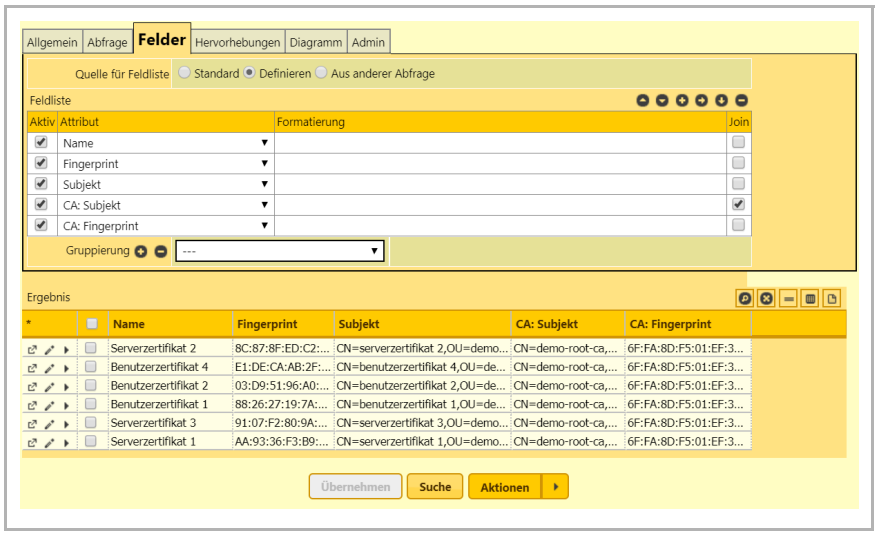
Über die Funktion **» Definieren «** lassen sich die gewünschten Felder frei unter den Attributen des entsprechenden Konfigurationsobjektes auswählen.

In der Feldliste wird das gewünschte Attribut im Auswahl-Menü ausgewählt, das erscheint, wenn auf den Pfeil im Feld **» Attribut «** geklickt wird.

Um die Änderung wirksam zu machen, muss ein Haken im Feld **» Aktiv «** gesetzt und auf **» Übernehmen «** geklickt worden sein (entweder in der Leiste des Konfigurationsobjektes auf das Symbol des Hakens ✔ oder auf die **» Übernehmen «**-Schaltfläche unter dem Formular).

Um weitere Felder hinzuzufügen oder vorhandene Felder zu löschen, werden die Symbole ✚ und ━ in der Symbolleiste der Feldliste verwendet.

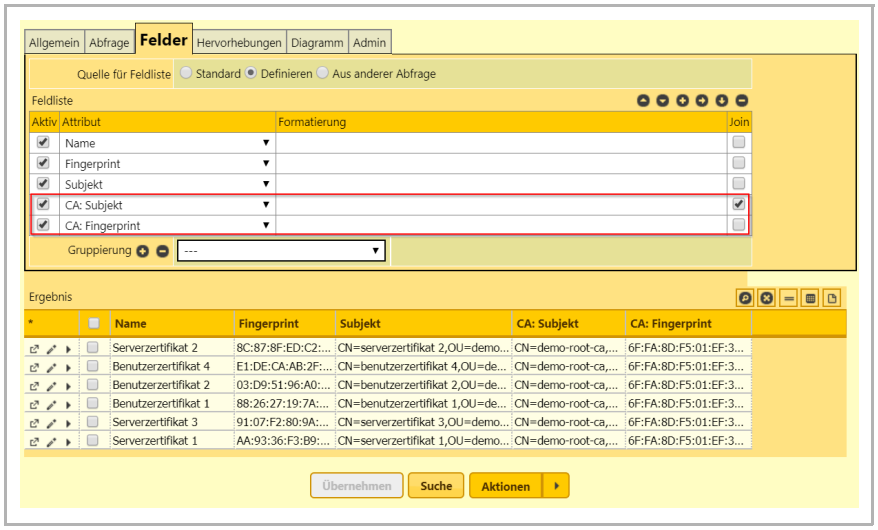
Mithilfe der Pfeil-Symbole kann man die Reihenfolge der Felder anpassen.



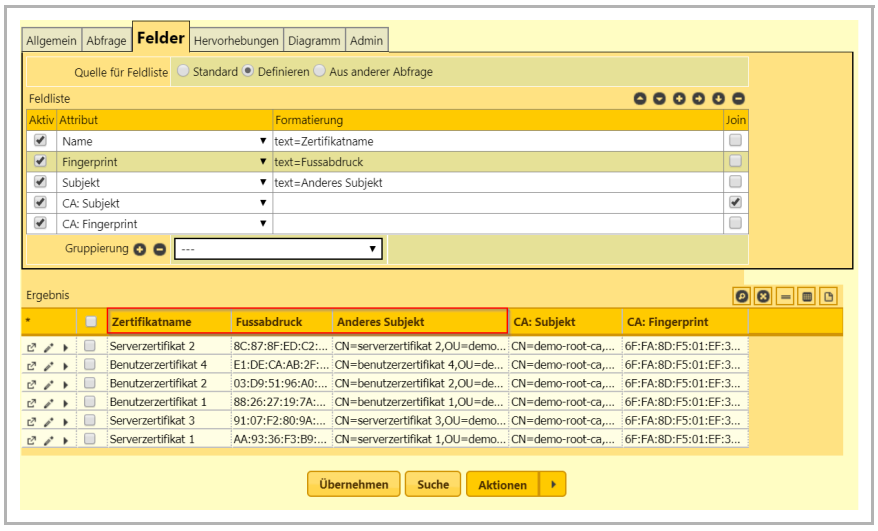
Neben den Attributen des Dokumenttyps selbst lassen sich auch einige Zusatzfelder auf verbundenen Objekten als Spalten für die Tabelle wählen. So können z. B. beim Dokumenttyp **» Zertifikat «** die Attribute **» Fingerprint «** und **» Subjekt «** des Konfigurationsobjektes CA als Felder wählen.

Fügt man Felder ein, die sich auf andere Konfigurationsobjekte beziehen, so besteht die Möglichkeit auch deren Attribute in der Tabelle anzuzeigen. Dafür muss ein Haken bei **» Join «** gesetzt sein. Ist der Haken gesetzt, tauchen die Attribute des Konfigurationsobjektes nun auch im Auswahl-Menü der Attribute auf. Im Beispiel wurde das Feld **» CA «** eingefügt und **» Join «** aktiviert. Attribute von CA sind im Auswahl-Menü der Attribute durch ein vorangestelltes **» CA -> «** gekennzeichnet.

Diese zusätzlichen Attribute werden dann ebenfalls in der Auswahlfunktion der Registerkarte **» Abfrage «** aufgelistet.



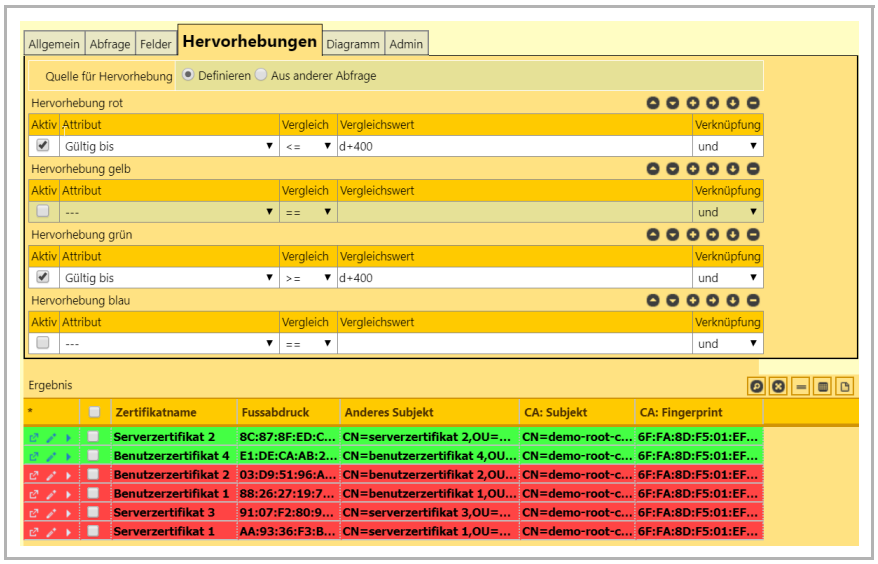
Mithilfe des Feldes **» Formatierung «** in der Feldliste lässt sich die Ansicht der Tabellenfelder anpassen. Der Ausdruck **» text = xy «** bei Formatierung führt dazu, dass der Name des entsprechenden Spaltenkopfes in **» xy «** umbenannt wird.



13.6.4 Hervorhebungen

Es besteht die Möglichkeit, Konfigurationsobjekte in der Tabelle farblich hervorzuheben. Dies funktioniert nach demselben Prinzip wie die Auswahlfunktion in der

Registerkarte » **Abfrage** «. Man wählt unter der gewünschten Farbe (zur Auswahl stehen rot, gelb, grün und blau) das Kriterium nach dem Objekt markiert werden sollen aus und aktiviert die Hervorhebung über die Box » **aktiv** « und die Funktion » **Übernehmen** «. Erfüllt ein Konfigurationsobjekt die Kriterien von Hervorhebungen mit unterschiedlichen Farben, wird es mit der Farbe mit der höchsten Priorität markiert. Die Prioritäten in absteigender Reihenfolge sind: rot, gelb, grün, blau.



13.7 Lesezeichen

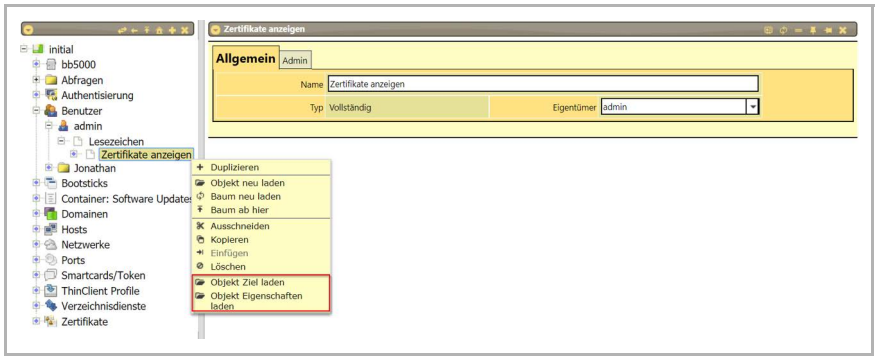
Lesezeichen ermöglichen den schnellen Zugriff auf einzelne Konfigurationsobjekte oder auch ein komplettes Seitenlayout.

Lesezeichen werden für jeden Benutzer getrennt gespeichert. Im Baum findet sich unter jedem Benutzer ein Ordner » **Lesezeichen** «, in welchem alle gespeicherten Lesezeichen hinterlegt sind. Durch Auswahl eines der Lesezeichen öffnet sich das entsprechende Konfigurationsobjekt bzw. eine Seite mit mehreren Konfigurationsobjekten, auf die das Lesezeichen verweist.

Durch Rechtsklick auf ein Lesezeichen öffnet sich ein Auswahl-Menü. Für eine Erklärung der Optionen. → *Siehe „2.4.2 | Kontext-Menü" auf Seite 18*.

Bei » **Lesezeichen** « ist das Menü um die Optionen » **Dokument Ziel laden** « und » **Dokument Eigenschaften laden** « erweitert. Die Option » **Dokument Ziel laden** « öffnet das Konfigurationsobjekt bzw. mehrere Konfigurationsobjekte, auf die das Lesezeichen verweist. Die Option » **Dokument Eigenschaften laden** « öffnet dage-

gen das Formular des Lesezeichens, in welchem man das Lesezeichen anpassen kann, z. B. den Namen oder den Eigentümer des Lesezeichens ändern.



Um ein Lesezeichen zu löschen, muss das entsprechende Lesezeichen mit Rechtsklick im Baum angeklickt und anschließend im Rechtsklick-Menü **» Löschen «** ausgewählt werden.

Zum Anlegen von Lesezeichen → *Siehe „2.6.2 | Menüleiste Konfigurationsobjekt" auf Seite 28* und für weitere Möglichkeiten zum Aufrufen von Lesezeichen → *Siehe „2.5.2 | Lesezeichen" auf Seite 24*.

13.8 Berechtigungen

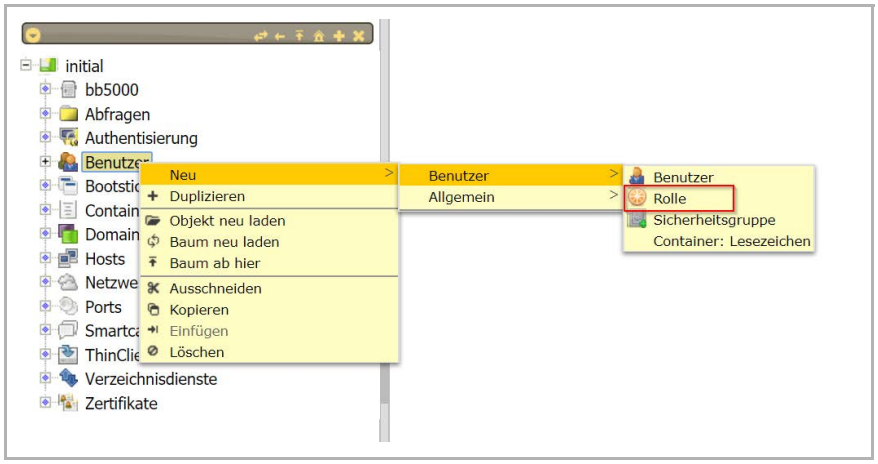
Jedem Benutzer lassen sich Berechtigungen zuweisen, die festlegen, auf welche Konfigurationsobjekte er Zugriff hat. Einzelnen Benutzern kann im Formular des jeweiligen Benutzers unter dem Reiter **» Allgemein «** Admin-Zugriff erteilt werden. Als Administrator hat dieser Benutzer sämtliche Berechtigungen und kann auf alle Konfigurationsobjekte und Funktionen zugreifen und diese auch beliebig bearbeiten und löschen.

Soll ein Benutzer nur eingeschränkte Berechtigungen erhalten, wird dem Benutzer eine Rolle zugewiesen. Rollen können individuell angelegt und mit ausgewählten Berechtigungen verknüpft werden.

Dazu ist es notwendig, beim Benutzer **» Zugriff auf Admin-Oberfläche «** zu aktivieren. Nur dann kann dieser sich überhaupt an der Admin-Oberfläche anmelden. Welche Objekte er dann sieht bzw. ändern darf, wird über die Zuordnung der Rollen bestimmt.

13.8.1 Rollen anlegen

Um eine neue Rolle zu erstellen, mit der rechten Maustaste auf den Ordner **» Benutzer «** klicken und unter **» Neu > Benutzer > Rolle «** auswählen.

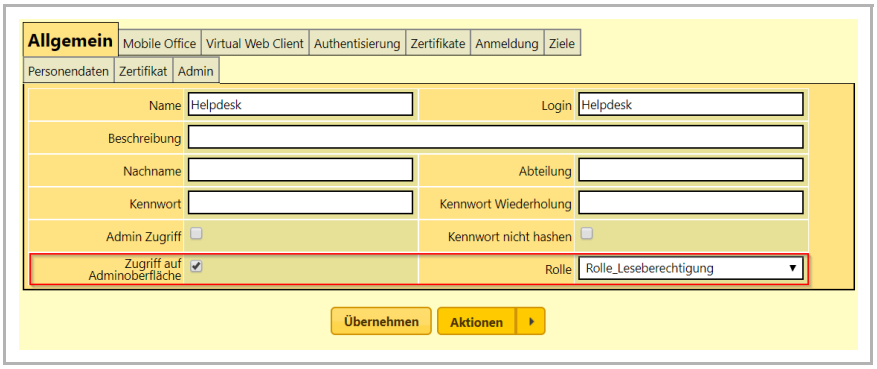


Es öffnet sich das Formular für die Rolle, in welchem der Rolle ein Name und eine Beschreibung gegeben wird. Mithilfe der Schaltfläche **» Anlegen «** wird die Rolle gespeichert und sie erscheint im Baum im Ordner **» Benutzer «**.

13.8.2 Benutzern Rollen zuweisen

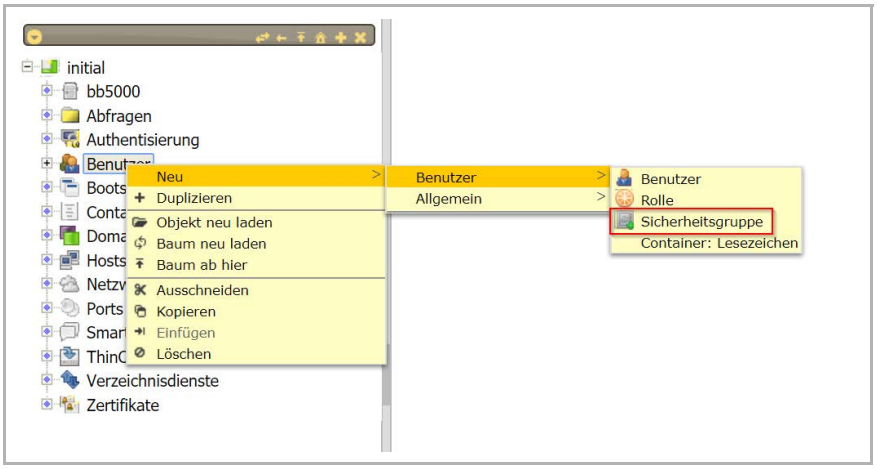
Bereits erstellte Rollen können Benutzern im Formular des Benutzers unter dem Reiter **» Allgemein «** zugeordnet werden. Bei einem Klick auf den Pfeil neben der Auswahlbox des Feldes **» Rolle «** erscheint ein Auswahl-Menü mit allen angelegten Rollen.

Durch Klicken auf eine der Rollen und anschließendem Klicken auf **» Übernehmen «**, wird diese dem Benutzer zugeordnet.



13.8.3 Rollen zu Gruppen zusammenfassen

Angelegte Rollen werden zu Sicherheitsgruppen zusammengefasst, denen wiederum Berechtigungen zugewiesen werden können. Zum Anlegen einer neuen Sicherheitsgruppe, mit der rechten Maustaste auf den Ordner **» Benutzer «** klicken und unter **» Neu > Benutzer > Sicherheitsgruppe «** auswählen. Daraufhin öffnet sich das Formular für die Sicherheitsgruppe, in welchem die Sicherheitsgruppe benannt und ihr Rollen zugeordnet werden können.



Durch Klicken auf den Pfeil rechts neben der Auswahlbox **» Rollen «** öffnet sich ein Auswahl-Menü mit allen angelegten Rollen. Über die Schaltflächen + − können weitere Rollen hinzugefügt bzw. gelöscht werden.

Mithilfe der Schaltfläche **» Anlegen «** wird die Gruppe gespeichert.

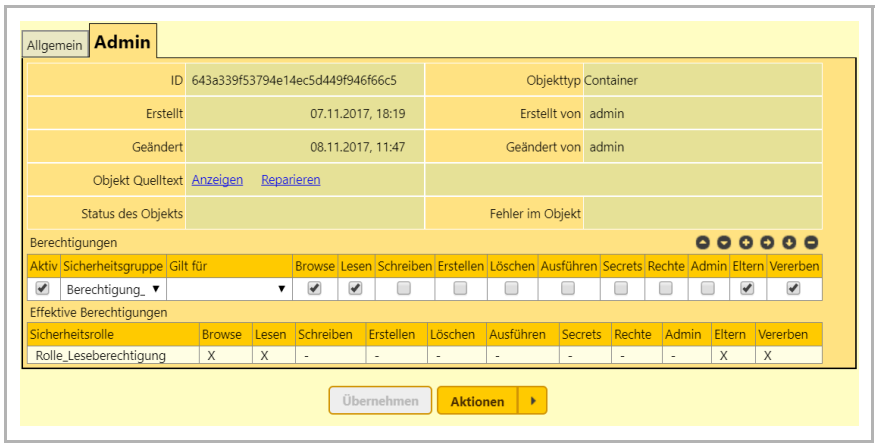
13.8.4 Gruppen Berechtigungen zuweisen

Im Reiter **» Admin «** des Konfigurationsobjektes, dessen Zugriff man regulieren möchte, kann einer Gruppe eine Berechtigung zugewiesen werden. Berechtigungen können nur von Benutzern, die **» Admin-Zugriff «** haben oder das Recht **» Rechte «** für das entsprechende Objekt besitzen, vergeben werden.

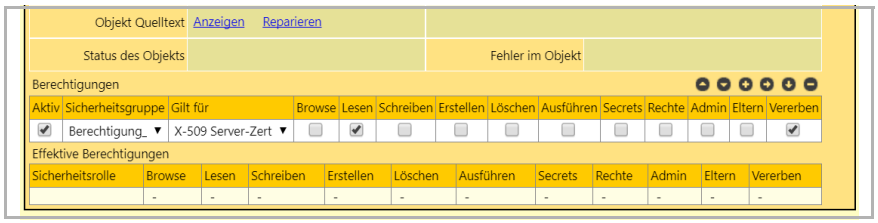
In der Tabelle **» Berechtigungen «** kann die Sicherheitsgruppe ausgewählt und die gewünschten Berechtigungen an diese Gruppe durch Setzen der entsprechenden Haken in den Feldern **» Browse «**, **» Lesen «**, **» Schreiben «**, **» Erstellen «**, **» Löschen «**, **» Secrets «**, **» Rechte «**, **» Admin «**, **» Eltern «** und **» Vererben «** vergeben werden.

Um die Berechtigungen zu aktivieren, muss der Haken bei **» Aktiv «** links in der Tabelle gesetzt und die Änderungen mithilfe von **» Übernehmen «** gespeichert worden sein.

Welche Rollen welche Berechtigungen für das aktuell angezeigte Objekt besitzen, lässt sich in der Tabelle **» Effektive Berechtigungen «** nachvollziehen.



Weiterhin können die Berechtigungen auf einen bestimmten Objekttyp beschränkt werden. Dies macht Sinn im Zusammenhang mit den Recht **» Vererben «**. Dabei wird die entsprechende Einstellung nur auf Objekte des ausgewählten Typs angewandt.



13.8.5 Rechtearten

13.8.5.1 Browse

Benutzer mit der Berechtigung **» Browse «** sehen das entsprechende Konfigurationsobjekt im Baum. Außerdem wird das Konfigurationsobjekt in der Suche angezeigt. Die Benutzer können das Formular des Konfigurationsobjektes jedoch nicht öffnen.

13.8.5.2 Lesen

Benutzer mit der Berechtigung **» Lesen «** für ein Konfigurationsobjekt, können das entsprechende Formular öffnen, jedoch keine Änderungen darin vornehmen.

13.8.5.3 Schreiben

Benutzer mit der Berechtigung **» Schreiben «** können das entsprechende Konfigurationsobjekt öffnen und Änderungen in seinem Formular vornehmen.

13.8.5.4 Erstellen

Benutzer mit der Berechtigung **» Erstellen «** können neue Konfigurationsobjekte desselben Typs anlegen.

13.8.5.5 Löschen

Benutzer mit der Berechtigung **» Löschen «** können bereits vorhandene Konfigurationsobjekte des entsprechenden Typs löschen.

13.8.5.6 Secrets

Benutzer mit der Berechtigung **» Secrets «** erhalten Zugriff auf Authentisierungsinformationen, wie z.B. Passwörter.

13.8.5.7 Rechte

Benutzer mit der Berechtigung **» Rechte «** dürfen an andere Benutzer Rechte vergeben.

13.8.5.8 Admin

Benutzer mit der Berechtigung **» Admin «** haben Zugriff auf die Administration eines Objekts. Sie können sich z. B. den Quelltext anzeigen lassen und Objekte reparieren.

13.8.5.9 Eltern

Ist ein Haken bei **» Eltern «** gesetzt, erhalten automatisch alle Konfigurationsobjekte, die im Baum über dem entsprechenden Konfigurationsobjekt stehen, das Browse-Recht, so dass der Anwender im Baum zu dem berechtigten Objekt navigieren kann.

13.8.5.10 Vererben

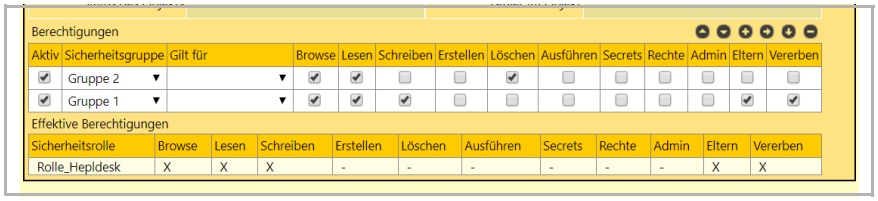
Ist ein Haken bei **» Vererben «** gesetzt, gelten die zugewiesenen Berechtigungen automatisch auch für Konfigurationsobjekte, die im Baum unter dem entsprechenden Konfigurationsobjekt existieren. Im Reiter **» Admin «** der untergeordneten Objekte lassen sich die Berechtigungen anpassen.

13.8.6 Sonderfälle bei Berechtigungen

13.8.6.1 Eine Rolle wird mehreren Gruppen zugeordnet

Eine Rolle kann mehreren Sicherheitsgruppen gleichzeitig zugeordnet sein. Ist dies der Fall, so verhalten sich die Berechtigungen der beiden Gruppen additiv, das heißt, besitzen die beiden Sicherheitsgruppen unterschiedliche Rechte für dieselben Objekte, so erhält der Benutzer die Berechtigungen beider Gruppen.

Beispiel: Sicherheitsgruppe 1 hat für das Objekt Lese-und Schreib-Zugriff. Sicherheitsgruppe 2 hat für dasselbe Objekt Lese-, und Lösch-Zugriff. Ein Benutzer, dessen Rolle beiden Sicherheitsgruppen zugeordnet wird, erhält Lese-, Schreib- und Lösch-Zugriff für dieses Objekt.

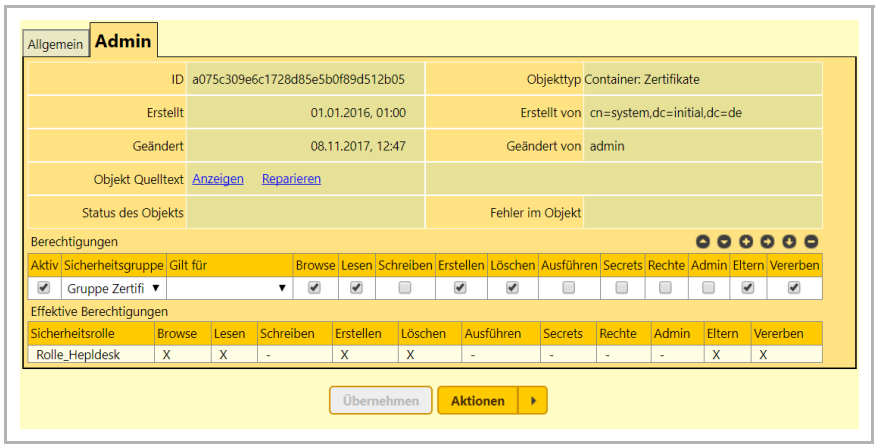


13.8.6.2 Unterschiedliche Rechte für Eltern und untergeordnete Objekte

Wird die Berechtigung **» Vererben «** bei einem Konfigurationsobjekt für eine Sicherheitsgruppe gesetzt, erhält diese Gruppe automatisch die ausgewählten Berechtigungen für alle Konfigurationsobjekte, die im Baum unter dem Objekt stehen. Wird der Sicherheitsgruppe andere Berechtigungen für ein untergeordnetes Objekt zugewiesen, so überschreibt diese Berechtigungsauswahl die des Eltern-Objektes.

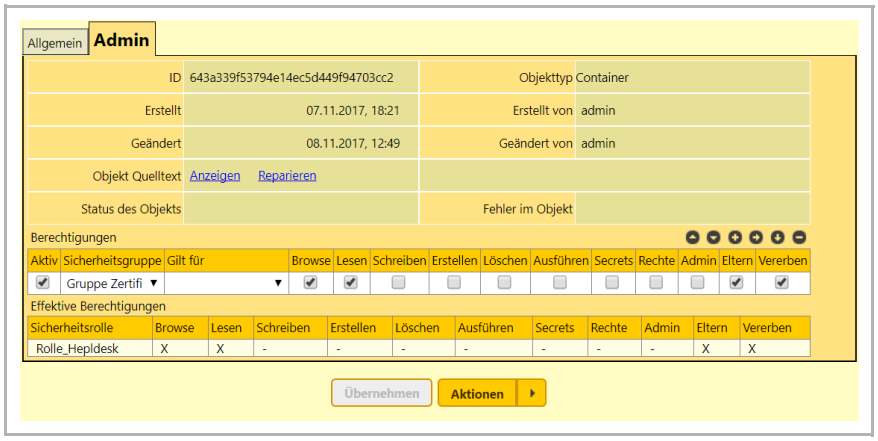
Beispiel: Im Container-Objekt **» Zertifikate «** wird der Sicherheitsgruppe **» Gruppe Zertifikate «** das Browse-, Lesen-, Erstellen- und Löschen-Recht gegeben. Außerdem sind die Berechtigungen **» Eltern «** und **» Vererben «** gesetzt. Unter dem Feld **» effektive Berechtigungen «** lässt sich ablesen, welche Rollen welche Berechtigungen besitzen. In diesem Fall haben alle Rollen, die in der Sicherheitsgruppe **» Gruppe Zertifikate «** sind, die oben aufgezählten Rechte.

Da **» Vererben «** aktiv ist, gelten diese auch für alle untergeordneten Objekte, also sämtliche Zertifikate in diesem Fall.



Soll der Gruppe für einzelne untergeordnete Objekte oder auch Container mehr oder weniger Rechte zugewiesen werden, kann dies in der Registerkarte **» Admin «** des entsprechenden Objektes geregelt werden. Die Rechte des Eltern-Objektes werden dadurch überschrieben und sind nicht mehr gültig.

Im Beispiel hat die Sicherheitsgruppe **» Gruppe Zertifikate «** nur noch Browse-, Lesen-, Eltern- und Vererben-Berechtigungen für sämtliche Objekte des Containers **» CA-DEMO «**. Die Berechtigungen **» Erstellen «** und **» Löschen «** sind nicht mehr gesetzt, obwohl sie im Eltern-Objekt » Zertifikate « zugewiesen sind.


Allgemein
Admin
ID 643a339f53794e14ec5d449f94703cc2
Objekttyp Container
Erstellt 07.11.2017, 18:21
Erstellt von admin
Geändert 08.11.2017, 12:49
Geändert von admin
Objekt Quelltext Anzeigen Reparieren
Status des Objekts
Fehler im Objekt
Berechtigungen
Aktiv Sicherheitsgruppe Gilt für Browse Lesen Schreiben Erstellen Löschen Ausführen Secrets Rechte Admin Eltern Vererben
Gruppe Zertifi
Effektive Berechtigungen
Sicherheitsrolle Browse Lesen Schreiben Erstellen Löschen Ausführen Secrets Rechte Admin Eltern Vererben
Rolle_Hepldesk X X - - - - - - - X X
Übernehmen
Aktionen

14 Technischer Support

Für technische Fragen zu unseren Produkten, wenden Sie sich gerne an unseren Support.

Sie erreichen uns unter:

Tel.: +49 (6133) 939-300
E-Mail: support[at]ecos.de

Für die Störungsannahme erreichen Sie uns Mo.-So. in der Zeit von 0.00 – 24:00 Uhr.

Die Bearbeitung der Supportfälle erfolgt Mo.-Fr., außer an gesetzlichen Feiertagen, in der Zeit von 8:00 – 18:00 Uhr.

Bitte halten Sie die Seriennummer Ihres Gerätes bereit.

Als Ihren primären Ansprechpartner, empfehlen wir Ihnen den Kontakt zu dem ECOS-Partner, über den Sie Ihre Produkte bezogen haben. Unsere Partner erhalten unsere bestmögliche Unterstützung, um Ihnen kompetent weiterzuhelfen und sind auch mit IT-Infrastruktur vertraut.

Hardwaretests bitte mit einer kurzen Beschreibung sowie Kontaktinformationen an hwtest@ecos.de senden.

Security-Vorfälle bitte schriftlich an support@ecos.de melden. Bitte eine ausführliche Beschreibung sowie Ihre Kontaktdaten beifügen.

Informationen zu Updates sind mit den ECOS Release.Notes erhältlich. Dazu besteht die Möglichkeit sich auf der ECOS Website unter Support anzumelden.

ECOS TECHNOLOGY GMBH
Sant' Ambrogio-Ring 13a-b
D-55276 Oppenheim

Telefon: +49 (6133) 939-0
E-Mail: info@ecos.de
Internet: www.ecos.de